

**A NOVEL DEEP LEARNING BASED CYBER ATTACK
DETECTION SYSTEM WITH BAIT BASED APPROACH FOR
MITIGATION**



**THESIS SUBMITTED TO SRINIVAS UNIVERSITY
FOR THE AWARD OF THE DEGREE OF**

Doctor of Philosophy

in

Computer Science

Researcher

Sangeetha Prabhu

Reg. No: 19SUPHDF38

Institute of Computer Science & Information Science
Srinivas University, Mangaluru - 575001

Research Guide

Dr. Nethravathi P. S.

Professor

Institute of Computer Science & Information Science
Srinivas University, Mangaluru - 575001

DECEMBER 2023

DECLARATION

I, **Ms. P. Sangeetha Prabhu** bearing **Reg. No: 19SUPHDF38**, Research Scholar in Institute of Computer Science & Information Science, Srinivas University, Mangaluru is herewith submitting my Ph.D. thesis report of the research work carried out towards the research title “**A Novel Deep Learning based Cyber Attack Detection System with Bait based Approach for Mitigation**”.

I declare that the research work has been carried out independently under the supervision of Dr. Nethravathi P. S., Professor, Institute of Computer Science & Information Science, Srinivas University, Mangaluru, and is fully a novel implemented, idea justified, results & authenticated through standard publications.

The work reported herein is original and does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on the earlier occasion or to any other scholar. I declare that the thesis and publication are my own work, except where specifically acknowledged, and has not been copied from other sources or been previously submitted for award or assessment.

Signature of the Candidate



(Sangeetha Prabhu)

Research Scholar

Place: Mangaluru

Date: 12/12/2023



SRINIVAS UNIVERSITY

(PRIVATE UNIVERSITY ESTABLISHED UNDER KARNATAKA STATE ACT NO. 42 OF 2013)

Srinivas Nagar, Mangaluru - 574 146, Karnataka State, INDIA. Phone: 0824-2477456

Web: www.srinivasuniversity.edu.in, Email: info@srinivasuniversity.edu.in

CERTIFICATE

This is to certify that the thesis entitled “**A Novel Deep Learning based Cyber Attack Detection System with Bait based Approach for Mitigation**” submitted to Srinivas University for the award of the degree of Doctor of Philosophy in Computer Science is based on the original work done by **Ms. Sangeetha Prabhu**, in the Institute of Computer Science and Information Science, Srinivas University, Mangaluru, under our guidance and supervision during the period August 2019 to December 2023 and that the thesis has not previously formed the basis for the award of any Degree, Diploma, Fellowship or any other similar title.

Signature

(Dr. Nethravathi P. S.)

Professor

ICIS, Srinivas University

Mangaluru-575001

Place: Mangaluru

Date: 12/12/2023

ACKNOWLEDGEMENT

Foremost, I would like to express my sincere gratitude to my advisor Dr. Nethravathi P. S. Professor, Institute of Computer Science and Information Sciences, Srinivas University, Mangaluru, for the continuous support of my Ph.D. study and research, for her patience, motivation, enthusiasm, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis.

I shall place on record my deep sense of gratitude to my guide and supervisor Dr. P. S. Aithal, Vice Chancellor, Srinivas University, Mangaluru, whose inspiration, encouragement and immense help made this work possible.

I thank our honorable Chancellor and Pro Chancellor of Srinivas University, Mangaluru for their encouragement in successful completion of my research work.

I would like to extend my acknowledgement to Dr. Subrahmanya Bhat and Dr. Krishna Prasad K for their timely support throughout my research work.

I am indebted to my parents, my sisters, my brother-in-law's and my beloved husband for given me constant encouragement, motivation time to time and to go ahead with my research work.

I take this opportunity to thank my friends and colleagues for their assistance during various stages of my research work. Lastly, I thank the almighty for reaching my goal without which the work would not have been completed in time.

MS. SANGEETHA PRABHU

TABLE OF CONTENTS

	Page No.
SYNOPSIS	I
LIST OF TABLES	Xliv
LIST OF FIGURES	Xlvii
LIST OF SYMBOLS AND ABBREVIATIONS	Xlix
CHAPTER - 1 INTRODUCTION	1-27
1.1 Preface	1
1.2 Overview of Cyber-Attack Detection	2
.2.1 When an Attack Deemed a Targeted Attack?	3
1.3 Types of Cyber Attacks	3
1.3.1 Cyber-Attack Handling Mechanisms	13
1.3.2 Cyber Security in Various Domains	14
1.4 Network Attack Detection and Prevention Techniques	16
1.4.1 Intrusion Detection System	16
1.4.2 Intrusion Prevention System	19
Intelligent Network Attack Mitigation Techniques to	
1.5 Detect Unknown Threats	22
1.6 Research Motivation	23
1.7 Research Problem	23
1.8 Research Queries for the Study	23
1.9 Objective of the Work	24
1.10 Thesis Contribution	24
1.11 Organization of the Thesis	25
CHAPTER - 2 REVIEW OF LITERATURE	28-52
2.1 Introduction	28
Overview of Systematic Literature Review	
2.2 Methodology	28
2.2.1 Study-Related Research Questions	29
2.3 Cyber Security Datasets	29

3.8	Proposed Cyber-Attack Detection and Mitigation System	70
3.9	Pre-Processing	72
3.10	Feature Extraction	72
3.11	Feature Selection by TWMA	73
3.11.1	Proposed TWMA	75
3.12	Classification by Means of BReLU-ResNet	81
3.12.1	Proposed BReLU-ResNet	84
3.13	Data Encryption Using ESHP-ECC	85
3.13.1	Secure Access ECC	85
3.13.2	Encrypted Secure Hash Probability	87
3.13.3	Proposed ESHP-ECC Algorithm	88
3.14	Shortest Pathway Calculation	91
3.15	Decryption through DSHP-ECC	91
3.16	Attack Mitigation System based on Bait Approach	91
3.17	Conclusion	93

CHAPTER - 4 RESULT AND DISCUSSION 94-131

4.1	Introduction	94
4.2	Programming Background	94
4.3	Database Description	95
4.4	Performance Metrics	96
4.5	Confusion Matrix of ANFIS algorithm	101
4.6	Confusion Matrix of NN algorithm	103
4.7	Confusion Matrix of CNN algorithm	105
4.8	Confusion Matrix of BReLU ResNet algorithm	107
4.9	Performance Analysis of the Proposed BReLU-ResNet	109
4.10	Performance Analysis of the Proposed SHP-ECC	118
4.11	Receiver Operating Characteristic Curve	124
4.12	Conclusion	126

CHAPTER - 5	ABCD ANALYSIS OF CYBER ATTACK DETECTION AND MITIGATION MODEL	132-173
5.1	Introduction	132
5.2	Objectives of the Study	133
5.3	Dimension of the ABCD Framework	133
5.4	Applications of the ABCD Framework	134
5.5	Advantages and Benefits of the ABCD Framework	135
5.6	Constraints and Disadvantages of the ABCD Framework	136
5.7	The Methodology of ABCD Framework	137
5.8	Determinant Issues and Key Attributes Involved in the ABCD Analysis	140
5.8.1	Advantages	140
5.8.2	Benefits	141
5.8.3	Constraints	142
5.8.4	Disadvantages	143
5.9	Framework of Systematic Review of its Usage	145
5.10	Review of Factors and Elemental ABCD Analysis with Determinant Issues	148
5.10.1	A review of Factors and Elemental ABCD Analysis and Determinant Issues	149
5.11	Key Attributes under Cyber Security in ABCD Analysis	149
5.12	ABCD Analysis of Cyber Security in Terms of Performance Metrics	156
5.12.1	ABCD Analysis of Cyber Security in Terms of Performance Metrics Sensitivity	157
5.12.2	ABCD Analysis of Cyber Security in Terms of Performance Metrics Specificity	158
5.12.3	ABCD Analysis of Cyber Security in Terms of Performance Metrics Precision	159
5.12.4	ABCD Analysis of Cyber Security in Terms of Performance Metrics Recall	161

5.12.5	ABCD Analysis of Cyber Security in Terms of Performance Metrics F-measure	162
5.12.6	ABCD Analysis of Cyber Security in Terms of Performance Metrics Accuracy	163
5.12.7	ABCD Analysis of Cyber Security in Terms of Performance Metrics False Positive Rate	165
5.12.8	ABCD Analysis of Cyber Security in Terms of Performance Metrics False Negative Rate	167
5.12.9	ABCD Analysis of Cyber Security in Terms of Performance Metrics Matthews Correlation Coefficient	168
5.12.10	ABCD Analysis of Cyber Security in Terms of Performance Metrics Encryption and Decryption Time	170
5.12.11	ABCD Analysis of Cyber Security in Terms of Performance Metrics Security Level	171
5.12	Conclusion	173
CHAPTER - 6	CONCLUSION	174
CHAPTER - 7	FUTURE SCOPE OF THE WORK	176
7.1	Future Work	176
	REFERENCES	177-195
	LIST OF JOURNAL PUBLICATIONS	196
	PLAGIARISM REPORT OF THE THESIS	

SYNOPSIS

Ph.D. Topic: A Novel Deep Learning Based Cyber Attack Detection System with Bait Based Approach for Mitigation

INTRODUCTION:

Almost every industry, government along with financial institution has transformed their transactions into cyberinfrastructure owing to augmenting trust and utilization of the Internet. Thus, the cyber system is made vulnerable to cyber-attacks. A malicious effort by an individual or else organization for breaching another system's information system is termed a cyber-attack organization. The (1) business organization, (2) military, (3) government, with (4) other financial institutions like banking are focused by the cyber-attacks either to hack secured information or for a ransom.

The threat or crime related to a malicious event owing to a malware attack in cyber-space, which distraction and loss in business and money, is termed Cyber-risk. It frequently takes place in the form of security threats like spamming, hacking, and phishing. By stealing the information along with gaining admission to the remote objective, malware, which is malicious software, is developed to damage computer resources .exe, scripts, dlls, files, macros, et cetera are a few forms of malware that could function at the system's background. For 80% of cyber-attacks globally, present-day malware is responsible. By aiming at commercial enterprises, elevated valued persons, and government that is linked to the Internet, much malware is propagated via the internet. For stealing data from infected targets, most cybercriminals take advantage of internet-centric services. Internet-centric attacks on government and corporate have increased by 47% as per the Bureau of Information Resource Management and Federal Information Security (FIS). On the federal network, FIS has records of 4500 malicious samples, 4.5 million spam emails, together with over a billion spams.

Owing to the malware variants' easy accessibility on the internet like Malware as a Service (darknet), Ransomware as a service, along with Hacker as a service (Hire a Hacker), there is an augmentation in the internet. In open source operating systems like BackTrack, Kali Linux, Parrot, etc., Built-in exploit kits are present. From the prevailing samples, over 2.5 billion fresh variants are engendered as per the statistical report by Virus where such variants aim just the Windows-centric machines. In cyber-space, hackers cleverly compromise the systems along with exploit the

user's confidential information namely credit card details; hence, heavy financial loss is caused. Cyber threat analysis is a significant aspect of threat hunting. Hunting maturity relays on data collection's ability along with how this data is evaluated. Data, which can be historical or live, is the most valuable source, which could be wielded for detecting a cyber threat. When weighed against traditional attacks, Modern-day cyber-attacks like Targeted Cyber Attacks (TCAs), Advanced Persistent Threats (APTs), etc., are hugely developed.

The cyber-attacks and wireless communication technologies are faced by several private companies along with government organizations globally. The globe is hugely reliant on electronic technology; in addition, it was a challenging problem to protect from cyber-attacks. In the Cyber Security (CS) community, the enhancement of more innovative and effective cyber detection mechanisms is considered an urgent requirement. By deploying a new Classification and Encryption methodology, a fresh system was proposed for attack node mitigation for attaining the aims. For preparation and testing, the UNSW-NB15 dataset is achieved along with classified initially. Within the preparation time frame, the information pre-handled together with incorporated is eliminated. For recognizing the associated highlights, the TWM is deployed. The input into went after along with non-went behind groups are sorted by the BRELU-RESNET. In the security log record, the compromised information is saved. By employing the ESHP-ECC, the typical data is encrypted. By employing the Euclidean Distance (ED), the shortest path distance is calculated. The data is present lately. The information is decrypted by deploying the DSHP-ECC. It is considered the sought-after data if the information is present in the log document in testing along with is secured from the transmission. The process of digital assault recognition starts if it is absent. The study is grounded on the UNSW-NB 15 dataset. For awareness, particularity, exactness, Precision, review, F-proportion, False Positive Rate, False Negative Rate, and Matthew's connection coefficient, the proposed system attains 98.34, 77.54, 96.6, 97.96, 98.34, 98.15, 22.46, 1.66 77.38 respectively. An extreme Security Level (SL) of 93.75% was attained by the proposed technique

When is an attack considered to be a targeted attack?

When the attack fulfils the key criteria, it could be regarded as a targeted cyber-attack. A particular organization or an individual is focused on by the attacker along with setting up the targeted attack; it has to spend some time, effort, together with resources. Stealing the information by infiltrating the system along with doing the data exfiltration via transforming communication that is, the hidden communication, which shields the data being shared as well as the connection betwixt the

sender along with receiver is the attacker's target launching a TCA. The attack is persistent; in addition, by utilizing automated and highly sophisticated malware, it was attained.

Research Motivation:

For organizations, cyber risk is a major concern. Criminals, amateur hackers, government actors, hackers, and other adversaries are included in the cyber system. Recently, media attention to CS issues has grown dramatically. The drawback is that most urbanized network attack detection methodologies rely on pre-defined signature-centric attacks. Since the attackers detected novel ways to exploit NS, the attackers' database has to be updated constantly. The predictive accuracy of detecting along with classifying network attacks is improved with the evolution of intelligent-centric methodologies like ML and DL. Hence, intelligent-based was wielded in NS, which is a thriving field for research.

Research Problem:

For protecting the network and data, cyber-attack along with threat intelligence work together. For understanding a cyber-attack in an organization's network and handling this cyber-attack efficiently, it is necessary to utilize suitable cyber-attack methodologies. By installing along with running anti-virus software that could consume huge computer memory as well as hard disk space, slowing down the computer, anti-virus software draws down the PC or network. For securing a network from being attacked, cyber threat intelligence can work as a preventive measure. Since that provides an enhanced understanding of the attack's nature that could be valuable knowledge for improving cyber threat intelligence, both methodologies must work together for securing the cyber-attack.

LITERATURE REVIEW:

Preventing cyber security attacks beyond a set of fundamental functional needs and knowledge about risks, threats or vulnerabilities requires analyzing cyber security data and building the right tools to process them successfully. Several machine learning techniques, which include but are not limited to feature reduction, regression analysis, unsupervised learning, finding associations or neural network-focused deep learning techniques can be used to effectively extract the insights or patterns of security incidents. This is briefly discussed in the "Machine learning techniques in cyber security" section. These learning techniques can detect anomalies or malicious conduct and data-driven patterns of related security issues and make intelligent judgments to avert cyber-assaults. Machine learning is a partial but significant departure from traditional well-known security solutions, including user authentication and access control, firewalls, and cryptography

systems, which may or may not be effective in meeting today's cyber business need. The critical difficulty is that domain experts and security analysts fix these manually in situations where ad hoc data management is required. However, as a growing number of cyber security incidents in various formats are emerging over time, traditional solutions have proven ineffective in managing these cyber-hazards. As a result, a slew of new, complex attacks emerges and spreads rapidly over the network. Thus, several academics apply diverse data analytic and knowledge extraction models to create cyber security models, which are covered in the section "Machine learning techniques in cyber security", based on the efficient identification of security insights and the most recent security trends that may be more relevant. According to research, addressing the cyber problem necessitates the development of more flexible and efficient security systems that can adapt to attacks and update security policies to eradicate them on a timely basis intelligently. To do this, a huge amount of relevant cyber security data collected from different sources, such as network and system sources, must be analyzed. Moreover, these techniques should be implemented in a way that increases automation, with minimal to no human intervention. An exhaustive literature survey is carried out mainly on cyber-attack detection and classification algorithms are explained in the below sections.

Research Queries for Study:

The following research questions were derived from the goals of the literature review and were concerned in responding to the following research problems:

- Q1: What are the various tactics for detecting and mitigating cyber-attacks?
- Q2: What are the most up-to-date ways for imposing a model for detecting and mitigating cyber-attacks?
- Q3: What are the research gaps in cyber-attack detection and mitigation strategies?

Overview of Systematic Literature Review Methodology:

The review of literature is an important procedure that offers a strong foundation for the growth of knowledge. It makes it easier to look at areas where more research is needed. The goal of this project is to undertake a comprehensive review of the literature to provide current research solutions for the development of a cyber-assault detection and mitigation device. The process for conducting a literature review to address the study's objectives is discussed in the subsections that follow. In the following subsections, the literature assessment framework outlines the questions for studies to consider, the technique for discovering relevant studies, the selection of studies to

include in the literature overview, the evaluation of reviewed articles, and the synthesis of study findings.

Cyber Security:

Cyber security means maintaining the Integrity, Confidentiality, and Availability (ICA) of computing benefits belonging to an organization or connecting to another organization's network.

- **Saravanan A et al. (2019)** explained cyber security and the fifth-generation cyber-attacks. Ensuring cyber security was an extremely complex task as it required domain knowledge about the attacks and the capability of analyzing the possibility of threats. The results showed that there were more than 25 % of attacks leveraged a new vulnerability. Unfortunately, most organizations had not evolved and were still using second or third-generation security even after the evolution of the fifth generation. So, the awareness among the organizations along with the security solutions must be increased.
- **Victoria Wang et al. (2020)** described the cyber security breaches, practices, and capability of internet banking in Nigeria. An online survey was conducted with 100 experienced professionals working in both the Nigerian banking and banking security service sectors. Data indicated that all 80 participants agreed or strongly agreed that subscribing to transaction alerts on the activities on accounts and not sharing personal account details with anyone were effective preventative measures. Nigerian banks were facing many difficulties in managing appropriate responses to cyber security threats when occurred.
- **Shaikha Hasan et al. (2021)** evaluated the cyber security readiness of organizations and its influence on performance. Organizations faced the challenge of enhancing their cyber security to prevent and combat cyber-attacks, but discussion of factors impacting the cyber security awareness/readiness of organizations from a holistic perspective was lacking. The results showed that cyber security readiness was found to positively impact organizational security performance which in turn positively affected financial and non-financial performance. The negative impact of government support on cyber security readiness found couldn't be generalized.

Cyber Security Challenges:

Cyber security is the main component of the country's overall national security and economic security strategies. With the increase in cyber-attacks, every organization needs a secure analyst where the system could be more secure. These security analysts face many challenges related to

cyber security such as securing confidential data of government organizations and securing the private organization servers etc. In the world of information technology, data security plays a significant role. Data security has become one of today's main challenges. Block chain technology has a proven track record when it comes to the enhancement of cyber security which is why it is now being used at the biggest tech companies in the world, ranging from Google. Following are some of the important cyber security challenges.

- Ransomware evolution
 - Block chain revolution
 - IoT threats
 - AI expansion
 - Server fewer apps vulnerability
- **Alex R. Mathew et al. (2019)** explained cyber security through block chain technology. Block chain technology had seen adoption in many industries and most predominantly in finance through the use of crypto currencies. The results showed that the block chain could potentially seal challenging security loopholes that were beyond the scope of conventional security tools. Since only the two parties in the communication would be able to read and manipulate the data, any stolen data would be unusable and third parties would also not be able to modify it.
 - **Lee et al. (2020)** described the Internet of Things (IoT) cyber security and IoT cyber risk management. The purpose of IoT cyber security was to reduce cyber security risk for organizations and users through the protection of IoT assets and privacy. The results showed that using the LP model, Option 3 generated a lower total cost than Option 2, even with a smaller investment cost. This illustration showed the effectiveness of the LP model in complicated IoT cyber resource allocation decisions. However, it found that 26% of the organizations did not use security protection technologies.

Review of Machine Learning Techniques in Cyber-Security:

Data security combines data from various sources and looks for correlations within the data. A security analysis tool may use different methods for analyzing the data. These include traditional rules-based methods as well as statistical analysis and machine learning. A machine learning security model for detecting anomalies is effective in terms of prediction accuracy as well as reducing the feature dimensions based on the decision tree classification approach with feature selection. There were six ML models considered for the review such as Random Forest (RF),

Support Vector Machine (SVM), Naïve Bayes (NB), Decision Tree (DT), Artificial Neural Network (ANN), and Deep Belief Network (DBN).

- **Defu et al (2019)** presented a machine learning-based attack detection model for power systems that were trained using data and logs obtained by phasor measurement units (PMUs). The findings demonstrate that the data processing method could increase the model's precision, and the AWW model could efficiently identify 37 different types of power grid behaviors. The feature development engineering was completed, and the data was then sent to various machine learning models, with the random forest being selected as AdaBoost's simple classifier. Finally, various comparison criteria were used to equate the proposed model to other ones. The experimental findings show that this model can reach a 93.91 percent accuracy rate and a 93.6 percent identification rate, which is better than eight recently established techniques.
- **Ban Mohammed Khammas (2020)** have proposed a novel method based on static analysis to detect ransomware. The significant characteristic of the proposed method is dispensing of the disassembling process by direct extraction of features from raw byte with the use of frequent pattern mining, which remarkably increases the detection speed. The Gain Ratio technique was used for feature selection, which exhibited that 1000 features were the optimal number for the detection process. The current study involved using a random forest classifier with a comprehensive analysis of the effect of both tree and seed numbers on ransomware detection. The results showed that tree numbers of 100 with seed number of 1 achieved the best results in terms of time-consuming and accuracy. The experimental evaluation revealed that the proposed method could achieve high accuracy of 97.74% for the detection of ransomware.
- **Yasir Ali Farrukh et al (2021)** proposed a two-layer hierarchical machine learning model having an accuracy of 95.44 % to improve the detection of cyberattacks. The first layer of the model is used to distinguish between the two modes of operation – normal state or cyberattack. The second layer is used to classify the state into different types of cyberattacks. The layered approach provides an opportunity for the model to focus its training on the targeted task of the layer, resulting in improvement in model accuracy.
- **Sumathy S et al (2021)** presented a Support Vector Machine (SVM) based PHY-layer authentication algorithm to detect the possible security attacks in 5G wireless communication at the physical layer. It is utilized in increasing the rate of authentication

with test features. The detection rate is improved further with test statistic features. The model is implemented on multiple-input multiple-output (MIMO) channel. The simulation results show that the proposed method yields a high detection rate on all attacks.

- **Iqbal H Sarker et al (2021)** presented “Cyber Learning”, a machine learning-based cybersecurity modeling with correlated-feature selection, and a comprehensive empirical analysis of the effectiveness of various machine learning-based security models. In our Cyber Learning modelling, they take into account a binary classification model for detecting anomalies, and a multi-class classification model for various types of cyber-attacks. To build the security model, we first employ the popular ten machine learning classification techniques, such as naive Bayes, Logistic regression, Stochastic gradient descent, K-nearest neighbors, Support vector machine, Decision Tree, Random Forest, Adaptive Boosting, extreme Gradient Boosting, as well as Linear discriminant analysis. Then, they presented the artificial neural network-based security model considering multiple hidden layers. The effectiveness of these learning-based security models is examined by conducting a range of experiments utilizing the two most popular security datasets, UNSW-NB15 and NSL-KDD. They aimed to serve as a reference point for data-driven security modelling through our experimental analysis and findings in the context of cybersecurity.
- **Jatinder Manhas and Shallu Kotwal (2021)** provided different techniques of machine learning namely K-nearest neighbor, multilayer perceptron, decision tree, Naïve Bayes, and support vector machine have been evaluated for implementation of IDS to classify network connections as normal or malicious. Four measures, i.e., accuracy, sensitivity, precision, and F-score, have been taken to assess the ability of machine learning techniques under study

In table 2.1. Experimental results have shown that the decision tree is the best classifier for IDS.

Table 2.1 Performance Comparison of ML Models Applied in Cyber Security

Author	Dataset	Detection	Accuracy	Disadvantages
Muhammad Shakil Pervez et al. (2014)	NSL-KDD	Hybrid based	82.37%	if there was a grouping of mining classifiers with SVM, accuracy would be more when compared to the present accuracy.

Preeti Mishra et al (2019)	KDD	Misuse-based	99.96%	It was difficult to detect low-frequency attacks just by examination of network features.
Donghwoon Kwon et al (2019)	NSL-KDD	Anomaly-Based	90.40%	The labeled (or trained) traffic dataset from real network traffic was not available to develop such ADNIDS.
Ayyaz-Ul-Haq Qureshi et al (2019)	NSL-KDD	Anomaly-Based	94.50%	NSL-KDD did not play a significant part in attack detection methods.
Ying Gao et al (2019)	KDD	Anomaly-Based	99.95%	It was not very effective in DDoS attack detection because attackers often change the types and methods of attacks and thence it was difficult to determine the pattern.
Mrutyunjaya Panda et al (2007)	DARPA	Misuse-based	99.90%	Misuse detection had a low false-positive rate, but cannot detect novel attacks.
W. A Awad et al (2011)	Spam base	Email spam	96.90%	Identification of legitimate messages was not as high as that of the implemented classifier.
Ramani Sagar et al. (2020)	Twitter	Spam tweets	98.88%	The scope of the security applications was broad which couldn't be limited to a few applications in the recent technological advancement.
Karthika Renuka D (2015)	Spam base	Email spam	84.00%	The rank of the feature was determined by a metric and also it eliminates all features that do not achieve an adequate score by means of feature ranking methods.
Vivek Nandan Tiwari et al	KDD CUP99	Anomaly-Based	-	The analysis was a tedious one and network administrators do not have

(2016)				the resources to analyze the data for security policy violations.
Vinaya kumar R et al (2019)	NSL-KDD	Hybrid-Based	75.30%	The applied system did not give detailed information on the structure and characteristics of the malware.
Anna L Buczak et al (2016)	DARPA	Anomaly-Based	80.00%	The major difficulty of the anomaly detection lies in discovering the boundaries between known and unknown categories.
Gary Stein et al (2005)	KDD	Hybrid based	99.85%	Generally, most existing systems had a false alarm rate because it was difficult to generate normal behavior profiles for protected systems.
Yara Rizk et al (2019)	Spam base	Email spam	89.2%	The network connections did not transmit data and they were not explicitly shown.
Sang Min Lee et al (2010)	Spam base	Email spam	95.43%	All features were not essential to classify emails because irrelevant features not only increase time and sources but also decrease classification rates.
Megha Rathi and Vikas Pareek et al (2013)	Spam base	Email spam	99.54%	It was quite difficult to achieve 100% accuracy but these two classifiers (Random Tree and Random Forest) were very nearby

Review of Deep Learning Techniques in Cyber-Security:

- **Wang et al (2018)** published a scenario-based two-stage sparse cyber-attack model for smart grids with complete and partial network details in 2018. The proven cyberattacks were successfully detected, and a security mechanism based on interval state estimation (ISE) was implemented in a novel way. The upper and lower limits of each state variable

were modelled as a dual optimization problem in this process to maximize the function variable's variance cycles. Furthermore, a popular deep learning algorithm, the stacked auto-encoder (SAE), was utilized to collect nonlinear and nonstationary features in electric load results. Such features were then used to increase predictive performance for electric loads, resulting in state variables with a narrow width. A parametric Gaussian distribution was used to represent the variance of forecasting errors. Comprehensive studies on numerous IEEE benchmarks have been used to show the validity of the current cyber-attack models and security mechanisms.

- In 2019, **Fan Zhang et al (2019)** created a CDS centered upon the notion of defense-in-depth that used the network traffic data, host system data, and also measured process parameters. Multiple-layer defense was offered by the AD system that decreased the defenders' valuable time before unrecoverable consequences occurred in the physical system. Firewalls, data diodes, along with gateways were encompassed by the 1st defense layer, which was the traditional intrusion prevention layer. Data-driven models were encompassed by the 2nd defense layer for cyber-AD centered on network traffic along with system data. It also comprised the classification model denoted by M1 and big data analytics models signified by M2. Early identification of attackers was offered by M1 and M2 when behavior deviation as of normal operation was produced by the attacks. The processed data was monitored by the last defense line if malicious activities couldn't be recognized by the secondary layer. The empirical models (indicated by M3) were utilized by the last defense line that considerably recognized the abnormal operations owing to cyber-attack. The result revealed that impactful cyber-attacks could be identified by the approach before considerable consequences occurred. But, for the advanced cyber-attacks, the scheme was ineffective.
- **Abdulrahman Al-Abassi et al (2020)** introduced a Deep Learning (DL) model that created balanced representations of the imbalanced datasets. An ensemble DL AD model that has particularly modeled for an ICS environment accepted the representations as input. Several unsupervised SAEs were contained by the DL model that learned new representations as of imbalanced datasets. Numerous Auto Encoders (AEs) were utilized by the SAE AD model that extracted new representations as of the unlabeled data; thus, disparate patterns were attained. Next, using a super vector, new representations as of each SAE were given to a DNN. Then, it was concatenated by using a fusion activation vector.

Lastly, the attacks were detected as of the newly merged representations by the DT which was employed as a binary classifier. The results exhibited that recent existent models were outperformed by the method. However, the drawback of poor backup capability was possessed by the scheme.

- **Moshe Kravchik et al. (2022)** created a technique for the recognition of anomalies and cyber-attacks in physical-level ICS data using 1 Dimensional Convolution Neural Networks (CNNs) that shallowed under complete AE, variational AE, and PCA. Besides, using the Kolmogorov-Smirnov test, a feature selection method was performed. The time-domain signals were converted into frequency representation using short-time Fourier transform and energy binning. The system was modelled in time along with frequency domains. The technique was assessed on '3' popular public datasets. The method was robust toward such evasion attacks as revealed by the results. The attacker was compelled to forfeit the desired physical impact on the system for evading detection. Nevertheless, the drawback of high energy consumption was possessed by the scheme.
- **Nevrus Kaja et al (2019)** modelled 2-stage intelligent IDS that were recognized and protected from such malicious attacks. The 2-stage architecture was encompassed by the approach centered on ML algorithms. The 2-stage ML approach's usage in the design of IDS after a 4-step effective data pre-processing was the novelty of the work. In the 1st stage, K-Means was utilized by the IDS that identified the attacks. Supervised learning was utilized in the 2nd stage that categorized such attacks and removed the number of false positives. Computationally, effective IDS were produced by applying the approach that was capable of detection and also the classification of attacks with higher accuracy. Also, the number of false positives was reduced. When contrasted to the existent state-of-the-art, the IDS's performance was superior. But, low detection rates along with higher False-Positive Rates (FPR) were possessed by the scheme.
- **Kaiyuan Jiang et al (2020)** presented a Network Intrusion Detection (ID) algorithm that merged hybrid sampling along with a Deep Hierarchical Network (DHN). Initially, the One-Side Selection (OSS) was utilized that decreased the noise samples in the common category. Next, the minority samples were augmented by utilizing the Synthetic Minority Over-sampling Technique. In that manner, a balanced dataset was determined. Due to this, the minority samples' features were fully learned by the model, and also the model's training time was significantly decreased. Secondly, to extract spatial features, a CNN was

utilized. For extracting temporal features, Bi-directional long short-term memory (Bi-LSTM) was employed, which created a DHN model. The experiments upon the NSL-KDD along with UNSW-NB15 datasets verified the Network ID algorithm. The model with excellent classification performance was attained. But, the disadvantage of high packet loss was possessed by the scheme and it was also ineffective in handling network overhead.

However, the drawback of higher energy consumption was possessed by the scheme in table 2.2.

Table 2.2 Various Deep Learning Models in Cyber-Attack Detection and Mitigation

Author	Adopted Methods	Features	Challenges
Zhe et al (2020)	RNN Model	<ul style="list-style-type: none"> • Small deviation • Reliable correction • Maximum destabilizing effects 	The starting state reconstruction was not limited.
Georgios et al (2020)	ANN Classifier	<ul style="list-style-type: none"> • Improved classification accuracy • Low energy failure • Less packet dropped failure 	The classification findings will benefit from the addition/removal of features from the illustrative datasets.
Huaizhi Wanget al (2018)	SAE Model	<ul style="list-style-type: none"> • High detection accuracy • MAPE • Robustness 	The development of an algorithm to solve L0-norm minimization problem must be prioritized.
Defu et al (2019)	AWV Model	<ul style="list-style-type: none"> • Better classification effect • High accuracy • Improved precision • Maximum recall • Higher F1 score 	The amount of relevant data must be increased, and progress on a deep learning platform that is integrated with Big Data analysis must be undertaken.
Jesus Arturo Perez-Diaz et al. (2022)	SDN Model	<ul style="list-style-type: none"> • Maximum accuracy • False alarm rate 	The proposed model did not incorporate the more recent

		<ul style="list-style-type: none"> • High Precision • Better recall • Maximum f1 measure 	ML and deep learning strategies.
Karimipour et al (2019)	DBN Model	<ul style="list-style-type: none"> • Better accuracy • True positive rate • Less FPR 	The proposed scheme success rate does not depend on the attack scenarios.
Fanrong Wei et al (2020)	Deep RL Framework	<ul style="list-style-type: none"> • Minimize cyber-attack impacts • Low MSE • Improve the system stability. 	The training facts no longer included the statistics created in scenario 1 and state of affairs 2.
MuhammadIsmail et al (2020)	Hybrid C-RNN detector Model	<ul style="list-style-type: none"> • Highest detection rate • Lowest false alarm 	The resilience of the following detector was put to the test in opposition to fresh cyber-attack that were not existent at the time of detector's training.

Research Gap:

The internet has evolved into a key infrastructure for both businesses and individual users, and its security has become a major concern. Protection is also a significant component in inspiring the purchaser confidence required to achieve commercial success for the new technologies that are emerging in today's connected world. Regression may be used to solve fraud detection in cybersecurity. It determines fraudulent transactions once a model is discovered from the historical transaction database, mostly based on observable attributes of recent transactions. System analysis methodologies are commonly used to solve a variety of cybersecurity issues. Advances in the realm of device understanding and deep mastery have the potential to provide viable answers to cybersecurity challenges. However, understand which set of rules is appropriate for particular usefulness. To keep the solution resistant to malware attacks and achieve high detection rates, multi-layered processes are required. When it comes to resolving cybersecurity difficulties, the choice of a selected version is crucial. Machine learning methods entail evaluating online data sets

to solve the problem of malicious attack detection. This is accomplished by utilizing an iteratively naïve Bayesian classifier. Active learning, on the other hand, allows the problem to be solved using a limited set of specified data points, which are also very expensive to obtain. Intrusion detection systems must detect and feedback network traffic in real-time while reducing latency and improving detection efficiency. The accuracy and generalization of intrusion detection have much room for improvement. A good model can detect more types of attacks and improve the performance of the intrusion detection system. Incorrectly classified attack data will affect the establishment of intrusion detection models.

OBJECTIVES:

Owing to the developed digital technologies wielded by hackers, cyber-attacks are augmenting quickly. For cyber-attacks and CS, several methodologies have been proposed; however, have high energy consumption, FPR rate, along with Backup capabilities. This research is done on CAD. The main aim of this effort is to develop efficient cyber-attack mitigation techniques, for detecting and mitigating attack node and their origin as early as possible at the receiver side through an effective novel encryption mechanism.

The problem was detected securely along with the objectives defined by the extensive literature survey on CAD with a BAIT-based approach for mitigation. For generating a proficient methodology, the subsequent notions should be considered.

- To design a deep ensemble methodology to detect the existence of attack; in addition, to alleviate it by employing the BAIT.
- To process the BAIT to mitigate the attackers as of the network.
- To develop a SHP-ECC to mitigate the attacker as of the network.
- To measure the proposed system's feasibility regarding particular performance metrics against other prevailing systems.

METHODOLOGY:

Electrical and mechanical devices, computers, along with manual operations supervised by humans are included in Industrial Control Systems (ICSs).

Proposed Cyber-Attack Detection and Mitigation System:

For people using the Internet and computers, Cyber-attacks and CS are the challenges. Even for people who aren't using them directly, the problems are increasing. Society hugely relies on networks and computers. With sensors and actuators, they haven't closed within cyberspace

anymore and have interaction with the real world. These systems are termed Cyber-Physical Systems (CPS), IoT/Everything (IoT/E), Industry 4.0, Industrial Internet, M2M, et cetera. Serious influence might be caused in real life by exploitation of any of these systems no matter what they are called; in addition, to mitigate those risks, suitable countermeasures must be taken. The concern for CS of ICS is increased by the evolving attacks against CPS. On firewalls, data diodes, along with other intrusion preventions that aren't apt for rising cyber threats as of motivated attackers, the present efforts of ICS CS are dependent. To detect the attacks with the aid of a DL system, the prevailing system presented an approach. The attack wasn't eradicated even though they are identified. A developed and powerful adversary should be offered as a solution to that issue.

For attack node mitigation, which is proffered employing a new Classification and Encryption methodology, a fresh framework was developed. For training along with testing data, the input data is split into 80% and 20%. Initially, the entire training data is pre-processed. From the input training dataset, features are extracted. To select the significant features, the feature is optimized by employing TWMA. By deploying the BReLU-ResNet, the feature is trained. Implementing the skip connection for offering input for the layer indiscriminately for merging the data flow for eradicating data loss and gradient vanishing problems is the goal of Residual neural networks (ResNet). Reducing noise is averaging this system; in addition, training accuracy and generalization are maintained by it. Achieving enhanced training accuracy and approximate level of traversal is the proficient way of enhancing maximum label data. The data is classified into attack and normal data. By employing BAIT, the Source IP Address is saved into a secure log file if the data is attack data. The data is ready for transmission if it is normal data. By utilizing the ESHP-ECC, the data is encrypted in Data Transmission. By employing ED, the shortest path distance is analyzed. By deploying the DSHP-ECC, the data is decrypted in the Destination. In the Security Log File (SLF), the testing data is checked in testing. The data is blocked, or attack detection is done if the data's source IP address is present already. In figure 1, the proposed framework's block diagram is depicted.

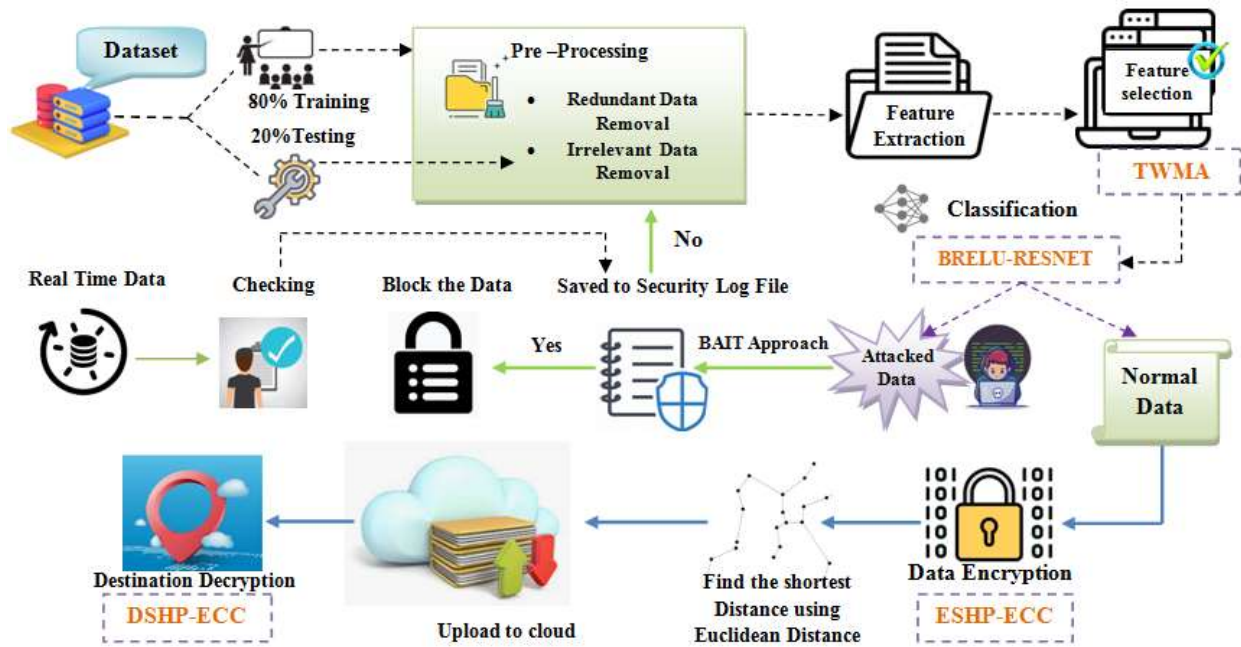


Figure 1: Structural Designs of the Proposed CAD and Mitigation System

Pre-Processing:

The input dataset is split into training as well as testing data to initiate the process of the CAD system. For converting the raw data into clean data, the data is pre-processed in the training phase. For enhancing the classification accuracy along with minimizing the training time, pre-processing is carried out. Redundant data removal and irrelevant information removal are deployed as pre-processing steps.

- Storing of same data in multiple locations is termed redundant data. A technique to remove duplicate data from the dataset is called redundant data removal. This reduces the computational complexity and results in better generalization for the classifier.
- The process of removing the data that are not required for the detection of cyber-attacks is termed irrelevant information removal. The processing time might be increased by the presence of such unrelated information and may result in an inaccurate attack detection rate. Hence, to improve the performance, the dissimilar data present in the input dataset is removed. Then, the features are extracted from the pre-processed data.

Feature Extraction:

It is the procedure of extracting the number of features by generating novel features as of the prevailing ones. Most information in the original feature sets is included in the novel features. The feature extraction/selection relies on a representative feature set as of the input patterns in training. To train the classifier, these features are deployed. For allocating the test patterns to one of the

pattern classes under selected features' consideration as of the training phase, the trained classifier is implemented in the classification phase.

- Common data reduction, that is, limiting storage needs along with maximizing system speed;
- The feature set reduction, that is, saving resources in the data collection or during usage's next round;
- Performance expansion, that is, gaining predictive precision;
- Data understanding, that is, gaining knowledge about the process engendered by the data or simply visualizing the data's feature set as of input patterns.

From the pre-processed dataset, the features like (1) source IP address, (2) source port number, (3) destination IP address, (4) destination port number, (5) transaction protocol, (6) source bits per second, (7) destination bits per second, etc are extracted. The set of extracted features $x_{(i)}$ is equated as,

$$x_{(i)} = x_{(1)}, x_{(2)}, \dots, x_{(n)} \quad (3.6)$$

Here, the number of extracted features is depicted by n .

Feature Selection by TWMA:

The significant features are selected using the novel Taxicab Woodpecker Mating Optimization (WMA) (TWMA). By the mating behaviour of red-bellied woodpeckers, WMA, which is a nature-inspired optimization, is presented. Woodpeckers, which deploy an effectual strategy of communication called drumming for attracting the other gender to mate, are wonderful birds; in addition, there are 200 different species of them. In structural optimization, WMA applies to tedious issues. Attaining optimal values meant for the parameters as of every possible value for maximizing or minimizing its result is termed optimization. In various engineering systems, the WMA is deployed for resolving real-world issues.

Proposed TWMA:

The population is categorized into male and female in WMA. By pecking the trees' trunks termed drumming, the male communicates with females. The females are attracted by relying on the sound quality produced by the male. Thus, the male's sound intensity drum indicates its ability to attract more females. The female move toward the male birds; in addition, communication and flow of information betwixt them takes place by hearing the sound. The female will attract the male along

with a move toward it if the male's sound intensity is closer to the female. Nevertheless, slow or premature convergence due to the loss of diversity within the population is a disadvantage in WMA. To update the female woodpecker's position during movement, Taxicab geometry is used; thus, the woodpecker population falling into local optimum could be avoided and also eliminates the slow or premature convergence in figure 3.8. TWMA is the enhancement made in general WMA.

Step 1: Initially, the woodpecker population (extracted features) is initialized as,

$$x_{(i)} = x_{(1)}, x_{(2)}, \dots, x_{(n)} \quad (3.7)$$

Here, the woodpecker population is depicted by $x_{(i)}$ and the woodpeckers in the population are signified by n .

Step 2: The fitness of each woodpecker is calculated for detecting the best woodpecker after population initialization. The woodpecker population is separated into male and female groups. The male becomes the search agent and the one with the uppermost fitness is regarded as x^* (the global best solution). Regarding classification accuracy, the fitness is calculated. The fitness evaluation $f(x_{(i)})$ is,

$$f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)}) \quad (3.8)$$

Step 3: By employing the below equation, the woodpecker's sound intensity is estimated.

$$\delta = \frac{2\pi^2 \gamma^2 A^2 DS}{\Psi} \quad (3.9)$$

Where, the sound intensity is signified by δ , the sound frequency is depicted by γ , the sound amplitude is mentioned by A , the density of the medium by which sound is travelling is delineated by D , the sound speed is described by S , and the area of sound is expounded by Ψ .

Step 4: Grounded on the source's sound, the sound intensity of the woodpecker may change. A few sources may emit the sound in one direction. Consider a sphere in the region of a source with a radius t . Via the sphere's surface, the sound waves will pass. The sound intensity (δ) is equated as,

$$\delta = \frac{2\pi^2 \gamma^2 \chi DS}{\psi \cdot 4\pi t^2} \quad (3.10)$$

Where, the propagation rate of sound waves is signified by χ and the area of the sphere is depicted by $4\pi t^2$. Sound intensity depends on the distance betwixt source and object.

Step 5: The better sound quality received by the female woodpecker is signified by the shortest distance between the source and the object. For estimating the distance between the source and object, the Taxicab distance is deployed; thus, the problem of premature convergence is surpassed along with obtains the global best solution.

$$t = \sqrt{(x_m - y_f)} \quad (3.11)$$

Here, the sound source position (male woodpecker) is depicted by x_m and the listener position (female woodpecker) is mentioned by y_f .

Step 6: Regarding the male bird's sound intensity, the female updates its position. The position updating process ($y_{f,j}^{\tau+1}$) is equated as,

$$y_{f,j}^{\tau+1} = y_{f,j}^{\tau} + r * \frac{\alpha_{f,j}^{\tau} \langle \beta^{x^*} (y_{x^*}^{\tau} - y_{f,j}^{\tau}) + \beta_{m,i} (x_{m,i}^{\tau} - y_{f,j}^{\tau}) \rangle}{2} \quad (3.12)$$

Here, the female woodpecker population is depicted by $j = 1, 2, \dots, m$, the current position of j -th woodpecker in τ th iteration is signified by $y_{f,j}^{\tau}$, the position of the best woodpecker is delineated by $y_{x^*}^{\tau}$, the position of i -th male woodpecker is expounded by $x_{m,i}^{\tau}$, a random number uniformly distributed in the interval $[0, 1]$ is indicated by r , a self-tuned random factor of j -th woodpecker is mentioned by $\alpha_{f,j}^{\tau}$, the attractiveness of the female bird to the male bird is depicted by β^{x^*} and $\beta_{m,i}$.

Step 7: The self-tuning random factor $\alpha_{f,j}^{\tau}$ is estimated by using the below equation.

$$\alpha_{f,j}^{\tau} = r * \eta \quad (3.13)$$

$$\eta = ts \left(1 - \frac{\tau}{\tau^{\max}} \right) \quad (3.14)$$

Where, the tangent sigmoid function is depicted by ts , the current and the maximum number of iterations is modelled by τ, τ^{\max} , a random value in the interval -2η to 2η be delineated by α . The search agent deviates from the target, which leads to exploration if $|\alpha| > 1$, and the female bird joins with the male bird, which leads to exploitation if $|\alpha| < 1$.

Step 8: The attractiveness (β) of male and females woodpeckers is equated as,

$$\beta = (1 + \delta(i, j))^{-1} \quad (3.15)$$

Where, the sound intensity of i -th male woodpecker heard by the j -th female woodpecker is depicted by $\delta(i, j)$. It is also termed step size of the female woodpecker since it specifies the closeness of the female woodpecker towards the male, β lies in the interval 0 and 1, and the accurate movement of the female toward the male woodpecker is delineated by the lower β value.

Step 9: The male woodpecker population decreases at each cycle, and finally, only one woodpecker will remain. In the initial phase, a large male population increases the exploration. Thus, the exploitation and accuracy of the solution are maximized by the decreasing population.

The population size ($x_{m,i}$) in each iteration is equated as,

$$x_{m,i} = \left[\text{round} \left(\frac{n}{2} * \left(1 - \frac{\tau}{\tau^{\max}} \right) \right) + 1 \right] \quad (3.16)$$

Here, the total woodpecker population is depicted by n , and the current and maximum number of iterations is signified by τ, τ^{\max} .

Step 10: In the end, one woodpecker and the global best woodpecker x^* is encompassed in the decreased population of woodpeckers. Thus, equation (3.12) can be modified as,

$$y_{f,j}^{\tau+1} = y_{f,j}^{\tau} + r * \left(\alpha_{f,j}^{\tau} \cdot (y_{x^*}^{\tau} - y_{f,j}^{\tau}) \cdot \beta_{m,i} \right) \quad (3.17)$$

Step 11: There is a possibility of deviation in direction during the movement of the female woodpecker towards the male; in addition, by other woodpeckers or hunting birds, the female birds might be attacked. To protect itself from danger, the female bird may change their path. This random change in the pathway is termed Run Away. This random escaping movement of the woodpecker consists of two types of movements, which are based on the sound intensity of x^* male bird. The two types of movements (μ) are,

$$\mu = \begin{cases} R & \beta \geq \xi \\ P & \text{else} \end{cases} \quad (3.18)$$

Here, the runaway movement and x^* runaway movement are depicted by R, P .

$$\xi = 0.8 \cdot \frac{\sum_{j=1}^{m-1} \beta_{x^*}^j}{m-1} \quad (3.19)$$

Where, the threshold for the sound intensity of x^* is signified by ξ .

Step 12: The female's position obtained from the runway is equated as,

$$\tilde{y}_{f,j} = L - (L - U) * r \quad (3.20)$$

Where, the position of j -th woodpecker after the runaway is delineated by $\tilde{y}_{f,j}$, a random number in the uniform distribution $[0, 1]$ is indicated by r and the upper and lower bounds of variables are denoted by L, U .

Step 13: The x^* runaway movement is denoted further,

$$P = \phi * \left(1 - \frac{\tau}{\tau^{\max}} \right) \quad (3.21)$$

Here, the runaway coefficient is depicted by ϕ . The position of a female woodpecker from x^* runaway movement ($y_{f,j}^{x^*}$) is equated as,

$$y_{f,j}^{x^*} = y_{f,j}^{\tau} + P^{bit} \langle y_{x^*}^{\tau} - y_r \rangle \cdot B \quad (3.22)$$

$$P^{bit} = \begin{cases} 1 & r \leq P \\ 0 & else \end{cases} \quad (3.23)$$

Where, a random number in the uniform distribution $[0, 1]$ is depicted by r and a random number $[-1, 1]$ is signified by B . Until the stopping criterion is met by comparing the position of i -th woodpecker with the former position together with the position of the best woodpecker, the process continues. Next, the better position is replaced with the other position. In the end, the optimal solution is obtained, i.e., the selected best features ($X^{(k)}$) are equated as,

$$X^{(k)} = X^{(1)}, X^{(2)}, \dots, X^{(K)} \quad (3.24)$$

Here, the number of features selected for further classification is signified by K . In figure 2, the proposed TWMA's pseudo-code is depicted.

Pseudocode for Proposed TWMA

Input: Extracted Features $x_{(i)}$

Output: Selected features $(X^{(k)})$

Begin

Create the initial population of woodpeckers

Compute $f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)})$

Obtain x^* based on $f(x_{(i)})$

While (stopping condition is not satisfied) **do**

Partition $x_{(i)}$

For $1 \leq i \leq n$

Determine the sound intensity δ

Compute Taxicab distance

Choose $x_{m,i}$ (i -th male woodpecker)

Evaluate β^{x^*} and $\beta_{m,i}$

Analyze $\alpha_{f,j}^z = r * \eta$

Update woodpeckers' position $(y_{f,j}^{z+1})$

Calculate sound intensity threshold ξ

If $\beta^{x^*,i} > \xi$

Estimate $\tilde{y}_{f,j} = L - (L - U) * r$

Else

Find out x^* runaway movement $(y_{f,j}^{x^*})$

End if

Appraise the new position of $y_{f,j}$

Renew x^*

End for

$\tau = \tau + 1$

End while

Obtain global best solution $(X^{(k)})$

End

Figure 2: Pseudo-code of the Proposed FS Technique

Classification by Means of BReLU-ResNet:

ANN's individual structural design is CNN. The visual cortex's several features are deployed by CNN. Estimating the input images' class labels is a significant role in image classification. In the

sequence of convolutional (Conv), nonlinear, pooling, together with Fully Connected (FC) layers, the images are accepted; then, the result is generated. The CNN's initial layer is the Conv layer. Via the pixel value, an image is depicted as a matrix. Fewer matrixes are selected, which is termed a filter (neuron or core). Convolution is engendered by the filter where the input image is presented. Develop the values with actual pixel values; in addition, each multiplication is added. It goes additional right with 1 unit executing the same function since the filters have interpreted the image from the upper left corner. A matrix is attained behind passing the filter; nevertheless, when weighed against the input matrix, it is reduced. Detecting edges and colours are analogous. Several Conv networks differed by nonlinear and pooling layers are encompassed in the system. The initial layer's outcome will become the 2nd layer's input if the image exceeds 1 Conv layer; in addition, it takes place with every further Convlayer. Every convolution function is followed by the nonlinear layer. The activation function, which deploys nonlinear property, is included in it. Then, the pooling layer is implemented. By employing width and height, it has functioned; in addition, executes the sampling function. The image volume is eradicated due to the result. A definite image won't require the extra procedure if it is applied while some features are analyzed in the prevailing Conv function; in addition, it could be minimized to lesser definite pictures. In networks, the resultant data is achieved in the FC layer. An N-dimensional vector is offered by connecting an FC layer to the final stage in which the number of classes as of which the desired classes could be enhanced is signified by N.

The 1st single-channel Residual Networks (ResNets) were exhibited in 2015. It is now extensively accepted as one of the modern DL techniques. Easy network optimization along with higher accuracy was provided by that technique. For the ILSVRC competition, the network called ResNet was the baseline of submissions in which, for the task of ImageNet detection along with localization, it won the 1st prize. Initial operations like convolution and max-pooling are performed by every ResNet subsequent to stacked convolutions. It solved the vanishing gradient issue.

Instead of investigating the unreferenced changes, it learns the residual operations concerning input layers, which is the key factor of ResNet. The aspects of ResNet are high accuracy, better optimization, and computational efficiency. One of the key advantages is that by using knowledgeable low-level frame extractors as an alternative to initialize with random weight.

The ultra DNN's training is stimulated since the ResNet is productive along with develops accuracy. From CNN's depth, the ResNet is evolved, which caused degradation problems. While enhancing the depth and minimizing the accuracy, the accuracy is maximized; in addition, it is

regarded as a demerit. The error might be discarded that is deeper along with doesn't provide maximal training samples error while a shallow network suffers the accuracy of saturation along with includes congruent mapping layers. Conveying the prevailing outcome to the upcoming layer with the assistance of congruent mapping is the goal. To solve the degradation and gradient vanishing problem, the residual block is implemented by ResNet. Under the input inclusion and residual block's output, those blocks in ResNet perform the left-over ones.

Proposed BReLU-ResNet Algorithm:

For categorizing the attacked data from the on-attacked data, the selected features $(X^{(k)})$ are fed into the BReLU-ResNet. Since ResNet surpasses the degradation caused due to the rise in network depth, it is wielded for classification. Convolutional, batch normalization, max pooling, flattening, and activation layers are encompassed in the ResNet. Initially, the selected features are inputted to the ResNet, the input is convoluted with the 2*2 filter in the convolutional layer, and it produces the output with reduced feature dimension. The result achieved as of the convolutional layer is given to the batch normalization layer in which the network time is stabilized along with epochs minimized. In convolutional and batch normalization, there are '3' layers. The data is given to the max-pooling layer, which down samples the data. For categorizing the results, the FC layer includes the average pooling and softmax layer. Nevertheless, owing to the activation function's randomized nature, ResNet has an over-fitting issue. In the ResNet, Bernoulli's value is used in the Leaky Rectified Linear Unit activation function instead of a random value. This modification in baseline ResNet is called BReLU-ResNet. Let $(X^{(k)})$ be the input features and a filter (Γ) of size (a, b) is used in the convolution layer, which is equated as,

$$conv(X^{(k)} * \Gamma) = \sum_{k=1}^K (X^{(k)} - a, X^{(k)} - b) \cdot \Gamma(a, b) \tag{3.25}$$

- The significant part of neural networks is activation function. The BReLU activation function $(f(X^{(k)}))$ is equated as,

$$f(X^{(k)}) = \max(0, b(X^{(k)})) \tag{3.26}$$

Here, Bernoulli's distribution function is delineated by $b(X^{(k)})$.

$$b(X^{(k)}(p, o)) = p \cdot o + (1 - p)(1 - o) \tag{3.27}$$

Where, the probability and possible outcome of $(X^{(k)})$ is signified by p, o .

- In the BReLU-ResNet the network layers are capable of approximating any function asymptotically. The approximation of residual function $\partial X^{(k)}$ is,

$$\partial X^{(k)} = f(X^{(k)}) * X^{(k)} \quad (3.28)$$

Where, the target function is depicted by $f(X^{(k)})$.

$$f(X^{(k)}) = \partial X^{(k)} + X^{(k)} \quad (3.29)$$

The attacked data is separated from the normal data by the classifier's output; then, by employing the Bait, the attacked data is stored in the SLF. By deploying the Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC), the normal data is encrypted. To transfer data in the cloud effectively, the shortest path between every node is estimated.

Data Encryption Using Proposed ESHP-ECC Algorithm:

By employing the Hashed ECC, the data is securely accessed. In retrieving the info, security is significant. The secure access utilizing hashed ECC is delineated further.

Secure Access ECC Algorithm:

To deploy Elliptic Curve (EC) Cryptography (ECC) as the baseline for discrete logarithm-centric cryptosystems was presented by Victor Miller and Neal Koblitz 1985 at the University of Washington 1985. In several cryptographic contexts like integer factorization and primarily proving, elliptic curves were deployed already. The science of keeping information secure is termed cryptography in a nutshell; thus, for cloud computing security, it is a helpful tool. To transmit over the Internet to the rightful recipients, encryption and decryption of messages were encompassed. To encrypt and decrypt the transmitted data information, any cryptographic scheme's secrecy is significant usage. Even though a few organizations believe in having the algorithmic key a top secret via encryption, most cryptographic algorithms are openly accessible. In the elliptic curve, the ECC discrete points over a finite field are deployed as a cyclic group. By employing ECC, every kind of public cryptography-centric scheme could be implemented as analogous. When weighed against other cryptosystems, the popularity of ECC is owing to the determination, which is grounded on a harder mathematical issue. For the conventional public-key cryptosystem like RSA and DSA, it is an alternative in which the factorization or the discrete log issue could be resolved in sub-exponential time. When analogized to competitive systems like the RSA and DSA, the smaller parameters could be wielded in ECC.

With a smaller key size, the same SL is provided by ECC; thus, in limited environments such as mobile phones, sensor networking, and smart cards, enhanced performance is caused. While

considering RSA with a key size of 1024 bits, the ECC with a key size of 160 bits offers the same SL. Scalar multiplication is encompassed by the main agreement, signature generation, signing, together with verification; in addition, they are the elliptic curve's key operations. In the entire system's efficacy, scalar multiplication plays a significant role. In a few environments like limited devices, and central servers, rapid multiplication is significant in which a large number of key agreements, signature generations, along with verification take place. On the complex of the EC Discrete Logarithm Problem (ECDLP), the ECC's security strength depends. Point doubling and adding operations are encompassed in scalar multiplication, which was adopted by ECC that are computationally more effectual when weighed against RSA exponentiation. For understanding the ECC along with breaking the security key, the ECC's complexity puts the attacker in difficulty. ECC helps to develop equal security with less battery usage and computing power. The category of security mechanism, which creates a hash value, checksum value, or message-digest for specific data, is signified by the hash function. For increasing the security strength, hashing is integrated with ECC. A kind of mechanism, which is espoused in the public-key cryptography employment, is termed ECC. With the utilization of a prime number function, that methodology is grounded on a curve with specific base points. In figure 3, the functions are deployed as a maximal limit.

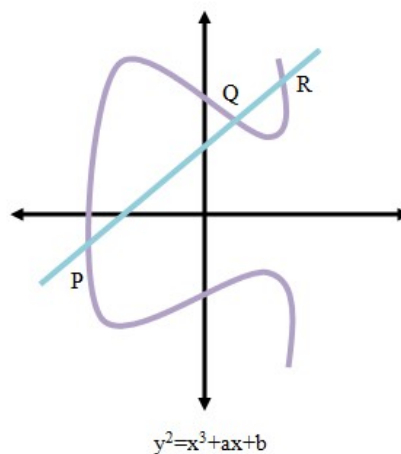


Fig 3: Elliptic Curve

By employing the hashed ECC system, the data is accessed securely. Hashed ECC, which is a public key encryption method, grounded on the EC theory could be deployed for generating faster, smaller, and more efficient cryptographic keys. Rather than the prevailing technique, keys are generated via the properties of the EC equation by hashed ECC as the product of very large prime numbers.

Encrypted Secure Hash Probability:

Secure Hash Algorithm (SHA) is the name of a series of hash algorithms; in 1993, the SHA-1 was presented [60]. A 160-bit hash value was generated by SHA-1. SHA-1 also has weak collision avoidance similar to MD5. In 2001 (<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>), SHA-2 was developed. SHA-224, SHA-256, SHA-384, along with SHA-512 are termed after the length of the MD each creates is encompassed in SHA-2.

From an arbitrary length string, a 160-bit hash value is generated by SHA-1. Huge applications namely SSH, SSL, S-MIME (Secure / Multipurpose Internet Mail Extensions), together with IPsec are deployed by it similar to MD5. It is computationally infeasible of detecting a message, which relates to a given MD or to detect '2' messages, which generate a similar message digest, which is the basis behind the security of SHA-1. Nevertheless, this principle is no longer valid. For replacing the present 160-bit version, more secure variations of SHA-1 are verified when there are no successful attacks on SHA-1. With the numbers reflecting the strength of the MD engendered on the application, SHA-256, SHA-384, together with SHA-512 are encompassed in it.

The superior version of the previous hash system termed SHA 0, SHA 1, SHA 256, as well as SHA 384 is this system. A function, which gathers the input data of any size along with generates the Message Digest (MD) of 512-bit size along with 1024-bit block length is termed the SHA-512. To form various 1024 bits, the message bits are enlarged with an extra system. This block is categorized into smaller parts of 1024 bits. With the generated hash code, the key block is incorporated with the initializing vector. With the previously created hash codes, further blocks are incorporated. Concerning the generated hash values allied with the closed frequent patterns, the hash tree is constructed. To index in a hash tree, hash values are utilized significantly. The closed frequent patterns indexed with a related hash value are depicted by every leaf node.

Hashing algorithms, which is also termed one-way encryption, deploy no key. For authenticating messages, digital signatures, and documents, hashing is employed. MD is referred to as a hash function that accepts a variable-length block of data as input and produces a fixed-length hash value. A function, which produces MD 512-bit size together with 1024-bit block length, is termed SHA 512 hash function. To accept input in the form of a message with any length or size, the cryptographic system operates with the SHA 512; in addition, MD, which has a fixed length of 512 bits, is generated. SHA- 512 works on a message in 1024-bit blocks along with generates a 512-bit MD. 2^{128} bits is the maximal message length acceptable.

Proposed ESHP-ECC Algorithm:

A public-key cryptosystem grounded on the EC hypothesis that is secure asymmetric encryption deployed for data security is termed the ECC. Via EC properties, public along with private keys are produced for every user. For encrypting and decrypting the data, those keys are employed. The keys are generated randomly in ECC. Hence, the main information might be hacked easily. Grounded on the engendered key value, the probability of ones and zeros are produced. By employing secured hashing, the key values are converted into a hash value in figure 3.4. The proffered system is termed the ESHP-ECC owing to the modifications in the general ECC. The ESHP-ECC's encryption process is detailed below,

- Initially, for key generation, the EC equation was used.

$$Y^2 = X^3 + aX + b \quad (3.30)$$

a, b Signifies the integers.

- Next, a random number (η) is generated from $[1, n-1]$ and the probability of ones and zeros of this random number is calculated as the private key. the public key (ρ) is equated as,

$$\rho = \eta * B \quad (3.31)$$

Where, the point on the EC is signified by B .

- Then, by using secure hashing, these public and private keys are converted into a hash value. A cryptographic hash function, which considers the keys as the input together with produces a 160-bit (20-byte) is termed SHA. The private and public keys are represented as η'' and ρ'' .
- Let, the message to be transmitted is depicted by M and it has the point Q on the EC. Randomly select σ from $[1, n-1]$. '2' cipher-texts $(C^{(1)}, C^{(2)})$ are calculated using the below equations.

$$C^{(1)} = \sigma * B \quad (3.32)$$

$$C^{(2)} = Q + \sigma * \rho \quad (3.33)$$

Here, the encrypted message, which is transmitted to the cloud server via the shortest path, is delineated by $(C^{(1)}, C^{(2)})$.

Input: Attack free message M
Output: Encrypted data $(C^{(1)}, C^{(2)})$

Begin
For each M
 Perform key generation
 Define the elliptic curve equation $Y^2 = X^3 + aX + b$
 For $1 \leq \eta \leq n-1$
 Generate (η)
 Compute the probability of ones and zeros of (η)
 Estimate the public and private keys $\rho = \eta * B$
 For each η, ρ
 Carry out SHA hashing
 Attain η'' and ρ''
 End for
 End for
 Execute data encryption
 Select randomly σ from $[1, n-1]$
 Calculate $C^{(1)} = \sigma * B$
 Attain the cipher text $C^{(2)} = Q + \sigma * \rho$
End for
Recognize the encrypted message $(C^{(1)}, C^{(2)})$
End

Figure 4: Pseudo-codes for Proposed ESHP-ECC Algorithm.

Shortest Pathway Calculation:

The number of sensor nodes available to transmit the encrypted message is signified by $(x_i = x_1, x_2, \dots, x_N)$. For efficient data transmission and for minimizing the computational time, the shortest path between each sensor node is identified. Thus, for calculating the distance, ED $E^{(d)}$ is wielded.

$$E^{(d)} = \left\| (x_i - x_j) \right\|^2 \tag{3.34}$$

Where, the j -th node is depicted by x_j . The shortest pathway obtained is used to transmit the encrypted message after distance computation. By employing DSHP-ECC, this encrypted message is decrypted at the receiver side.

Decryption through DSHP-ECC Algorithm:

The encrypted message is decrypted using the below equation,

$$Q = C^{(2)} - \eta * C^{(1)} \quad (3.35)$$

Here, the original message is depicted by Q .

Observations from the proposed model

Performance Analysis of the Proposed BReLU-ResNet Algorithm:

The proposed BReLU-ResNet is validated with prevailing Convolutional Neural Network, Artificial Neural Network, along with Adaptive Network-centric Fuzzy Inference System (ANFIS) regarding sensitivity, specificity, accuracy, precision, recall, F1 measure, False Positive Rate, False Negative Rate; Matthews Correlation Coefficient (MCC). The comparison is done with the current methods to state the efficiency.

Table 1: Performance Analysis of Proposed BReLU-ResNet based on Sensitivity, Specificity, and Accuracy

Techniques	Performance metrics (%)		
	Sensitivity	Specificity	Accuracy
Proposed BReLU-ResNet	98.34	77.54	96.6
CNN	97.81	63.62	94.58
ANN	95.78	58.84	93.23
ANFIS	91.17	44.42	90.61

In table 1, regarding sensitivity, specificity, together with accuracy, the proposed BReLU-ResNet's performance is analyzed with the current CNN, ANN, along with ANFIS. For sensitivity, specificity, and accuracy, the BReLU-ResNet achieved 98.34%, 77.54%, and 96.6%, while the prevailing system attained 94.92% for CNN, 55.62% for ANN, and 92.80% for ANFIS. Hence, a cyber-attack is exactly recognized by the BReLU-ResNet. In table 1, the network's confidentiality is depicted. To analogize with the BReLU-ResNet, the relevant research, which deploys ML for intrusion/attacks detection/classification, is chosen for enhancement along with extremely reasonable analysis. In figure 5, the classification accuracy, sensitivity, and specificity are

summarized for associated systems.

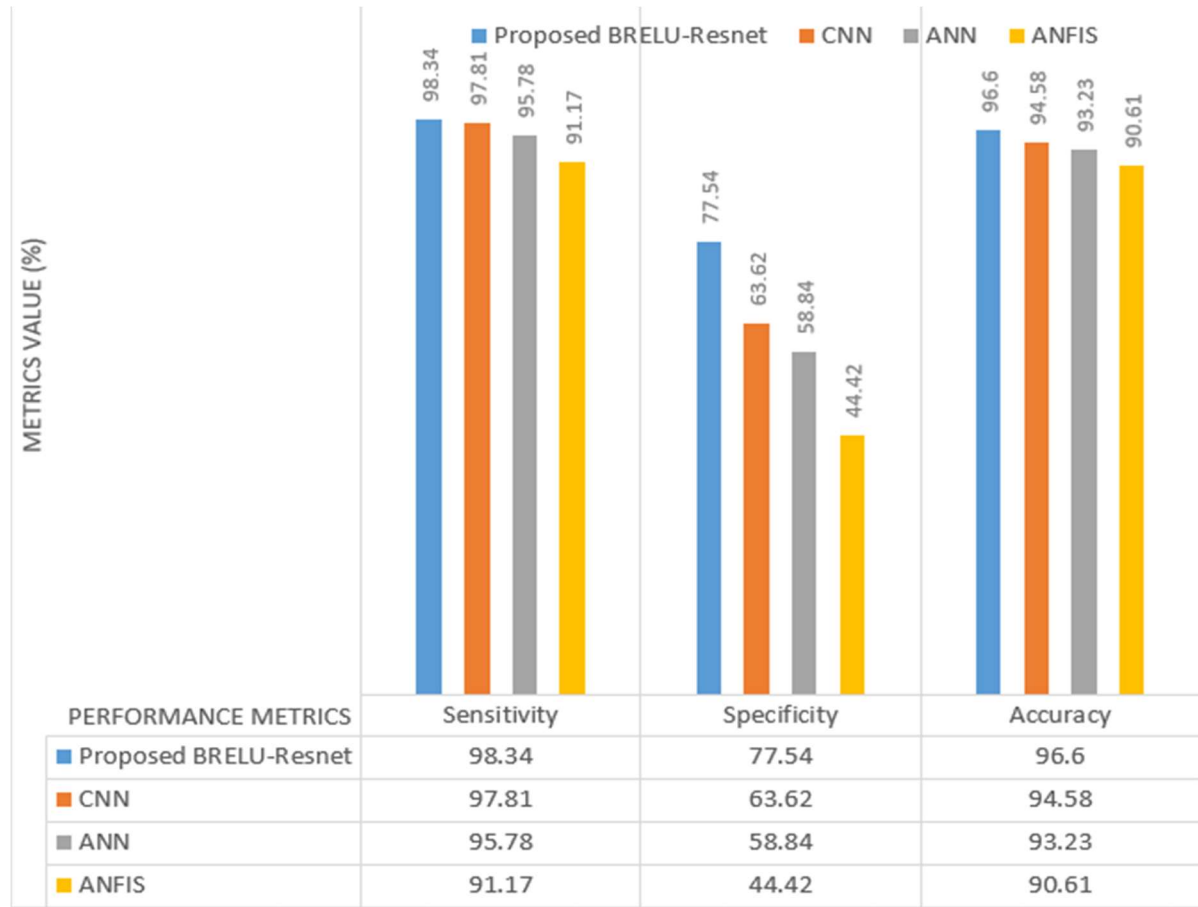


Figure 5: Comparative analysis of proposed BReLU-ResNet and other algorithms based on Sensitivity, Specificity, and Accuracy.

Table 2: Performance Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-measure.

Techniques	Performance metrics (%)		
	Precision	Recall	F-measure
Proposed BReLU-ResNet	97.96	98.34	98.15
CNN	96.26	97.81	97.03
ANN	96.9	95.78	96.34

ANFIS	92.49	97.17	94.77
--------------	-------	-------	-------

In table 2, regarding precision, recall, along with FM, the performance of BReLU-ResNet is evaluated with the prevailing CNN, ANN, and ANFIS. The model's significance is proved by the higher rate of precision, recall, and FM. For precision, recall, and FM, the BReLU-ResNet attained 97.96%, 98.34%, and 98.15%; whereas, the prevailing system achieved 95.21%, 96.92%, and 96.04% respectively. Thus, the BReLU-ResNet mitigated several complexities. In table 2, the CAD process's reliability is depicted.

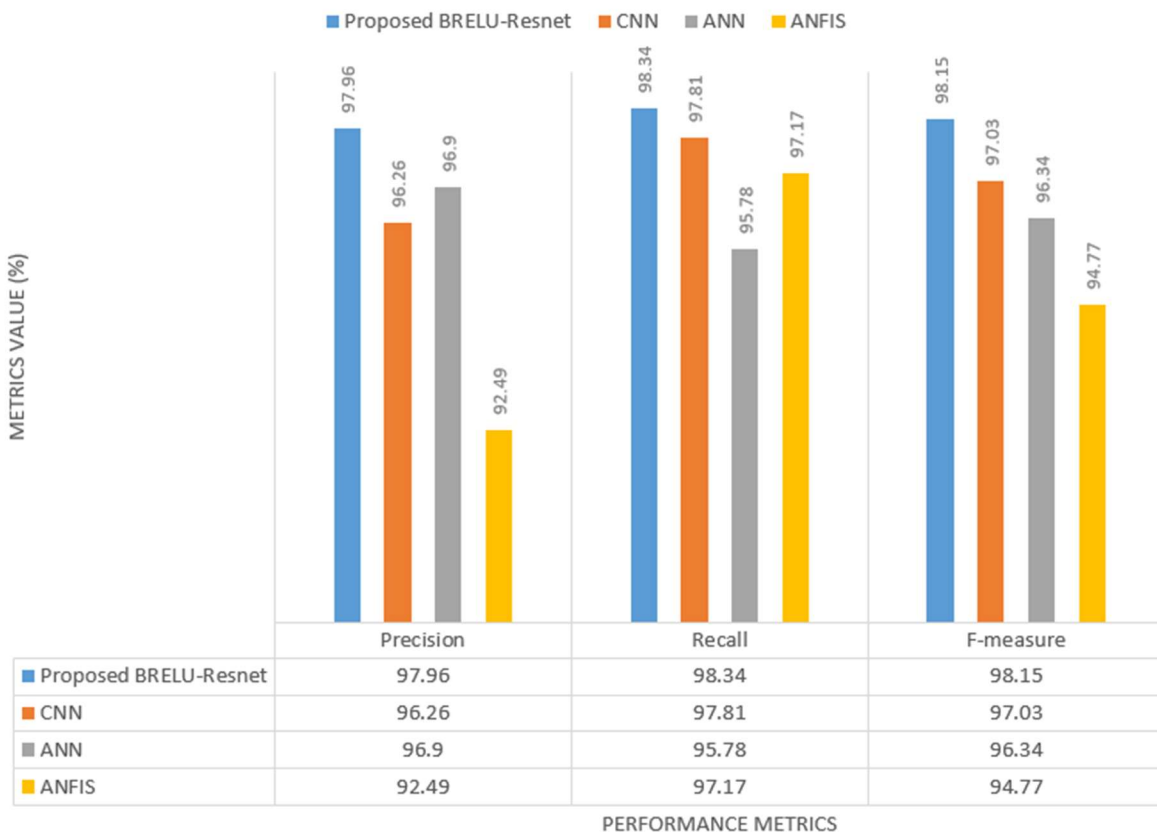


Figure 6: Comparative Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-Measure.

The FM values achieved by every technique are depicted in Figure 6, by attaining superior overall values, the DL exhibited enhanced performance when weighed against other learning techniques regarding FM. With elevated recall and precision, DL-centric detection could detect malicious attacks. There are some higher recall values along with lower precision values.

In figure 6, the proposed work's comparative analysis is depicted. The BReLU-ResNet attained

97.96%-98.34% for precision, and recall, along with FM; while the CNN, ANN, along with ANFIS acquired less percentage of 92.49%-97.81%. Thus, the BReLU-ResNet surpassed other top-notch methods along with offers more prominent results under disparate complex situations.

Table 3: Performance Analysis of Proposed BReLU-ResNet concerning False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.

Techniques	Performance metrics (%)		
	FPR	FNR	MCC
Proposed BReLU-ResNet	22.46	1.66	77.38
CNN	36.38	2.19	66.24
ANN	41.16	4.22	51.12
ANFIS	55.58	2.83	50.6

In table 3, regarding False Positive Rate, False Negative Rate, and MCC, the proposed BReLU-ResNet is analyzed with the prevalent techniques. By the lower value of FPR as well as FNR, the misclassification or misprediction error is discarded effectively. For FPR and FNR, the BReLU-ResNet attained 22.46% and 1.66%; while, the current techniques attained 44.37% and 3.08%. For MCC, the BReLU-ResNet achieved 77.38%; whereas, the prevailing one attained 55.98%. Thus, the BReLU-ResNet surpassed the current techniques; in addition, they are more dependable in table 3.

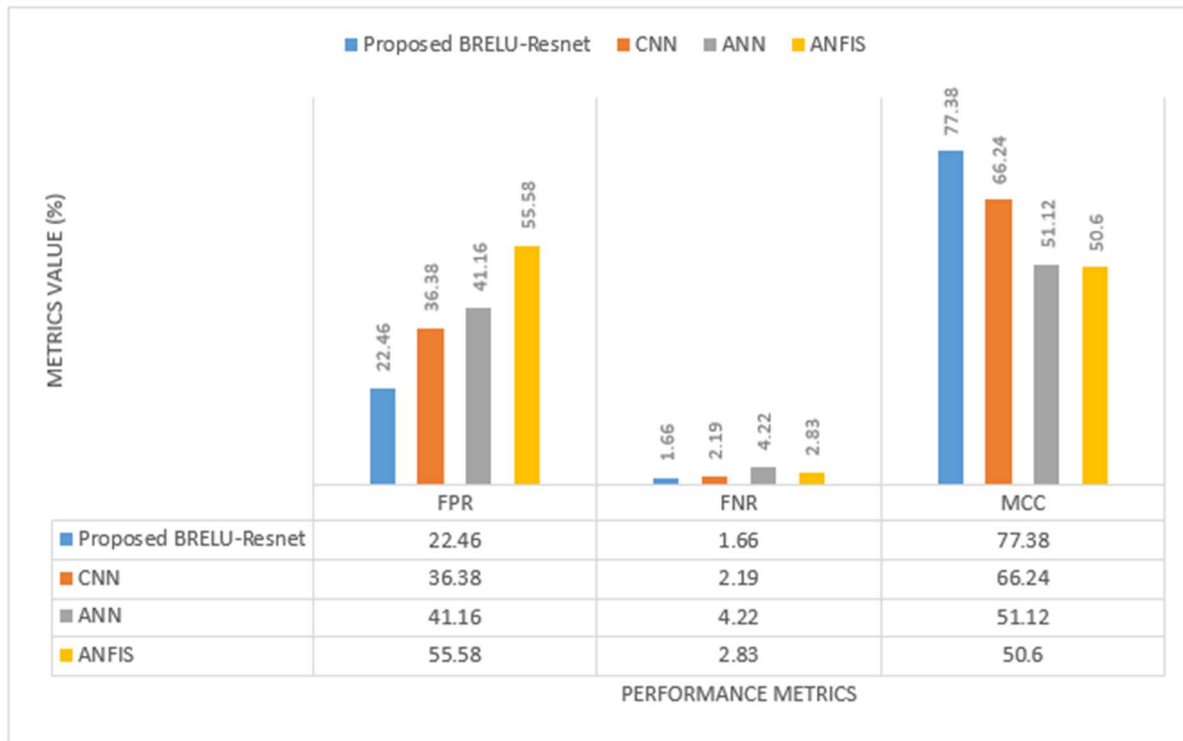


Figure 7: Comparative Analysis of Proposed BReLU-ResNet in Terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.

In figure 7, the Proposed BReLU-ResNet is analogized to the current works regarding FPR, FNR, and MCC. The system’s efficacy is depicted by the low value of FPR along with FNR and the high value of MCC. The BReLU-ResNet attains low FPR and FNR; in addition, high MCC. Hence, the BReLU-ResNet surpassed the other prevailing ones along with depicts enhanced results.

Performance Analysis of the Proposed SHP-ECC Algorithm:

The proposed SHP-ECC is analyzed with the prevailing Rivest, Shamir, Adleman (RSA), and Advanced Encryption Standard (AES), together with Data Encryption Standard (DES) regarding SL, Encryption Time (ET), and Decryption Time (DT).

In table 4, the security rates acquired by the SHP-ECC along with the prevailing RSA, AES, along with DES are depicted. The SHP-ECC achieved high security of 93.75%; while, the current system attained a lower value of 35.41%. Hence, the ET with DT is effectively performed by the SHP-ECC; in addition, alleviates the external attack. The SHP-ECC secured the cloud server against intruders.

Table 4: depicts the Encryption and Decryption time Achieved by the Proposed SHP-ECC Method and the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard (AES), together with Data Encryption Standard algorithms.

Techniques	Encryption time	Decryption time
Proposed SHP-ECC	0.1980606	0.3009068
RSA	0.269298	0.311289
AES	2.984248	2.596526
DES	0.402872	0.312929

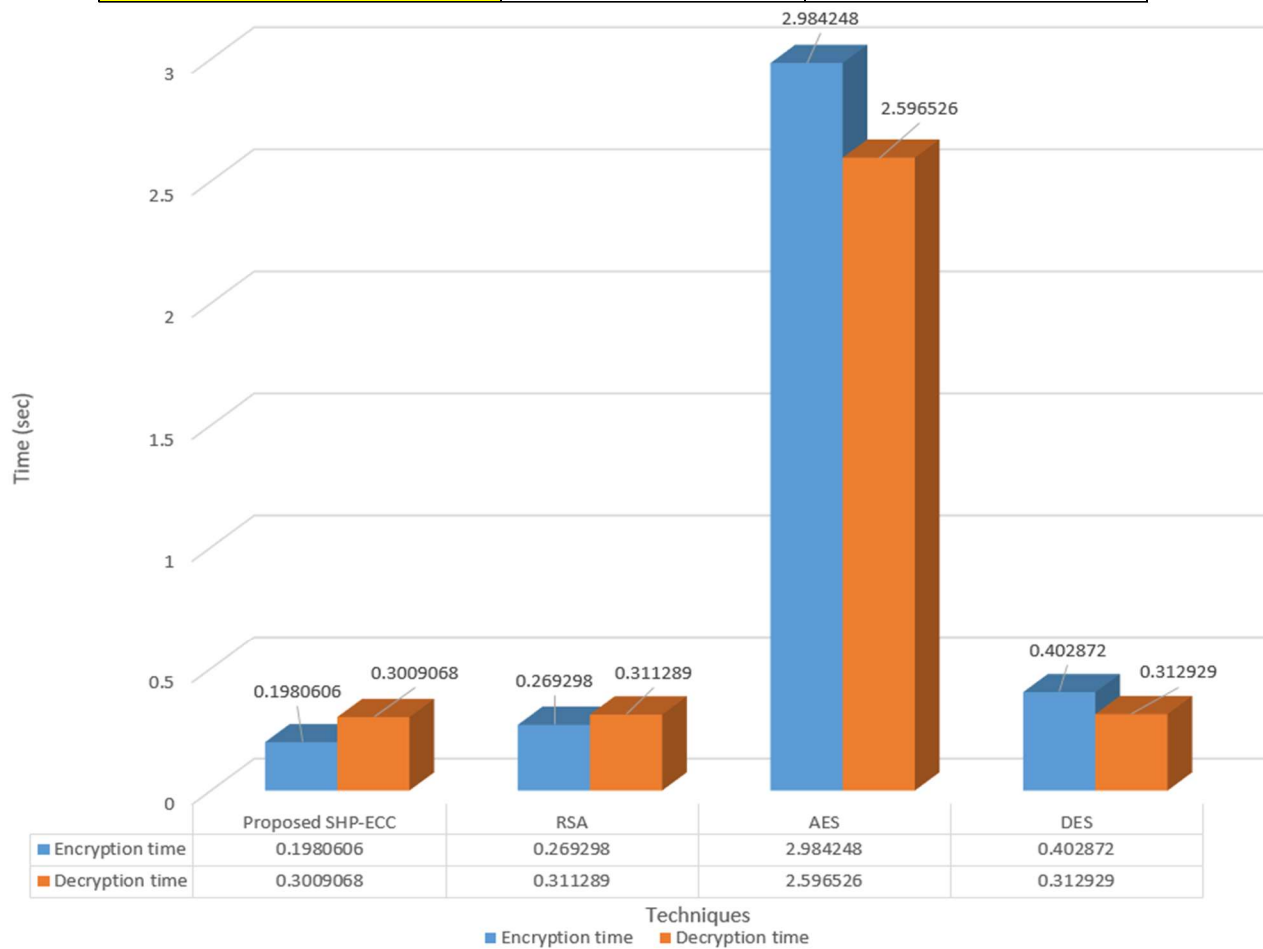


Figure 5: Comparative analysis of the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm in terms of Encryption Time and Decryption Time with the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms.

In figure 5, the comparison of ET with DT archived by the SFP-ECC together with the prevailing RSA, AES, and DES is exhibited. The model's efficacy is depicted by the low usage of ET with DT. The SFP-ECC took 0.1980606 seconds, and 0.3009068 seconds for ET and DT; while, the

prevailing one consumed 1.218806 seconds and 1.07358133 seconds. With less energy consumption, the ET and DT process is effectively executed by the SHP-ECC; in addition, assures data access security.

In table 5, regarding SL, the recommended SHP-ECC is analogized to prevailing Rivest, Shamir, Adleman, AES, and DES.

Table 5: Depicts the Security Rates Achieved by the Proposed SHP-ECC Method and the Existing Works like RSA, AES, and DES.

Techniques	Security level
Proposed SHP-ECC	93.75
AES	87.5
DES	12.5
RSA	6.25

In recognizing unknown attacks, the proposed technique attains a higher SL. When weighed against other encryption techniques, the proffered system has other encryption. In figure 4.6, the comparative outcomes are depicted. The other three techniques are surpassed by the security system a satisfying SL is depicted.



Figure 6: Comparison of Security Level

Receiver Operating Characteristic Curve:

The Receiver Operating Characteristic (ROC) curve is a graphical representation commonly used to assess the performance of binary classification algorithms, such as ResNet, CNN, NN (Neural Network), and ANFIS (Adaptive Neuro-Fuzzy Inference System), in distinguishing between two classes, typically "attack" and "normal" data. The ROC curve visually demonstrates the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) as the decision threshold of the classifier changes.

The below Figure 7 shows the Receiver Operating Characteristic curve comparison of the proposed BReLU-ResNet algorithm with Convolutional Neural Network, and Artificial Neural Network and, Adaptive Network-centric Fuzzy Inference System (ANFIS) in terms of True Positive Rate and False Positive Rate.

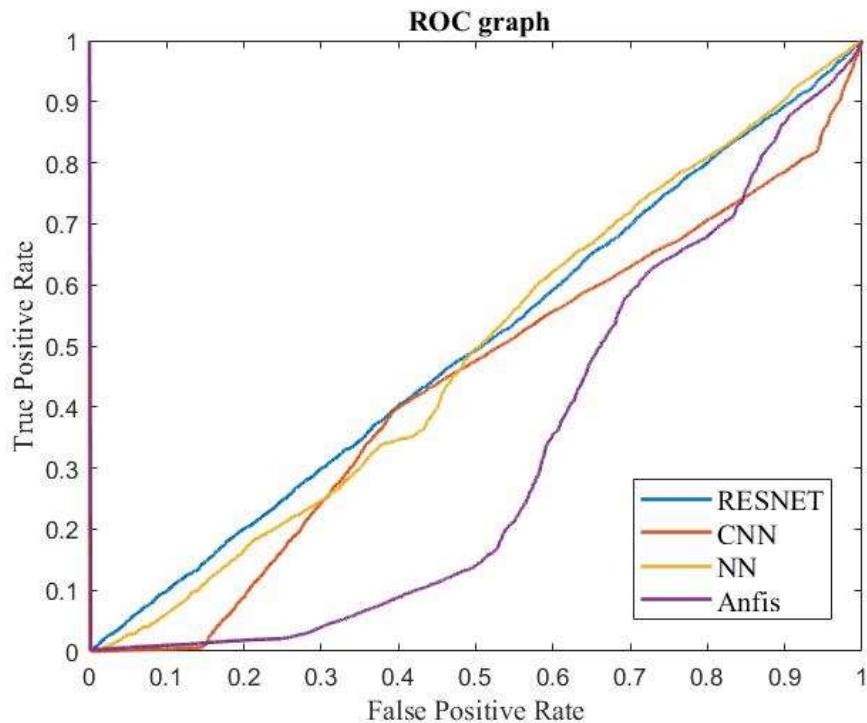


Figure 7: Receiver Operating Characteristic curve comparison of the proposed BReLU-ResNet algorithm.

THESIS CONTRIBUTION

The implementation of the research work can be discussed in two different stages namely the BReLU-ResNet model based cyber-attack detection and mitigation system, and the SHP-ECC model based data encryption and data decryption.

- The first part of the work is the model to detect and mitigation of cyber-attacks using BReLU-ResNet algorithm. In the proposed model, initially, the entire training data is pre-processed. From the input training dataset, features are extracted. To select the significant features, the feature is optimized by employing TWMA. By deploying the BReLU-ResNet, the features are trained. Implementing the skip connection for offering input for the layer indiscriminately for merging the data flow for eradicating data loss and gradient vanishing problems is the goal of Residual neural networks (ResNet). Reducing noise is averaging this system; in addition, training accuracy and generalization are maintained by it. Achieving enhanced training accuracy and approximate level of traversal is the proficient way of enhancing maximum label data. The data is classified into attack and normal data. By employing BAIT, the Source IP Address is saved into a secure log file if the data is attack data
- The second part of the work is the SHP-ECC model based data encryption and data decryption. The normal data which is classified by the proposed BReLU-ResNet algorithm is ready for the transmission. By utilizing the ESHP-ECC, the data is encrypted in Data Transmission. By employing ED, the shortest path distance is analyzed. By deploying the DSHP-ECC, the data is decrypted in the Destination. In the Security Log File (SLF), the testing data is checked in testing. The data is blocked, or attack detection is done if the data's source IP address is present already.

ORGANIZATION OF THE THESIS:

The thesis is divided into seven chapters namely

1. Introduction
2. Review of Literature
3. Research Methodology
4. Research findings of the model
5. Conclusions, Recommendations, and the Further Research Scope

Chapter 1: Introduction

This chapter gives an introduction to cyber security. The chapter gives importance to an overview of cyber security. The chapter highlights the various types of cyber-attacks in cyber space. The chapter also highlights the various mechanisms to handle cyber-attacks. The relation betwixt

several domains are discussed. The strategies used to detect and prevent cyber-attacks are also discussed in the chapter. The chapter mentions the current research problem. This chapter highlights the objective of the study and the thesis contribution.

Chapter 2: Review of Literature

This chapter gives the list of the various literature studies done on various cyber-attack and detection models. In the literature survey, it is observed that common techniques are used for the detection of cyber-attacks. But while referring to the mitigation of cyber-attacks various algorithms are adopted by different authors. It is observed that the cyber security is still in the research field for improvement. The chapter briefs about the various datasets that can be used to detect and mitigate cyber-attacks. The chapter also highlights the challenges faced by the developers during the implementation of the cyber-attack detection and mitigation models. This chapter gives a brief details about the current approaches which are used in the mitigation and detection of cyber-attacks by using machine learning and deep learning algorithms. The chapter also highlights the research gap.

Chapter 3: Methodology

This chapter deals with the conceptual model of the proposed design and explains the different parts of the model. The chapter explain the algorithms used to compare the proposed model with the prevailing systems. The chapter also deals with how the features are extracted, how the features are selected using TWMA algorithm. The chapter also includes how classification of attack and normal data are made using proposed BReLU-ResNet algorithm. The chapter explains how the data is encrypted and decrypted using proposed SHP-ECC algorithm and also explains the identification of shortest path to transfer the data in-between the source and destination using Euclidian distance algorithm. The chapter describes how the attacks are mitigated using Bait approach.

Chapter 4: Result and Discussion

This chapter deals with the analysis of the proposed model. Here the model is tested using different possible data and the output is found. The performance of the different parts of the model is shown in the table. The data base used to develop the proposed model is described in this chapter. Also this chapter highlights the performance matrix of ANFIS, NN, CNN, and proposed BReLU-ResNet algorithms. The Proposed BReLU-ResNet model is compared with the other prevailing systems using various performance matrices. Similarly, the Proposed SHP-ECC model is

compared with the other prevailing systems using various performance matrices. In this chapter the Receiver Operating Characteristic Curve is described with other prevailing algorithms.

Chapter 5: ABCD Analysis of Cyber Attack Detection and Mitigation Model

This chapter gives an analysis of proposed cyber attack detection and mitigation model in terms of Advantages, Benefits, Constraints and Drawbacks with the various performance matrices like sensitivity, specificity, accuracy, precision, recall, F1 measure, False positive rate, False Negative Rate, Matthews Correlation Coefficient matrices. The chapter also describes the analysis of attack detection and mitigation in terms of encryption and decryption time. The ABCD analysis is made based on security level of cyber attack detection and mitigation model.

Chapter 6: Conclusion

This chapter gives concluding remarks with the various benefits of using the model. Several uncertainties might be tackled by the proposed system; in addition, propitious outcomes could be achieved. When weighed against the prevailing techniques, the developed system depicted enhanced performance along with sustains to be dependable and robust. The research will be elaborated for including more superior neural networks along with various kinds of realistic attacks in the future.

Chapter 7: Future Scope of the Work

The chapter gives the idea of the further improvements that are possible from this research findings. Finally, the List of References, journal publications, and Annexure is appended to the last chapter.

JOURNAL PUBLICATIONS

- ▶ Prabhu, Sangeetha, & Bhat, Subramanya (2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(2), 40-64.
- ▶ Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 149-159. DOI: <https://doi.org/10.5281/zenodo.6349848>
- ▶ Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with Bait Based Approach for Mitigation.

International Journal of Applied Engineering and Management Letters (IJAEML), 6(1), 243-258. DOI: <https://doi.org/10.5281/zenodo.6530129>

- ▶ Sangeetha Prabhu, & Nethravathi, P. S., (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 176-183. DOI: <https://doi.org/10.5281/zenodo.6350841>
- ▶ Prabhu, S., PS, N., Spulbar, C., & Birau, F. R. (2022). Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation. *Annals of the University of Craiova, Mathematics and Computer Science Series*, 49(1), 174-182.
- ▶ Prabhu, Sangeetha, & Nethravathi, P. S., (2023). ABCD Analysis of Cyber Attack Detection and Mitigation Model. *International Journal of Engineering & Scientific Research*, 11(10), 7-15.

CONCLUSION

The advancement of technology has brought about radical changes in modern society. But, human experience has shown that every technological change brings with it some unforeseen problems, taking advantage of which the lawbreakers explore new techniques to perpetrate their criminal activities. In fact, technology-generated crimes not only affect individuals or a nation but have widespread ramifications throughout the world. Internet is one such gray area, which has given rise to the menace of cybercrimes. The convergence of computer networks and telecommunications facilitated by digital technologies has given birth to a common space called 'cyberspace'. This cyberspace has become a platform for a galaxy of human activities, which converge on the internet.

The proposed novel approach of BReLU-ResNet-based Cyber-Attack Detection System with a BAIT-based approach for mitigation. This approach involved several operations designed to check cyber-attacks quickly. Several operations were concerned about the effectiveness of this technique in detecting cyber-attacks. Pre-processing, characteristic extraction, feature selection, and classification are all used to detect intrusions. The typing phase effectively determines whether the data are normal or malicious. The information transmission procedure commences if the records are normal. The work is pre-processed, feature extracted, feature selected, and classified for intrusion detection. The typing phase effectively determines whether the data are normal or

malicious. The classification phase efficiently detects whether the data is normal or attacked. If the data is normal, then the data transmission process begins. To ensure security, the encryption and decryption process is performed by the means of the SHP-ECC algorithm. The encryption and decryption methods are implemented using the SHP-ECC set of rules to ensure security. The experimentation assessment is then completed, with an overall performance evaluation and comparative analysis of the offered methods in terms of some overall performance indicators to validate the effectiveness of the given set of rules.

The experimental analysis is then carried out, which includes performance analysis and a comparison study of the offered methodologies in terms of various performance measures to test the proposed algorithm's efficacy. Moreover, to provide more insight into the performance of the system, the proposed system was evaluated using the confusion matrix parameters (i.e., TN, TP, FN, FP) and computed some other performance evaluation metrics including the classification precision, the classification recall, the F1-score of classification, FNR, and MCC.

The developed approach can handle various uncertainties and render more promising results. The publically available dataset called UNSW-NB 15 dataset is used for the analysis, in which the proposed method achieves 98.34% of sensitivity, 77.54% of specificity, 96.6% of accuracy, 97.96 % of Precision, 98.34% of recall, 98.15 % of F-measure, 22.46% of False Positive Rate, 1.66 % of False Negative Rate, 77.38 % of Matthew's correlation coefficient and excessive security level of 93.75 percent. The suggested cyber-attack detection methodology surpasses current state-of-the-art methodologies and remains more dependable and robust. In the future, the study will be expanded to include more advanced neural networks as well as different types of realistic attacks.

LIST OF TABLES

Table No.	Title	Page No.
2.1	ECML/PKDD Dataset Characteristics.	30
2.2	Data volume for each botnet scenario.	32
2.3	The elements of ADFD-LD.	34
2.4	UNSW-NB15 Dataset Specifications.	34
2.5	Performance Comparison of ML Models Applied in Cyber Security.	41
2.6	Various Deep Learning Models in Cyber-Attack Detection and Mitigation.	49
4.1	UNSW-NB15 Dataset.	96
4.2	Confusion Matrix Analysis.	97
4.3	Performance Analysis of Proposed BReLU-ResNet on the Basis of Sensitivity, Specificity, and Accuracy.	109
4.4	Performance Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-measure.	112
4.5	Performance Analysis of Proposed BReLU-ResNet concerning False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.	115
4.6	Depicts the Encryption and Decryption time Achieved by the Proposed SHP-ECC Method and the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard (AES), together with Data Encryption Standard algorithms.	118
4.7	Depicts the Security Rates Achieved by the Proposed SHP-ECC Method and the Existing Works like RSA, AES, and DES.	122
5.1	The summary of determinant issues and key attributes of various factors in terms of advantages.	140
5.2	The summary of determinant issues and key attributes of various factors in terms of benefits.	141

5.3	The summary of determinant issues and key attributes of various factors in terms of constraints.	142
5.4	The summary of determinant issues and key attributes of various factors in terms of advantages.	143
5.5	The summary of Systematic Review of ABCD Analysis Usage.	145
5.6	Advantages of key attributes under cyber security in ABCD analysis	150
5.7	Benefits of key attributes under cyber security in ABCD analysis	151
5.8	Constraints of key attributes under cyber security in ABCD analysis	153
5.9	Drawbacks of key attributes under cyber security in ABCD analysis	155
5.10	Advantages and Benefits of performance metrics sensitivity under cyber security.	157
5.11	Constraints and Drawbacks of performance metrics sensitivity under cyber security.	157
5.12	Advantages and Benefits of performance metrics specificity under cyber security.	158
5.13	Constraints and Drawbacks of performance metrics specificity under cyber security.	159
5.14	Advantages and Benefits of performance metrics precision under cyber security.	159
5.15	Constraints and Drawbacks of performance metrics precision under cyber security.	160
5.16	Advantages and Benefits of performance metrics recall under cyber security.	161
5.17	Constraints and Drawbacks of performance metrics recall under cyber security	161

5.18	Advantages and Benefits of performance metrics F-measure under cyber security.	162
5.19	Constraints and Drawbacks of performance metrics F-measure under cyber security.	163
5.20	Advantages and Benefits of performance metrics accuracy under cyber security.	164
5.21	Constraints and Drawbacks of performance metrics accuracy under cyber security.	164
5.22	Advantages and Benefits of performance metrics False Positive Rate under cyber security	165
5.23	Constraints and Drawbacks of performance metrics False Positive Rate under cyber security.	166
5.24	Advantages and Benefits of performance metrics False Negative Rate under cyber security.	167
5.25	Constraints and Drawbacks of performance metrics False Negative Rate under cyber security.	167
5.26	Advantages and Benefits of performance metrics Matthews Correlation Coefficient under cyber security.	168
5.27	Constraints and Drawbacks of performance metrics Matthews Correlation Coefficient under cyber security.	169
5.28	Advantages and Benefits of performance metrics encryption and decryption time under cyber security.	170
5.29	Constraints and Drawbacks of performance metrics encryption and decryption time under cyber security.	171
5.30	Advantages and Benefits of performance metrics Security Level under cyber security.	171
5.31	Constraints and Drawbacks of performance metrics Security Level under cyber security.	172

LIST OF FIGURES

Figure Number	Title	Page Number
1.1	Various Domains of Cyber Security	14
3.1	Advanced Encryption Standard Algorithm Structure	55
3.2	Advanced Encryption Standard Algorithm Encryption Process	56
3.3	Elliptic curve cryptography graph	61
3.4	Layers of artificial neural network	67
3.5	CNN building architecture.	69
3.6	Structural Design of the Proposed Cyber-Attack Detection and Mitigation System	72
3.7	Position of Female Woodpecker	74
3.8	Flowchart of TWMA	76
3.9	Pseudocode of the Proposed Feature Selection Technique	81
3.10	RESNET Architecture	83
3.11	Residual Network Building Block	84
3.12	Elliptic Curve	87
3.13	Pseudocode for Proposed ESHP-ECC	90
3.14	General Structure of Bait	92
4.1	Diagrammatic Representation of TP, TN, FP, and FN Regarding Relevant and Retrieved Docs.	97
4.2	Confusion matrix of ANFIS algorithm over attack and normal data.	102
4.3	Confusion matrix of NN algorithm over attack and normal data.	104
4.4	Confusion matrix of CNN algorithm over attack and normal data.	106
4.5	Confusion matrix of BReLU-ResNet algorithm over attack and normal data.	108
4.6	Comparative Analysis of Proposed BReLU-ResNet based on Precision, Sensitivity, Specificity, Accuracy	111

4.7	Comparative Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-Measure	114
4.8	Comparative Analysis of Proposed BReLU-ResNet in Terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.	117
4.9	Comparative analysis of the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm in terms of Encryption Time and Decryption Time with the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms.	120
4.10	Comparison of Security Level	123
4.11	Receiver Operating Characteristic curve comparison of the proposed BReLU-ResNet algorithm.	126

LIST OF SYMBOLS AND ABBREVIATIONS

Notations	Abbreviations
$x_{(i)}$	Extracted features
n	Number of Woodpeckers
x^*	Highest fitness
$f(x_{(i)})$	Fitness evaluation
δ	Sound intensity
γ	Sound frequency
D	Density of Medium
A	Sound amplitude
χ	Area of the sphere
S	Sound speed
ψ	Area of Sound
t	Shortest distance between the source and the object
$(y_{f,j}^{\tau+1})$	Position updating process
x_m	Source position
$x_{m,i}$	Population size
$y_{x^*}^{\tau}$	Position of the best woodpecker
y_f	Listener Position
tS	Tangent Sigmoid Function
r	Random Number
τ, τ^{\max}	Current and Maximum Number of Iterations Respectively
$\beta^{x^*}, \beta_{m,i}$	Attractiveness of the female bird to the male bird
α	Random Value
$\alpha_{f,j}^{\tau}$	Self-tuning random factor
μ	Movements
R	Runaway movement

P	Runaway movement of x^*
L	Lower Bound
U	Upper bound
ξ	Sound intensity of x^*
ϕ	Runaway coefficient
Γ	Filter
η	Random number is generated from $[1, n-1]$
p, o	The probability and possible outcome of X^k
X^k	Selected best features
∂X^k	Approximation of residual function
$f(X^{(k)})$	Target function
ρ	Public key
E^d	Euclidean Distance
Q	Original message
FIS	Federal Information Security
TCAs	Targeted Cyber Attacks
ID	Intrusion Detection
APTs	Advanced Persistent Threats
DL	Deep Learning
IDS	Intrusion detection Systems
IPS	Intrusion Prevention Systems
SQL	Structured Query Language
SQLi	Structured Query Language Injection
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
OS	Operating System
UDP	User Datagram Protocol
ICT	Information and Communications Technology
USB	Universal Serial Bus

OSI	Open Systems Interconnection
SPAN	Switch Port Analyzer
TAP	Traffic Access Point
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
PIDS	Protocol-based Intrusion Detection System
APIDS	Application Protocol-based Intrusion Detection System
IOC	Indicator Of Compromise
LAN	Local Access Network
ARP	Address Resolution Protocol
MAC	Media Access Control
MiTM	Man-in-The-Middle
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention Systems
HIPS	Host centric Intrusion Prevention Systems
NIPS	Network based Intrusion Prevention System
WIPS	Wireless Intrusion Prevention System
NBA	Network Behavior Analysis
IT	Information Technology
RL	Reinforcement Learning
LP	Linear Programming
LR	Logistic Regression
DT	Decision Trees
RF	Random Forest
SVM	Support Vector Machine
NB	Naive Bayes
KNN	K-Nearest Neighbour
SCADA	Supervisory Control and Data Acquisition
IoT	Internet of Things
RF	Random Forest
SVM	Support Vector Machine

PCA	Private Cloud Appliance
NS	Network Security
PNN	Probabilistic Neural Network
CAD	Cyber Attack Detection
AFRL	Air Force Research Laboratory
U2R	User-to-root
R2L	Remote-to-Local
ECML	European Conference on Machine Learning
<i>ISOT</i>	Information Security and Object Technology
CAMNEP	Cooperative Adaptive Mechanism for Network Protection
LAMS	Local Adaptive Multivariate Smoothing
UMN	Unus Mundus Network
DARPA	Defense Advanced Research Projects Agency
FTP	File Transfer Protocol
PHP	Hypertext Preprocessor
SSH	Secure Shell
LR-DDoS	Low-Rate Denial-of-Service
SDN	Software Defined Network
MIMO	Multiple-Input Multiple-Output
ICA	Integrity, Confidentiality, and Availability
DBN	Deep Belief Network
BC	Block Chain
AEs	Auto Encoders
CNNs	Convolution Neural Networks
ID	Intrusion Detection
OSS	One-Side Selection
Bi-LSTM	Bi-Directional Long Short-Term Memory
ESHP-ECC	Encrypted Secure Hash Probability-based Elliptic-curve cryptography
DSHP-ECC	Decrypted Secure Hash Probability-based Elliptic-curve cryptography

LPT	Left Plain Text,
RPT	Right Plain Text
NIST	National Institute of Standards and Technology
ECDLP	EC Discrete Logarithm Problem
MD	Message-Digest
S-MIME	Secure / Multipurpose Internet Mail Extensions
IPSec	Internet Protocol Security
AI	Artificial Intelligence
RNN	Recurrent Neural Networks
CPS	Cyber-Physical Systems
SL	Security Level
ICSs	Industrial Control Systems
DoS	Denial Of Service
CS	Cyber Security
BP	Back Propagation
ML	Machine Learning
DNN	Deep Neural Network
AUC	Area Under the Curve
SLF	Security Log File
KNN-ACO	K-Nearest Neighbors - Ant Colony Optimization
FC	Fully Connected layer
Convlayer	Convolutional Layer
ResNets	Residual Networks
ABC	Artificial Bee Colony
W	Linear Projection
AFS	Artificial Fish Swarm
IP	Initial Permutation
FCM	Fuzzy C-Means Clustering
CFS	Correlation-based Feature Selection

CART	Classification And Regression Tree
AdaBoost	Adaptive Boosting
NSGA- II	Non-Dominated Sorting Genetic Algorithm II
NSGA2-BLR	Non-Dominated Sorting Genetic Algorithm Binomial Logistic Regression
NSGA2-MLR	Non-Dominated Sorting Genetic Algorithm Multinomial Logistic Regression
CDS	Cross Domain Solutions
AD	Active Directory
DHN	Deep Hierarchical Network
PMUs	Phasor Measurement Units
TWMA	Taxicab Woodpecker Mating Optimization
WMA	Woodpecker Mating Algorithm
ANN	Artificial Neural Networks
ECC	Elliptical Curve Cryptography
SAE	Stacked Auto-Encoder
GPU	Graphical Processing Unit
ED	Euclidean Distance
CPU	Central Processing Unit
FAR	False Acceptance Rate
FRR	False Rejection Rate
FP	False Positive
TP	True Positive
FN	False Negative
TN	True Negative
TPR	True Positive Rate
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
VPN	Virtual Private Network
MCC	Matthews Correlation Coefficient
ANFIS	Adaptive Network-Centric Fuzzy Inference System

RSA	Rivest, Shamir, Adleman
AES	Advanced Encryption Standard
RREQ	Route Request
MN	Malicious Node
FM	F-Measure
SAR	Synthetic Aperture Radar
DES	Data Encryption Standard
ET	Encryption Time
DT	Decryption Time

CHAPTER 1

INTRODUCTION

1.1 Preface

For organizations and the huge public, cyber-attack has emerged to be an augmenting threat. Thus, a huge negative effect was caused on the economy along with people's daily life. The considerable development of cyber-attack incidents is caused by the exponential growth of Internet interconnections with disastrous along with grievous consequences. The initial choice of weapon for conducting intents in cyberspace, either by exploitation of prevailing vulnerabilities or usage of developing technologies' unique characteristics is termed malware. The computer system's deliberate exploitation is termed a cyber-attack. For modifying the computer code logic or data, malicious codes are deployed by the cyber-attack. A cyber-attack is a computer attack that targets a computer or network system's availability, integrity, and secrecy by using a sequence of computer operations. The weakness within the defense mechanisms that are responsible for securing them is highlighted by each successful cyber-attack on aimed devices along with networks. It is necessary to prevent potential attacks in the future to attain a thorough understanding of cyber threats. For avoiding cyber-attacks along with protecting the valuable assets of an organization, several efforts have been done. Nevertheless, sophistication's profound levels and the attacker's intelligence are depicted by the prevailing cyber-attacks; in addition, delineated conventional attack detection mechanisms fail in diverse attack circumstances. The problems and the challenges faced by alternative solutions are previously highlighted by various researchers. For recognizing potential cyber threats in real-time situations, there is an unprecedented requirement for a solution. A progressive, multi-faceted approach like cyber-attack modelling is suggested for cyber threat analysis. The majority of economical, industrial, cultural, social, and governmental engagements as well as international exchanges between people, non-governmental agencies, and governmental organizations are being carried out in cyberspace. The cyber-attacks and wireless communication technologies are faced by several private companies along with government organizations globally. The globe is hugely reliant on electronic technology; in addition, it was a challenging problem to protect from cyber-attacks. In the Cyber Security (CS) community, the enhancement of more innovative and effective cyber detection mechanisms is considered an urgent requirement. By deploying a new

Classification and Encryption methodology, a fresh system was proposed for attack node mitigation for attaining the aims. For preparation and testing, the UNSW-NB15 dataset is achieved along with classified initially. Within the preparation time frame, the information pre-handled together with incorporated is eliminated. For recognizing the associated highlights, the TWM is deployed. The input into went after along with non-went behind groups are sorted by the BReLU-ResNet. In the security log record, the compromised information is saved. By employing the ESHP-ECC, the typical data is encrypted. By employing the Euclidean Distance (ED), the shortest path distance is calculated. The data is present lately. The information is decrypted by deploying the DSHP-ECC. It is considered the sought-after data if the information is present in the log document in testing along with is secured from the transmission. The process of digital assault recognition starts if it is absent. The study is grounded on the UNSW-NB 15 dataset. For awareness, particularity, exactness, Precision, review, F-proportion, False Positive Rate, False Negative Rate, and Matthew's connection coefficient, the proposed system attains 98.34, 77.54, 96.6, 97.96, 98.34, 98.15, 22.46, 1.66 77.38 respectively. The proposed technique attained an extreme Security Level (SL) of 93.75%.

1.2 Overview of Cyber Attack Detection

Enormous security organizations sustain augmenting innovative systems for securing peripherals along with sensitive data as of cyber-attacks [1]. In broad security practices, network-centric along with host-centric systems, which secure cornered peripherals from illegal intrusion are included [2]; in addition, (A) Firewalls, (B) Intrusion Detection (ID) System (IDS), (C) threat protection, (D) simple control above system practices; (E) a flag advance grounded on configured detection priority in which ID plays a vital role are also encompassed. Moreover, it plays a key role in helping to forecast unlawful access, and variations, as well as the destruction of information systems in information security. The divisions of IDS are Signature-centric, statistical anomaly-centric, and combined [3]. Signature-centric employs predefined signatures of abuse activity for categorizing intrusion efforts [4].

Natural sequences are integrated by the Statistical anomaly-centric detection along with detecting the wary activity grounded on deviations of routine lines [5]. Abuse detection and anomaly detection methodologies are practiced by the merged approach of the detection system. For protecting networks along with user data as of (a) attacks, (b) anti-malware, (c) viruses; (d) threat protection are developed by several vendors such as (1) Microsoft, (2)

Checkpoint, (3) Symantec, (4) McAfee, (5) Kaspersky, DNS (6) Symantec, and (7) Microsoft McAfee. In resolving tedious issues, the DL technique plays a significant role. DL could be categorized as several multi-layered ML methodologies, which capture common notations of the tedious and huge amount of data. For various CS companies, security systems' modernization is provided at an optimal cost by DL.

1.2.1 When is an Attack Deemed a Targeted Attack?

When the attack fulfills the key criteria, it could be regarded as a targeted cyber-attack. A particular organization or an individual is focused on by the attacker along with setting up the targeted attack; it has to spend some time, and effort, together with resources. The attacker's goal while initiating a TCA is to steal information by breaking into the system and performing data exfiltration via transforming communication, also known as covert communication, which hides the data being sent and the link between the sender and recipient [6]. The attack is persistent; in addition, by utilizing automated and highly sophisticated malware, it was attained.

1.3 Types of Cyber Attacks

A procedure where an individual or else a group of persons tries to enter a system unlawfully for exploiting data or information is called a cyber-attacks. A computer network attack is termed integrity disruption or authenticity of data or information. The program's logic is modified by the malicious code written for this purpose along with executing certain unwanted activities. For attaining the system, which includes deprived security control along with stare for systems that are misconfigured, the hacking comprises Internet scanning. The hacker could remotely work the stained system together with the commands that could be sent to create the system to act as a spy, which might be wielded for disrupting the other systems' services once they infect the system. The infected system might be expected to have a few flaws like bugs in software, deficiency in anti-virus, and flawed system configuration by the hacker; thus, other systems could be infected via this system. Stealing or hacking the information of any organization or government office is the goal of a cyber-attack. Attacks can be divided into three types.

1. No former system knowledge or else Deep Learning (DL) along with black box attack is included by the attacker.
2. A few pieces of information, design elements, together with credible information are understood by the gray box test attackers [7].

3. About the white-box model that just takes place in the most critical case, the attacker has broad details.

A system to (1) hurt, (2) reveal, (3) change, (4) destroy, (5) steal, or else (6) obtain unlawful entry to a network system resource is termed a cyber-attack. The significant cyber-attacks are as follows,

1. Denial of Service Attack (DoS):

Whilst spreading a considerable quantity of traffic in a unique method to the chosen recipient, it takes place. For operating the network, target users don't have permission. Enduringly or momentarily suspending or else terminating the service is the key goal. By relocating traffic to the chosen recipient, it is tackled; they aren't permitted to network operation [8].

The most popular way to carry out a DoS attack is to swarm the targeted server or network with unauthorized service requests. The use of a bogus IP address, which prevents the server from authenticating the user, is the distinguishing feature of these assaults. The server becomes overloaded while handling the barrage of fraudulent requests, which slows it down and occasionally causes it to crash, interfering with real users' access. Most DoS attacks require the malicious actor to have access to more bandwidth than the target to be successful.

A DoS attack can be carried out in a variety of ways. Attackers most frequently target network servers by saturating them with traffic. In this kind of DoS attack, the attacker floods the target server with requests, causing it to become overloaded. These service requests are fraudulent and contain fake return addresses, which deceive the server when it tries to verify the requester's identity. The server becomes overloaded as the junk requests are continuously processed, which results in a DoS circumstance for legitimate requestors.

- i. **Application Layer:** These attacks create fictitious traffic for domain name system (DNS) or hypertext transfer protocol (HTTP) servers, among other internet application servers. Some application layer denial-of-service attacks bombard the victim's application server or protocol with network data while others target the victim's application server or protocol in search of flaws.

- ii. **Overflowing buffer.** This kind of attack involves sending a network resource more traffic than it was intended to receive.
- iii. **Amplification of the DNS:** In conducting a DNS denial-of-service attack, the attacker creates DNS requests that appear to have come from an IP address in the targeted network and delivers them to incorrectly configured DNS servers run by other organizations. As the intermediary DNS servers answer the bogus DNS requests, the amplification takes place. It may take more resources to process the responses from intermediate DNS servers to the requests since they carry more data than standard DNS responses. This may prevent legitimate users from using the service.
- iv. **Ping of death:** These attacks misuse the ping protocol by delivering request messages with excessively large payloads, which overwhelms the target systems, prevents them from responding to valid service requests, and may even cause system crashes on the victim's end.
- v. **State exhaustion:** These attacks, commonly referred to as Transmission Control Protocol (TCP) attacks, occur when an intruder addresses them and loads them with attack data. They are aimed at the state tables kept in firewalls, routers, and other connected devices. Intruders may be able to overload the state tables and prohibit legitimate users from accessing the network resource by starting more TCP connections than the victim's system can manage at once when these devices offer stateful inspection of network recourses.
- vi. **SYN flooding:** The TCP handshake protocol, which is utilized to create a TCP connection between a server and a client is exploited in this attack. When launching an SYN flood assault, the attacker sends a lot of open TCP connections to the target server without planning to cancel any of the connections. A successful attack may prevent authorized users from accessing the server being targeted.
- vii. **Teardrop:** The handling of fragmented IP packets by earlier operating systems (OSes) is one weakness that these attacks make use of. The IP protocol permits packet fragmentation and requires that packet fragments contain fragment offsets when packets are too large to be handled by intermediate routers. The fragment offsets are set up for teardrop attacks to overlap. As a result, hosts running impacted OSes are unable to put the pieces back together, which can cause the attack to crash the system.

- viii. **Volumetric:** The DoS attacks use every bit of available bandwidth to reach network resources. To do this, attackers need to bombard the victim's computers with a lot of network traffic. Volumetric DoS attacks flood the devices of their victims with network packets utilizing UDP or Internet Control Message Protocol (ICMP). The network devices of the victim are simultaneously overloaded with network packets as they attempt to process the incoming malicious datagrams, whereas these protocols require relatively minimal overhead to generate high amounts of traffic.

2. Man in the Middle:

It is a form of malware, which infiltrates along with encrypts significant files as well as systems; hence, preventing a person from accessing their data [9]. A cyberattack known as a man-in-the-middle (MiTM) attack involves the perpetrator discreetly intercepting and relaying messages between two parties who believe they are speaking directly to one another. An attack is a form of eavesdropping in which the assailant overhears the full discussion before taking control of it. MiTM hacks pose a serious risk to internet security because they provide the attacker real-time access to and control over sensitive information including login credentials, account information, and credit card details.

Cybercriminals interject themselves into online conversations or data transactions during MiTM attacks spreading malware, an attacker can quickly get access to a user's web browser and the information it sends and receives throughout transactions. MiTM attacks are particularly effective in stealing login passwords and other sensitive information from online banking and shopping sites, which demand safe authentication using a public key and a private key.

Data interception and decryption, a two-step procedure, are typically used to carry out these attacks. A data transfer between a client and a server may be intercepted by an attacker as part of data interception. The attacker tricks the client and server into thinking they are sharing information by intercepting the data, connecting to a trustworthy website, serving as a proxy to read and inject misleading info into the conversation, and so on.

The following stages make up one common data interception technique:

1. An attacker deploys a packet sniffer to identify potentially hazardous network traffic, for instance when a user uses an unprotected public hotspot or views an HTTP-based website.
2. When a user logs onto a hazardous website, the hacker obtains their information and sends them to a fraudulent one.
3. The spoof website duplicates the genuine one and gathers all essential user data. The attacker can then use this information to access all useful resources on the genuine website.

The data that was intercepted is not encrypted until the decryption stage. This crucial stage enables the attacker to ultimately decode the data and use it to their benefit, for as by committing identity theft or interfering with business processes.

3. Trojan horse:

Malware that poses as trustworthy programs or software is known as a Trojan horse (Trojan). Attackers have access to all actions that a legitimate user could perform once they are within the network, including exporting files, editing data, deleting files, and otherwise changing the contents of the device. Trojans may come pre-installed with a game, tool, app, or even software patch downloads. To get the user to take the intended action, many Trojan assaults also include spoofing, phishing, and social engineering techniques. It frequently resembles a beneficial program that the user is prepared to run while concealing hazardous code.

Trojan infections prey on users' ignorance of security issues and computer security safeguards like antivirus and antimalware software to do their dirty job. A Trojan usually takes the form of email-attached malware. The program, application, or file seems to originate from a reliable source. The reputable source the email attachment comes from could be a hoax as the user examines it. Getting the user to download and open the file is the aim.

The computer or other devices then have malware or other malicious stuff installed and activated. Malicious content spreading to other files on the device and harming the computer is one typical attack method. From Trojan to Trojan, this is accomplished in different ways. Everything depends on the purpose and design of the hackers who created the Trojan infection. One thing to keep in mind while implementing security measures to counteract Trojans is how well a Trojan performs. Even though the phrase "Trojan virus"

is frequently used, the more precise description is "Trojan malware." Both desktops and mobile devices can be used by viruses to execute and replicate themselves. This cannot be done using Trojan malware. The Trojan must be launched by the user for it to carry out the intended hacker action.

4. SQL Injection:

A Structured Query Language (SQL) injection is a quite common attack that occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. It is a general attack, which takes place when an attacker interleaves malicious code into a server, which deploys SQL together with forces the server to disclose the information it commonly wouldn't. By acquiescing malicious code into a vulnerable website search box, an attacker might conduct a SQL injection. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box. SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

SQL Injection (SQLi) is a type of injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

5. Poisoning and Evasion Attacks:

Every DL planning step includes a poison assault. The intruder then inserts the virus within the preparation samples, lowering the DL technique's ability to predict outcomes [10]. Attacks that intentionally introduce erroneous data into a network or infrastructure are referred to as poisoning attacks. Attackers can use this to steal private information or carry out other nefarious deeds. the many poisoning assault types.

- i. **Web cache poisoning:** Adding infamous websites to the cache through requests made from a system under the control of the attacker.
- ii. **DNS cache poisoning:** The Domain Name System (DNS) transforms human-readable website addresses into computer-processable IP addresses. By taking advantage of flaws, the attacker hopes to divert web traffic away from trustworthy servers and onto counterfeit ones.
- iii. **ARP cache poisoning:** This is when an attacker alters the Media Access Control (MAC) address to fill the system's ARP cache with phony ARP requests and response packets.
- iv. **Model poisoning:** It is a form of assault carried out against AI and machine learning systems. Attackers change the training datasets used to alter the outcomes to suit their purposes.

Evasion attacks are the most frequent kind of attacks that could happen in hostile surroundings when a system is in use. As an illustration, spammers, and hackers commonly attempt to evade detection by hiding the infected code and content. The goal of the evasion option is to have harmful samples be misclassified as legal to avoid detection. There is no way to alter the training data.

6. Bitcoin Attack:

It is an attack that uses an unidentified pattern or targets to exploit a potentially critical software security vulnerability that neither the developer nor security staff are aware of.

7. Probing:

The attackers look over the networks and successfully take information and data. Probing attacks are an invasive method for bypassing security measures by observing the physical silicon implementation of a chip. As an invasive attack, one directly accesses the internal wires and connections of a targeted device and extracts sensitive information. In combination with reverse engineering, this poses a serious threat. A typical probing attack

will begin with decapsulation to expose the silicon die. Once done, an attacker can begin reverse-engineering the device. By extracting the netlist, one can begin to understand the functionality and identify signals to target. Once the attacker finds a targeted signal and can map them to coordinates on a device, it can begin milling. By milling they expose the internal wires of the device. They can then form an electrical connection and begin extracting information. To protect against such attacks, a designer needs to identify possible targets and take appropriate measures.

8. Sniffer:

Sniffer is another application that listens in on routing information and scans each packet in the data stream for certain data, such as passwords. Sniffing attacks are also called “packet sniffing” or “network sniffing” attacks because cybercriminals sniff data packets within a network. A data packet is a unit of data sent and received on a network. Sniffers are also known as network protocol analyzers. While protocol analyzers are network troubleshooting tools, they are also used by hackers for hacking networks. If the network packets are not encrypted, the data within the network packet can be read using a sniffer. Sniffing refers to the process used by attackers to capture network traffic using a sniffer. Once the packet is captured using a sniffer, the contents of the packets can be analyzed. Sniffers are used by hackers to capture sensitive network information, such as passwords, account information, etc.

9. Worms:

This is a self-sustaining running program, which does not need another file or program to copy itself. Worms replicate over a network using protocols. Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data or delete files. Some payloads even create backdoors in host computers that allow them to be controlled by other computers. Malicious parties can use networks of these infected computers (“botnets”) to spread spam and perform denial-of-service attacks. Computer worms make use of some of the deepest and most dangerous vulnerabilities in a victim's computer. Whereas a Trojan uses social

engineering techniques to trick you into activating it, and a virus exploits holes in application code to piggyback a ride, a worm finds seams in the computer's operating system that allow it to install and make copies of itself. To propagate itself further, it will then follow known holes in networking and file transfer protocols. The latest incarnation of worms makes use of known vulnerabilities in systems to penetrate, execute their code, and replicate to other systems such as the Code Red II worm that infected more than 259 000 systems in less than 14 hours. On a much larger scale, worms can be designed for industrial espionage to monitor and collect server and traffic activities and then transmit them back to their creator.

10. Logic Bomb:

Another sort of assault is a logic bomb, in which a programmer inserts code into a computer so that, in the case of a particular circumstance, the software automatically engages in harmful behavior [11]. A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs. When this condition is met, the logic bomb is triggered devastating a system by corrupting data, deleting files, or clearing hard drives.

A logic bomb is a type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system to cause harm to a network when certain conditions are met. It is triggered at a specific event and used to devastate a system by clearing hard drives, deleting files, or corrupting data. An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system.

To maximize damage before being noticed, logic bombs are mainly used with trojan horses, worms, and viruses. The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system. The devastation caused by a logic bomb can be a huge level.

There are two types of conditions that can set off a logic bomb: positive and negative. Logic bombs with positive triggers are those that are detonated once a condition is met, such as the date of a key company event or when you open a specific file. And a logic bomb that is launched when a condition is not met is known as a logic bomb with negative triggers. And a logic bomb that is launched when a condition is not met is known as a logic bomb with

negative triggers, such as when the bomb is not deactivated on time, or an employee is unable to deactivate the code by a specific time.

The attacks caused by a logic bomb can be huge level. There are multiple examples of logic bombs that describe how they have wiped out some organizations and servers of major financial institutions. Anything that has the potential to destroy the server of an organization or institution can be more powerful to the general population it serves, as well as devastating the company itself.

11. Botnet:

A botnet is a collection of compromised remote control devices that are used to spam, coordinate assaults, and spread malware. Botnets are usually secretly installed on the target computer, allowing the unauthorized user to remotely control the target system to achieve their malicious goals [12]. Each machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out coordinated criminal action. The scale of a botnet (many comprised of millions of bots) enables the attacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under the control of a remote attacker, infected machines can receive updates and change their behavior on the fly. As a result, bot-herders frequently can rent out access to certain areas of their botnet on the black market for a sizable profit.

Botnets are produced when the bot-herder uses file-sharing, email, social media application protocols, or other bots as a middleman to deliver the bot from his command and control servers to an unaware receiver. The bot reports back to command and control after the recipient opens the malicious file on his computer, allowing the bot-herder to issue orders to infected devices.

Bots and botnets are highly suited for persistent incursions due to several distinctive functional characteristics. The bot-herder can update the bots to change their entire operation according to what he or she wants them to do and to accommodate adjustments and defenses made by the target system. The bot-herder has access to a virtually limitless number of communication channels through which to react to shifting circumstances and disseminate updates thanks to the ability of bots to use other infected machines in the botnet as communication channels. This demonstrates that the most crucial phase is an infection

because functionality and communication channels may always be altered as necessary in the future. Governments, businesses, and individuals are extremely concerned about the cybersecurity of botnets since they are one of the most advanced forms of contemporary malware.

12. Spoofing:

Spoofing is a cyberattack in which a person or program creates bogus data to impersonate another to gain unauthorized access to a system. These threats are frequently present in emails whose sender's address has been faked [13]. The ability of a hacker to pose as someone or something else is essential for spoofing. Some attackers make their phone calls and emails look like they are coming from a reliable source to gain their trust. Hackers attempt to fool you into disclosing sensitive personal information using these kinds of spoofing attacks.

Attacks using DNS or IP address spoofing are another more technical form of spoofing. Network security spoofing entails deceiving a computer or network by utilizing a fake IP address, rerouting internet traffic at the DNS (Domain Name System), or fabricating ARP (Address Resolution Protocol) data within a local access network (LAN).

1.3.1 Cyber Attack Handling Mechanisms

Some of the significant cyber-attack handling mechanisms are:

- i. **Scientific Approach:** To increase intellectual resources and prioritize research requirements, fundamental understanding is merged with experimentation theory and modeling. For developing system architecture, the usage of science and mathematics together with techniques of systems' protection from attacks, which are enhanced to prevailing techniques are aimed.
- ii. **Add-on Approach:** It is a sort of a system, which tackle a specific attack for preventing the data's valuable source; where, if there is a requirement, it can add a new feature.
- iii. **Dead-end Approach:** This is an approach that is the overturn of the add-on in which once the approach is presented, no updating or alteration could occur.
- iv. **Game-Changing Approach:** It ensures that uniform SL will be offered across the ecosystem as per the user requirements; hence, the complete computing environment is beneficial.

1.3.2 Cyber Security in Various Domains

In Cyberspace, information's (a) confidentiality, (b) integrity, along with (c) availability are ensured by CS. CS includes several other domains' coordination for guaranteeing security although it is a single term. In figure 1.1, the relation betwixt several domains is delineated.

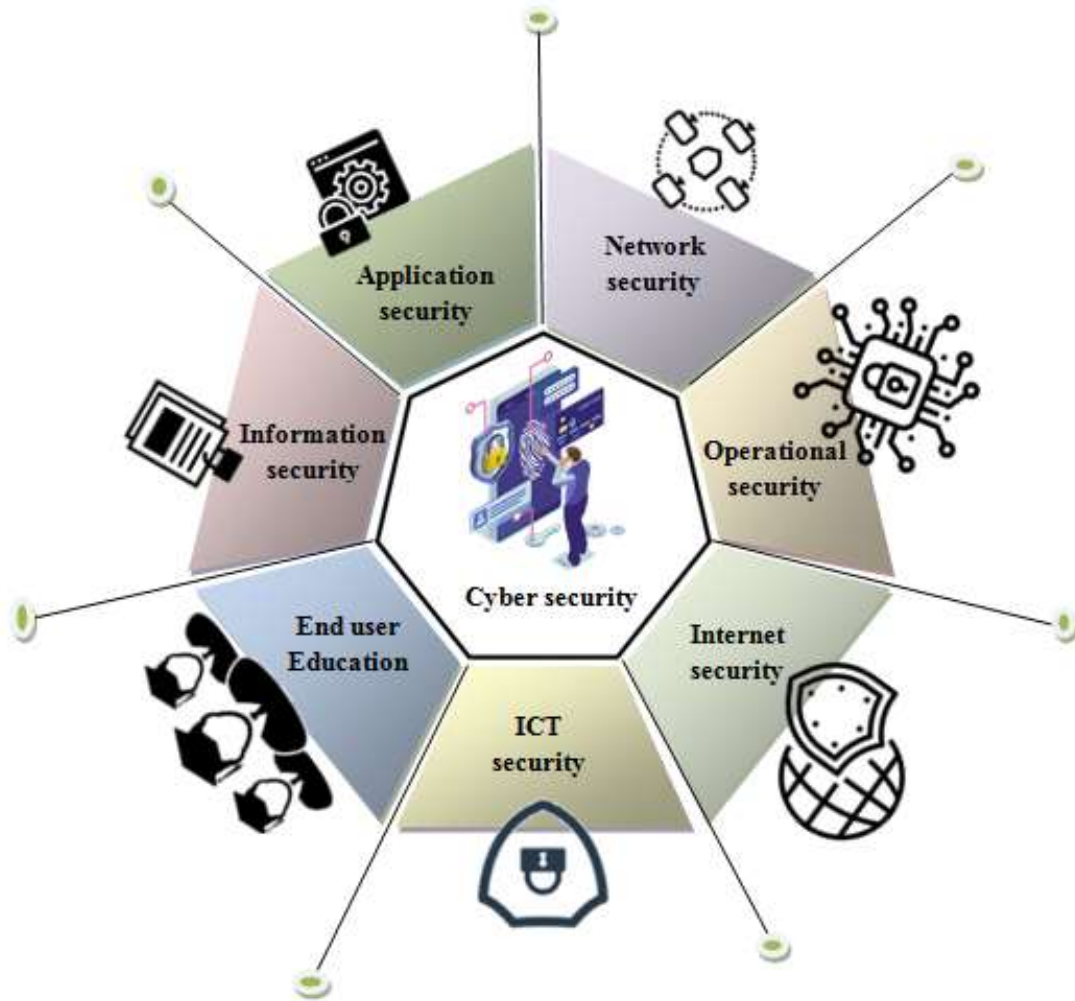


Fig. 1.1: Various Domains of CS

1. To increase an application's security, security testing applies a variety of methods. This is frequently accomplished by keeping an eye on the program and identifying, resolving, and avoiding security flaws. Application security is the implementation of multiple defenses into all software and services used within an organization to guard against a wide range of threats. To decrease the likelihood of any illegal

access or alteration of application resources, it is required to create secure application structures, develop secure software, design strong data input validation, undertake threat modeling, and do other duties.

2. A set of processes or practices for maintaining (1) confidentiality, (2) integrity, along with (3) availability of business data as well as information in several outlines is termed information security.
3. Network security is a procedure created to safeguard the network's usability and integrity as well as to offer protected access to the network's contents. Hardware and software components are always a part of network security. Network security is the practice of using both hardware and software methods to protect the infrastructure and network from unauthorized access, interruptions, and misuse. To defend an organization's assets from both internal and external attacks, network security is crucial.
4. Operations security is the process of locating and defending unclassified essential information, which is frequently alluring for the rival or enemy to obtain accurate information. It also discusses the methods and options utilized to manage and protect digital assets. This covers the policies that control where and how data may be transferred, as well as the privileges users, have while accessing a network.
5. To ensure the online transaction's security, Internet security encompasses several implemented security processes. Protecting browsers, networks, and operating systems, together with other applications of attacks is included in it by making exact rules as well as regulations.
6. The capability for securing Confidentiality, Integrity, together with the accessibility of an organization's digital information property is termed ICT security.
7. The need for end-user knowledge is greatest since human beings are the weakest link in the cybersecurity chain. It addresses people, the unpredictable element in cyber security. Anyone who disobeys good security practices runs the risk of unwittingly introducing a virus into an otherwise protected system. Users must be instructed to remove suspicious email attachments, stay away from putting in unidentified USB devices, and other important lessons for a company to be secure. Nearly 90% of cyberattacks are driven by human behavior, and 50% of cyberattacks are caused by user ignorance of cybersecurity concerns.

1.4 Network Attack Detection and Prevention Techniques

For identifying, defending, and recovering from network assaults, security along with defense systems are designed. The three goals of NS systems are confidentiality, availability, and integrity. For detecting, and preventing network threats or a combination of both, network ID and prevention methodologies could be categorized as grounded on the system [14]. IDS, along with Intrusion Prevention Systems (IPS) are the two categories of it [15].

1.4.1 Intrusion Detection System

It is also termed Network-centric IDS (NIDS). The malicious network activities are checked by this system along with notifying officials if the detected attack with no prevention abilities [16]. For detecting threats, there are '2' techniques wielded by IDS; they are, Signature- and anomaly-centric detection. For determining suspicious events, signature-centric processes are implemented for detecting just known threats depending on a database with a list of pre-prevailing characteristics of known attacks [17].

A network intrusion detection system (IDS) uses integral intrusion signatures to detect any malicious activity that might damage your network. IDS is a method or program designed to safeguard networks against vulnerability exploitation. It gives you the ability to respond quickly and thwart harmful, spoof, and unauthorized network packets from infecting your target systems. An efficient IDS program keeps track of all incoming and outgoing traffic, keeps tabs on the data packets that traverse the network, and alerts the user if the traffic deviates from the planned course. One can take preventative measures to thwart prospective infiltration risks by being alerted in advance of them.

However, a poorly set up or inefficient IDS also generates false alarms for many kinds of network traffic activity. To achieve complete enterprise network security, innovative and intelligent software must be implemented to convert existing intrusion detection capabilities into intrusion prevention capabilities. Most intrusion detection programs look for well-known attack signatures or anomalous deviates from predefined norms. The OSI (Open Systems Interconnection) model's protocol and application layers are then contacted to do more research into these strange network traffic patterns.

To serve as a detection system, an IDS is implemented within your network architecture outside of the real-time communication band (a channel linking the information transmitter and receiver). Instead, it employs a SPAN or TAP port for network monitoring and analyses

a copy of inline network packets to make sure the streaming traffic is not counterfeit or otherwise fabricated (acquired by port mirroring). The IDS efficiently identifies compromised components such as Xmas scans, DNS poisonings, malformed data packets, and more that have the potential to impair the functioning of the whole network.

There are four fundamental categories of intrusion detection systems based on the different mitigation techniques employed to identify suspicious behavior. Following is a description of the many types of intrusion detection systems:

1. **Network Intrusion Detection System (NIDS):** NIDS are placed at a preset point on the network to monitor all network traffic. It observes every incoming and outgoing subnet communication and contrasts it with a database of known attacks. The administrator can get a warning as soon as an assault is discovered or strange behavior is recognized. An example of a NIDS in use is installing one on the subnet where firewalls are to monitor for attempts to breach the firewall.
2. **Host Intrusion Detection System (HIDS):** HIDS tracks intrusions on various hosts or devices linked to the network. A HIDS just monitors the device's incoming and outgoing packets, alerting the administrator to any odd or malicious activity. It contrasts the most recent and prior snapshots of the system files. The administrator receives a notification to investigate any potential changes or deletions to the analytical system files. An example of HIDS usage is with mission-critical equipment whose layout is not expected to change.
3. **Protocol-based Intrusion Detection System (PIDS):** A protocol-based intrusion detection system is made up of a system or agent that regularly sits at the server's front end and controls and interprets the protocol used by users and devices to communicate with the server (PIDS). It makes an effort to protect the web server by continually monitoring the HTTPS protocol stream and accepting the related HTTP protocol. The system would need to be hosted within this interface to use HTTPS, as HTTPS isn't secured and doesn't instantly reach the web presentation layer.
4. **Application Protocol-based Intrusion Detection System (APIDS):** A server cluster frequently houses a device or agent known as Application Protocol-based Intrusion Detection System (APIDS). It recognizes intrusions by monitoring and analyzing communication on application-specific protocols. For instance, this would record the SQL protocol that the middleware expressly uses when speaking with the database of the web server.

5. **Hybrid Intrusion Detection System:** Combining two or more intrusion detection system approaches results in a hybrid intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network data to get a complete view of the network system. Hybrid intrusion detection systems are more effective than other intrusion detection systems. Prelude provides a demonstration of hybrid IDS.

The two main methods of threat detection used by intrusion detection systems are signature-based and anomaly-based. These methods alert network management to possible threats. Finding known threats is frequently where signature-based detection is most useful. It works by using a pre-programmed list of known threats and associated signs of compromise (IOCs). A pattern of behavior that commonly precedes a malicious network attack, malicious domains, recognized byte sequences, file hashes, or even the subject line of an email can all be considered IOCs. A signature-based IDS keeps track of the packets traveling over the network and examines each one against a database of known IOCs or attack signatures to look for any unusual behavior.

Anomaly-based intrusion detection systems, on the other hand, can alert when they spot unidentified strange behavior. Instead of searching for known threats, a machine learning-based anomaly-based detection technique teaches the detection system to recognize a normalized baseline. The baseline depicts the system's typical behavior, and all network activity is compared to it. An anomaly-based IDS simply recognizes any unusual behavior to raise alarms as opposed to looking for known IOCs.

With an anomaly-based IDS, anything that differs from the current normalized baseline, like a user trying to log in outside of normal operating hours, new devices being introduced to a network without consent, or a flood of new IP addresses trying to connect to a network, will potentially raise a flag for concern. This has the disadvantage of labeling many innocuous behaviors as deviant even when they are not malevolent. The full investigation of all possible danger alarms may need more time and money due to anomaly-based intrusion detection's higher propensity to generate false positives.

Anomaly-based intrusion detection may have a disadvantage, yet it can find zero-day vulnerabilities that signature-based detection misses. Only known, current threats are included in signature-based detection. In contrast, it also processes information quickly and detects known assaults with greater precision. These two methods of detection have benefits and drawbacks that, in most cases, go well together, and they are frequently utilized together for maximum effectiveness.

1.4.2 Intrusion Prevention System

It is also termed ID and Prevention Systems (IDPS). For the existence of illegal or rogue control points, which are detected regarding changes in behavior, the network is scanned continuously [18]. For tackling the threats along with defending the system, the system automatically takes countermeasures. Keeping malicious packets along with attacks as the routing injury is the key goal of an IDPS [19]. When analogized to IDS, the IDPS is more effectual since it not just recognizes threats but is capable of taking action beside them. For detecting any suspicious activities and Host-centric IDPS (HIDPS), which are wielded to check host activities, there are two kinds of IDPS like Network-centric IDPS (NIDPS), which evaluate the network protocol.

An automated network security tool called an intrusion prevention system (IPS) is used to track and address possible threats. Similar to an intrusion detection system (IDS), an IPS analyses network traffic to identify potential threats. Intrusion prevention systems automatically react to threats based on established criteria specified by the network administrator due to the speed with which an exploit may be implemented after an attacker has obtained access.

An IPS' primary duties include spotting suspicious activity, recording pertinent data, making an effort to stop it, and then reporting it. Firewalls, antivirus programs, and anti-spoofing programs are all components of an IPS. Companies will use an IPS for these additional objectives in addition to identifying problems with security rules, monitoring current threats, and deterring people from violating security regulations. IPS are now a crucial part of all significant security systems in contemporary businesses.

To act as an additional filter for harmful activities, intrusion prevention systems are typically installed behind a firewall. Since intrusion prevention systems are installed in-line, they may analyze all network traffic flows and take automatic action. Administrators may be informed, risky packets may be dropped, malicious activity's source address may be blocked, and connections may be restarted, among other things. It is crucial to remember that an effective intrusion prevention system needs to be efficient to prevent impairing network functionality. Furthermore, intrusion prevention systems need to operate swiftly and precisely to detect malicious activities in real-time and prevent false positives.

The two most common techniques for identifying malicious activity by intrusion prevention systems are statistical anomaly-based detection and signature-based detection. A dictionary of distinctively recognizable signatures is contained in the code of each exploit and is used

by intrusion prevention systems as part of their signature-based detection technique. Both exploit-facing and vulnerability-facing signature-based detection techniques are used by intrusion prevention systems. While vulnerability-facing methods try to identify malicious activity by detecting specific vulnerabilities, exploit-facing methods detect malicious activity based on typical attack patterns. On the other hand, intrusion detection systems that rely on statistical anomaly-based detection randomly sample network traffic and compare the samples to a predetermined performance threshold.

Most intrusion prevention systems employ one of the three detection methods: stateful protocol analysis, statistical anomaly-based, or signature-based.

1. **Signature-based detection:** Signature-based IDS keeps track of network packets and compares them to "signatures," or planned attack patterns. Patterns for normal behaviors and deviant behaviors are developed using data from the history of operations and transactions carried out by authorized users and hackers in networks. It is possible to distinguish between authorized users and hackers by comparing these patterns or signatures with the existing users' activity patterns. The main drawback of this strategy is that we cannot tell if a person is permitted or unapproved if their signature or pattern is new and there are no previous examples of their signature or pattern in the database.
2. **Statistically-based anomaly-based detection:** An anomaly-based IDS will track network traffic and evaluate it in comparison to anticipated traffic patterns. The baseline will show what is "normal" for that network, including the protocols that are utilized and the types of packets that are typically sent over it. A false positive alarm for legal usage of bandwidth may be generated, nevertheless, if the baselines are not set up properly.
3. **Stateful protocol analysis detection:** This method identifies protocol violations by contrasting actual events with previously created activity profiles of usual activities. The requirement to keep state information (information about a connection to a prospective attack) on such a system presents a potential vulnerability. Stateful protocol analysis refers to this information gathering. The host and remote computer connections are checked against state table entries when an IDPS receives a packet. The source IP address and port, destination IP address and port, and protocol are all kept in a state table that keeps track of connections between machines. Additionally, the event horizon of the attack, also known as the event horizon, must be maintained by the IDPS. When long attacks,

such as those that last from user logon to user logoff, occur, the IDPS might not be able to maintain the state information for a long enough time, which would allow the attacker to bypass the system. Maintaining this information might require an IDPS to review numerous packets of data. Stateful protocol analysis can use some techniques, including:

- i. **Communication rate monitoring** allows the IDPS to halt and restart all TCP traffic if it notices an unexpectedly large increase in traffic, such as that brought on by a denial of service (DoS) attack.
- ii. **Protocol state monitoring (stateful packet filtering):** By implementing stateful packet filtering similar to what firewalls do, some IDPSs can go beyond matching packet signatures. The IDPS keeps track of the connection's status and only permits packets to reach the internal network if a connection has already been made.
- iii. **Dynamic Application Layer Protocol Analysis:** An attacker may occasionally be able to get around an IDPS by employing an Application Layer Protocol on a non-standard port. In a dynamic application layer protocol analysis, the protocol in use is first detected, and then analyzers that can spot apps that don't use conventional ports are turned on.
- iv. **IP packet reassembly:** Some IDPSs are capable of reassembling broken IP packets to stop them from reaching the internal network.

Four main categories can be used to classify intrusion prevention systems:

- i. **Network-based intrusion prevention system (NIPS):** Looks for any suspicious traffic by analyzing protocol behavior throughout the whole network.
- ii. **Wireless intrusion prevention system (WIPS):** Looks for any suspicious traffic by analyzing network protocol activity throughout the whole wireless network.
- iii. **Host-based intrusion prevention system (HIPS):** An additional software program that monitors a single host for suspicious behavior and analyses activities taking place there.
- iv. **Network behavior analysis (NBA):** This technique looks at network traffic to find risks that cause unusual traffic patterns. Distributed denial of service attacks, different types of malware, and policy violations are the most frequent

threats that use pattern matching to find attacks. An easy way to evade detection is to make a little adjustment to the attack architecture.

To ensure dependable and safe information exchange across many organizations in today's networked business environments, a high level of security is required. An intrusion prevention system acts as a flexible safeguard for system security after traditional technologies. Lower expenses and more performance flexibility result from the ability to stop invasions using an automated approach without the need for IT intervention. Since cyberattacks will only get more sophisticated, defense systems must evolve to thwart them.

1.5 Intelligent Network Attack Mitigation Techniques to Detect Unknown Threats

For detecting and preventing cyber threats, technical safeguards multitude is present for organizations. Misuse and anomaly detection are wide categories of concepts. For determining notorious attack patterns elucidated by rules the first one was aimed; while, for recognizing unusual activity patterns, the second one was designed [20]. Here, various ML techniques are wielded like classification, and regression, together with clustering methodologies namely Logistic Regression (LR), Decision Trees (DT), et cetera. For depicting the decision-making process sequences in a tree, Random Forest (RF), which is an ensemble of DT, is deployed. Owing to distinctly classifying the data points by constructing a hyperplane in an n-dimensional space in which the features are depicted by n, the Support vector machine (SVM) was hugely wielded. Naïve Bayes (NB), which is another ML classifier that was hugely deployed. In the end, for classification, the K-Nearest Neighbour (KNN) along with K-means clustering, which is an unsupervised approach, was wielded by a few researchers.

Owing to the dependence on rule sets, the major prevailing system could be categorized as misuse detection. Blacklist- and whitelist-centric techniques are the classifications of rule-centric solutions; while, signature- and heuristic-centered are the divisions of blacklist-centric systems. Grounded on threat patterns like malicious byte sequences, the signature-centric system finds threats; whereas, centered on expert-centric probabilistic rule sets, which portray malicious pointers, heuristic methodologies detect threats. Susceptibility to elevated false positive rates is a huge demerit even though heuristic approaches regularly complement signature-centric solutions. For using Machine Learning (ML) as an option along with a more correct scheme to current methods to sense unknown threats of known

threats, interest has developed in the security community for surpassing challenges like the constrained facility to perceive mysterious bullying by signature-centric together with absence detection precision by behavior-centric methodologies. Hence, for attack detection, DL methodologies are proposed.

1.6 Research Motivation

For organizations, cyber risk is a major concern. Criminals, amateur hackers, government actors, hacktivists, and other adversaries are included in the cyber system. Recently, media attention to CS issues has grown dramatically. The drawback is that most urbanized network attack detection methodologies rely on pre-defined signature-centric attacks. Since the attackers detected novel ways to exploit NS, the attackers' database has to be updated constantly. The predictive accuracy of detecting along with classifying network attacks is improved with the evolution of intelligent-centric methodologies like ML and DL. Hence, intelligent-based was wielded in NS, which is a thriving field for research.

1.7 Research Problem

For protecting the network and data, cyber-attack along with threat intelligence work together. For understanding a cyber-attack in an organization's network and handling this cyber-attack efficiently, it is necessary to utilize suitable cyber-attack methodologies. By installing along with running anti-virus software that could consume huge computer memory as well as hard disk space, slowing down the computer, anti-virus software draws down the PC or network. For securing a network from being attacked, cyber threat intelligence can work as a preventive measure. Since that provides an enhanced understanding of the attack's nature that could be valuable knowledge for improving cyber threat intelligence, both methodologies must work together for securing the cyber attack.

1.8 Research Queries for the Study

For the literature review, the following research questions were derived and were concerned with further depicted research issues,

- Q1. What are the several tactics to detect along with mitigating cyber-attacks?
- Q2. What are the advanced ways to impose a system to detect along with mitigating cyber-attacks?

- Q3. What are the study gaps in mitigation techniques and cyberattack detection (CAD)?

1.9 Objective of the Work

Owing to the developed digital technologies wielded by hackers, cyber-attacks are augmenting quickly. For cyber-attacks and CS, several methodologies have been proposed; however, have high energy consumption, FPR rate, along with Backup capabilities. This research is done on CAD. The main aim of this effort is to develop efficient cyber-attack mitigation techniques, for detecting and mitigating attack node and their origin as early as possible at the receiver side through an effective novel encryption mechanism.

The problem was detected securely along with the objectives defined by the extensive literature survey on CAD with a Bait-based approach for mitigation. For generating a proficient methodology, the subsequent notions should be considered.

1. To present the deep ensemble methodology to detect the existence of attack; in addition, to alleviate it by employing the Bait.
2. To process the Bait to mitigate the attackers of the network.
3. To process an SHP-ECC to mitigate the attacker as of the network.
4. To measure the proposed system's feasibility regarding particular performance metrics against other prevailing systems.

1.10 Thesis Contribution

The implementation of the research work can be discussed in two different stages namely the BReLU-ResNet model based cyber-attack detection and mitigation system, and the SHP-ECC model based data encryption and data decryption.

- The first part of the work is the model to detect and mitigation of cyber-attacks using BReLU-ResNet algorithm. In the proposed model, initially, the entire training data is pre-processed. From the input training dataset, features are extracted. To select the significant features, the feature is optimized by employing TWMA. By deploying the BReLU-ResNet, the features are trained. Implementing the skip connection for offering input for the layer indiscriminately for merging the data flow for eradicating data loss and gradient vanishing problems is the goal of Residual neural networks (ResNet). Reducing noise is averaging this system; in

addition, training accuracy and generalization are maintained by it. Achieving enhanced training accuracy and approximate level of traversal is the proficient way of enhancing maximum label data. The data is classified into attack and normal data. By employing BAIT, the Source IP Address is saved into a secure log file if the data is attack data

- The second part of the work is the SHP-ECC model based data encryption and data decryption. The normal data which is classified by the proposed BReLU-ResNet algorithm is ready for the transmission. By utilizing the ESHP-ECC, the data is encrypted in Data Transmission. By employing ED, the shortest path distance is analyzed. By deploying the DSHP-ECC, the data is decrypted in the Destination. In the Security Log File (SLF), the testing data is checked in testing. The data is blocked, or attack detection is done if the data's source IP address is present already.

1.11 Organization of the Thesis

The thesis is divided into seven chapters namely

1. Introduction
2. Review of Literature
3. Methodology
4. Result and discussions
5. ABCD Analysis of Cyber Attack Detection and Mitigation Model
6. Conclusion
7. Future scope of the work

Chapter 1: Introduction

This chapter gives an introduction to cyber security. The chapter gives importance to an overview of cyber security. The chapter highlights the various types of cyber-attacks in cyber space. The chapter also highlights the various mechanisms to handle cyber-attacks. The relation betwixt several domains are discussed. The strategies used to detect and prevent cyber-attacks are also discussed in the chapter. The chapter mentions the current research problem. This chapter highlights the objective of the study and the thesis contribution.

Chapter 2: Review of Literature

This chapter gives the list of the various literature studies done on various cyber-attack and detection models. In the literature survey, it is observed that common techniques are used for the detection of cyber-attacks. But while referring to the mitigation of cyber-attacks various algorithms are adopted by different authors. It is observed that the cyber security is still in the research field for improvement. The chapter briefs about the various datasets that can be used to detect and mitigate cyber-attacks. The chapter also highlights the challenges faced by the developers during the implementation of the cyber-attack detection and mitigation models. This chapter gives a brief details about the current approaches which are used in the mitigation and detection of cyber-attacks by using machine learning and deep learning algorithms. The chapter also highlights the research gap.

Chapter 3: Methodology

This chapter deals with the conceptual model of the proposed design and explains the different parts of the model. The chapter explain the algorithms used to compare the proposed model with the prevailing systems. The chapter also deals with how the features are extracted, how the features are selected using TWMA algorithm. The chapter also includes how classification of attack and normal data are made using proposed BReLU-ResNet algorithm. The chapter explains how the data is encrypted and decrypted using proposed SHP-ECC algorithm and also explains the identification of shortest path to transfer the data in-between the source and destination using Euclidian distance algorithm. The chapter describes how the attacks are mitigated using Bait approach.

Chapter 4: Result and Discussion

This chapter deals with the analysis of the proposed model. Here the model is tested using different possible data and the output is found. The performance of the different parts of the model is shown in the table. The data base used to develop the proposed model is described in this chapter. Also this chapter highlights the performance matrix of ANFIS, NN, CNN, and proposed BReLU-ResNet algorithms. The Proposed BReLU-ResNet model is compared with the other prevailing systems using various performance matrices. Similarly, the Proposed SHP-ECC model is compared with the other prevailing systems using various performance matrices. In this chapter the Receiver Operating Characteristic Curve is described with other prevailing algorithms.

Chapter 5: ABCD Analysis of Cyber Attack Detection and Mitigation Model

This chapter gives an analysis of proposed cyber attack detection and mitigation model in terms of Advantages, Benefits, Constraints and Drawbacks with the various performance matrices like sensitivity, specificity, accuracy, precision, recall, F1 measure, False positive rate, False Negative Rate, Matthews Correlation Coefficient matrices. The chapter also describes the analysis of attack detection and mitigation in terms of encryption and decryption time. The ABCD analysis is made based on security level of cyber attack detection and mitigation model.

Chapter 6: Conclusion

This chapter gives concluding remarks with the various benefits of using the model. Several uncertainties might be tackled by the proposed system; in addition, propitious outcomes could be achieved. When weighed against the prevailing techniques, the developed system depicted enhanced performance along with sustains to be dependable and robust. The research will be elaborated for including more superior neural networks along with various kinds of realistic attacks in the future.

Chapter 7: Future Scope of the work

The chapter gives the idea of the further improvements that are possible from this research findings. Finally, the List of References, journal publications, and Annexure is appended to the last chapter.

CHAPTER 2

REVIEW OF LITERATURE

2.1 Introduction

Beyond a set of well-defined requirement specifications and awareness of potential dangers, risks, or other vulnerabilities, CS evaluation and the creation of precise processing tools are needed to prevent CS attacks. For extracting security incidents' insights or patterns of various ML methodologies that encompass but are not constrained by (1) feature reduction, (2) regression evaluation, (3) unsupervised learning, (4) detecting associations; (5) neural network-focused DL methods could be wielded. In CS, that is elucidated in ML systems. These learning approaches might identify anomalies or harmful behavior as well as data-driven patterns of related security issues and make wise decisions for preventing cyber-assaults. A partial but significant shift away from traditional security measures such as user authentication, access control, firewalls, and encryption systems, which may or may not be effective in meeting the needs of online businesses [21-323]. In the circumstance in which ad hoc data management is essential, the domain experts along with security analysts fix these manually [24]. Nevertheless, as augmented CS occurrences in various formats are appearing, fundamental solutions have failed to manage such cyber hazards. Thus, a slew of novel, tedious attacks stimulates along with widespread speedily. Many academics develop "ML techniques" for CS, which are centered on the efficient identification of security insights and current security trends that may be more related, using various data analytics and knowledge extraction models. Handling the cyber issue requires the improvement of flexible and effective security systems, which could react to assaults and updated security rules, to eradicate them on a timely basis intelligently. Diverse associated CS data collected from several sources like networks along with system sources should be evaluated. Those methodologies must be applied; thus, automation should be maximized with minimum to no human intervention. Further, an exhaustive literature survey conducted on CAD and classification algorithms is elucidated.

2.2 Overview of Systematic Literature Review Methodology

A crucial process that provides a solid framework for knowledge expansion is the review of the literature. It makes it simpler to identify areas that require additional research [25].

This project will conduct a thorough evaluation of the literature to present current research suggestions for the creation of a cyber-assault detection and mitigation tool. We used Kitchenham's [26] systematic literature review recommendations to develop a framework for the literature review. The subsections that follow provide an overview of how to conduct a literature review to accomplish the objectives of this study. The next subsections of the literature evaluation framework outline the concerns that studies should consider, how to discover related studies, how to choose studies for the literature overview, how to evaluate reviewed publications, and how to synthesize study findings.

2.2.1 Study-Related Research Questions

The objectives of the literature review guided the development of the following research questions, which addressed the following research concerns:

- Q1. What are the different strategies for spotting and thwarting cyberattacks?
- Q2. What are the most modern techniques for enforcing a model for identifying and thwarting cyberattacks?
- Q3. What are the areas of research that need to be filled in to identify and mitigate cyberattacks?

2.3 Cyber Security Datasets

A variety of data sets are being assembled by many research teams, both for their investigations and to add to public repositories. The datasets now utilized in security are explained in this section using machine learning and artificial intelligence studies.

2.3.1 KDD Cup 1999 Dataset (DARPA1998)

In 1998, MIT Lincoln Laboratory received funding from DARPA and the Air Force Research Laboratory (AFRL) to collect and disseminate the first benchmark data for the assessment of computer network intrusion detection systems. The information received from MIT Lincoln Labs includes the KDD Cup 1999 results in addition to the tcpdump and BSM list files. This dataset was created by Fraley et al. [27] using data from the DARPA'98 IDS evaluation program. This dataset is furthermore recognized as benchmark data for assessing intrusion detection systems. User-to-root (U2R), remote-to-local (R2L), denial-of-service (DoS), and probing are the four main types of assaults covered by the data. In addition, the dataset includes 38 numerical features and 3 content features. The

characteristics comprise the basic TCP connection features, the information features inside a connection that is recommended by domain expertise, and the traffic features estimated within a two-second timeframe. One of the most used data sets to assess the effectiveness of anomaly detection techniques is KDD'99. The KDD dataset is now used in thirty investigations [28–33].

2.3.2 ECML-PKDD 2007 Dataset

The 2007 European Conference on Machine Learning and Knowledge Discovery inspired the creation of the ECML-PKDD 2007 dataset. The ECML/PKDD Discovery Challenge, a data mining contest, was part of the 18th European Conference on Machine Learning (ECML). Table 2.1 lists the characteristics of ECML/PKDD 2007.

Table 2.1: ECML/PKDD Dataset Characteristics

	Testing Set	Training Set
Total Request	70,143	50,116
Valid Request	42,006 (60%)	35,006 (70%)
Attacks	28,137 (40%)	15,110 (30%)
Cross-Site Scripting	11%	12%
LDAP Injection	16%	15%
Command Execution	23%	23%
SQL Injection	18%	17%
Path traversal	18%	20%
XPATH Injection	16%	15%
SSI	12%	13%

Extensible Markup Language is used to define the dataset (XML). Context, class,

and query are the three main components of the sample, and each one is represented by a distinct id throughout [34–41].

2.3.3 ISOT (Information Security and Object Technology) Data set

The ISOT (Information Security and Object Technology) dataset, which mixes many publicly accessible botnets with ordinary statistics, has a 1,675,424 total traffic flow. The Storm and Waledac botnets' French honeynet project provided the data for the malicious traffic in ISOT. Hungary's Traffic Lab Ericson Research provided non-harmful traffic. After that, another dataset produced by Lawrence Berkeley National Lab was integrated with this traffic (LBNL). This collection comprises HTTP web surfing, World of Warcraft, and Azureus BitTorrent client traffic, as well as typical traffic from many different kinds of software. As a result, this traffic represents a sizable large dataset for Ericson Lab. 22 subnets were covered by the LBNL network trace from 2004 to 2005. Additionally, LNBL traffic encompasses five enormous datasets and a medium-sized enterprise network [42].

2.3.4 HTTP CSIC 2010 Dataset

The HTTP CSIC 2010 dataset consists of a sizable number of web requests performed automatically and produced by the CSIC Information Security Institute (Spanish Research National Council). Evaluation of web attack defense methods may be done using the dataset. With 6,000 normal queries and more than 25,000 aberrant requests, this data categorizes HTTP requests as normal or abnormal. The dataset has been divided into three subgroups for convenience: training, anomalous, and testing. Unusual requests refer to a variety of application layer attacks. Three main types of assaults are included in this dataset: static, dynamic, and unintentionally illegal requests. Examples of dynamic attacks include SQL injection, CRLF injection, cross-site scripting, buffer overflows, etc. Attacks using the static technique seek buried resources. These requests cover a wide range of topics, including session IDs in URL rewriting, default files, outdated files, and configuration files. Despite not having a malicious purpose, unintentional unlawful requests violate the web application's usual behavior and do not follow the same structure as ordinary parameter values [43].

2.3.5 CTU-13 (Czech Technical University) Dataset

The CTU-13 dataset is made up of 13 different malware samples that were discovered in a real-world network setting. Actual mixed botnet traffic will be captured by this dataset.

Botnet traffic was produced by infected hosts, whereas regular traffic was produced by verified normal hosts. Last but not least, background traffic is the remainder of the traffic whose exact nature is unknown. Thirteen separate botnet sample captures often referred to as scenarios, are included in the CTU-13 dataset. Each of the situations was carried out using a specific malware that utilized multiple protocols and performed some tasks. One of the largest and most comprehensive datasets ever created was by the CTU University of Prague in the Czech Republic in 2011. Starting with the CTU-13 dataset, Grill et al. [44] proceeded. Using the CTU-13 dataset, this paper evaluated various botnet detection approaches and developed a unique error metric [32]. Using the BClus, The Cooperative Adaptive Mechanism for Network Protection (CAMNEP), and BotHunter algorithms, this study assessed the effectiveness of botnet identification. This dataset has been applied in some studies. Grill et al. (2014) [44] used this data set to evaluate the performance of the local adaptive multivariate smoothing (LAMS) model for the identification of anomalous NetFlow. The proposed methodology has reduced the number of false alarms generated by anomaly detection on intrusion detection systems [44]. Table 2.2 with attributes contains the scenario's specifics. This dataset has the benefit of being meticulously annotated and having been collected in a controlled setting [41][45-49].

Table 2.2: Data volume for each botnet scenario [50].

Dataset	Duration (h)	NetFlow	Size (GB)	Bot name	Number of bots	Botnet flow
1	4.75	1,309,792	73	Rbot	10	106315 (8.11%)
2	11.63	129,833	37.6	Virut	1	695 (0.53%)
3	5.18	2,753,885	94	Neris	10	179880 (6.5%)
4	4.21	1,121,077	53	Rbot	1	1719 (0.15%)
5	4.21	1,808,123	60	Neris	1	18839 (1.04%)

6	66.85	4,710,639	121	Rbot	1	26759 (0.56%)
7	0.26	107,252	5.2	Rbot	3	8161 (7.6%)
8	0.38	114,078	5.8	Sogou	1	37 (0.03%)
9	16.36	1,925,150	34	Virut	1	38791 (2.01%)
10	6.15	2,824,637	52	Neris	1	39933 (1.41%)
11	1.21	325,472	8.3	NSIS.ay	3	2143 (0.65%)
12	2.18	558,920	30	Menti	1	4431 (0.79%)
13	19.5	2,954,231	123	Murlo	1	5052 (0.17%)

2.3.6 The ADFA Datasets

The majority of benchmark data sets that are currently accessible in the field of host-based anomaly detection, such as the intrusion detection data sets from UMN [51] and DARPA [52], were assembled more than 10 years ago and do not correctly represent the properties of modern computer systems. The Australian Defense Force Academy at the University of New South Wales published the Australian Defense Force Academy Linux Dataset in 2013. The ADFA dataset (Linux dataset) was created on an Ubuntu Linux 11.04 host OS with Apache 2.2.17 and PHP 5.3.5 to test host-based intrusion detection solutions. Releases included FTP, SSH, MySQL 14.14, and TikiWiki. System call traces from both trustworthy and malicious Linux-based systems are included in this collection. While performing a sampling step, the host that is set up to mimic a contemporary Linux server records the system call traces of genuine programs that are running often. The host is thereafter the target of a variety of assaults, including Hydra-FTP, HydraSSH, Adduser, Java-Meterpreter, Meterpreter, and Webshell, each of which generates 8–20 aberrant traces. Table III displays the ADFD-makeup.

Table 2.3: The elements of ADFD-LD [50].

Trace Type	Number	Label
Training	833	Normal
Java-Meterpreter	125	Attack
Meterpreter	75	Attack
Hydra-SSH	148	Attack
Validation	4373	Normal
Adduser	91	Attack
Hydra-FTP	162	Attack
Webshell	118	Attack

The ADFA dataset is meant to take the role of the existing benchmark data sets, which have fallen short of adequately capturing the traits of modern computer systems.

2.3.7 UNSW-NB15 Dataset

The Australian Centre for Cyber Security's Cyber Range Lab's IXIA PerfectStorm instrument generated the UNSW-NB 15 data set (ACCS). This dataset contains traffic records from a DDoS attack that lasted for around 1 hour in 2007 [53–57]. Nine main attack types are covered by this dataset: Fuzzers, Reconnaissance, DoS, Generic, Exploits, Backdoors, Shellcode, and Worms. The attack data was used to create a report using the IXIA PerfectStorm program, which is used to categorize this dataset. Table 2.4 lists the many contemporary attack types included in this dataset.

Table 2.4: UNSW-NB15 Dataset Specifications [53].

Category	Testing set	Training set
----------	-------------	--------------

Normal	37000	56.000
DoS	4089	12.264
Generic	18.871	40.000
Backdoor	583	1.746
Shellcode	378	1.133
Reconnaissance	3.496	10.491
Worms	44	130
Exploits	11.132	33.393
Analysis	677	2.000
Fuzzers	6.062	18.184
Total Records	82.332	175.341

This dataset has 49 characteristics. 12 models were created after the use of Argus and Bro-IDS tools to extract features. Only five categories flow features, fundamental features, content features, temporal features, and further produced features are used to classify characteristics. This dataset, when compared to previous datasets, has many attack families that, in the end, resemble contemporary minimal footprint attacks [58].

2.4 Cyber Security

The definition of CS is the maintenance of the Integrity, Confidentiality, and Availability (ICA) of computing benefits that belong to an organization or connect to the network of another organization [59]. For securing the information, networks, along with data against internal or external threats, practical measures are encompassed in CS. Networks, servers, intranets, together with computer systems are secured by CS professionals. Just authorized

individuals have access to information, which is guaranteed by CS [60]. To the victim organization and its clients, a breach in any CS causes a few forms of financial and non-financial losses; hence, the CS's purpose is to secure against those breaches [61].

Saravanan A et al. (2019) [62] elucidated CS and the 5th generation of cyber-attacks. Since domain knowledge was required about the attacks along with the capability of analyzing the threats' possibility, guaranteeing CS was a tedious task. A fresh vulnerability was leveraged by more than 25% of attacks. Even after the arrival of the 5th generation, most organizations hadn't evolved along with were still employing 2nd or 3rd generation security. Thus, awareness amongst organizations and security solutions should be maximized.

Victoria Wang et al. (2020) [63] described the CS breaches, practices, along with the ability of internet banking in Nigeria. An online survey was conducted with 100 seasoned experts who work in the banking and financial industries in Nigeria. A total of 80 participants agreed or strongly agreed that keeping private account information to themselves and signing up for transaction notifications on the activities were effective protective measures. The management of appropriate reactions to CS threats presented significant difficulties for Nigerian banks at the time.

Shaikha Hasan et al. (2021) [64] analyzed the CS readiness of organizations along with its influence on performance. For preventing and combating cyber-attacks, the issue of developing CS was faced by organizations; however, there was an absence of discussion of factors affecting the organizations' CS awareness/readiness from a holistic perspective. The organizational security performance was positively impacted by the CS readiness; thus, financial and non-financial performance was impacted positively. Government support for CS readiness's negative effect might not be generalized.

2.4.1 Cyber Security Challenges

The CS, along with economic security plans, is a crucial part of the nation's overall national security. Each organization requires a secure analyst in that the system might be extremely safe with the increase in cyber-attacks. These security analysts deal with some CS-related challenges, such as protecting the servers of commercial firms and safeguarding the personal information of governmental organizations [65]. Data security plays a vital role in information technology. One of the key challenges is data security [66]. In the development

of CS, Block Chain (BC) technology has a proven track record; hence, it is wielded by the biggest tech companies including Google [67]. A few significant CS issues are,

- Ransomware evolution
- BC revolution
- IoT threats
- AI expansion
- Server fewer apps vulnerability

Alex R. Mathew et al. (2019) [68] delineated CS via BC technology. In several industries, BC has seen adoption; particularly in finance via the usage of crypto currencies. Challenging security loopholes, which were beyond the scope of conventional security tools, could be taken by BC. Any stolen data might be unusable and 3rd parties couldn't be able to alter it as just '2' parties in the communication would be able to read along with manipulating the data.

Lee et al. (2020) [69] expounded on the Internet of Things (IoT) CS along with IoT cyber risk management. Minimizing CS risk for organizations as well as users via the protection of IoT assets and privacy is the purpose of IoT CS. When weighed against Option 2, Option 3 generated a lower total cost by employing the LP even with a less investment cost. In complicated IoT cyber resource allocation decisions, the LP model's efficacy was depicted. Nevertheless, security protection technologies weren't deployed by 26% of organizations.

2.5 Review of Machine Learning Techniques in Cyber-Security

Data from several sources are merged by data security along with correlations within the data. To evaluate the data, several techniques might be wielded by the security analysis tool. Prevailing rule-centric, statistical analysis, and ML are encompassed. ML security to identify anomalies is effective in terms of accuracy and minimizing feature dimensions based on the DT classification with Feature Selection (FS). The "six" ML approaches that are taken into consideration are RF, SVM, NB, DT, Artificial Neural Network (ANN), and Deep Belief Network (DBN).

In 2016, Nadeem et al. [70] employed Deep Belief Nets (DBNs) to discover malware. Downloadable examples of the PE files are available online. Compared to feed-forward neural networks with random weight initialization, DBNs are made to be less prone to

overfitting. This is accomplished via an unsupervised pre-training technique. DBNs surpass all other learning approaches, including SVM, KNN, and decision trees, in terms of classification results because they can learn from fresh unlabeled data. The accuracy rate of the approach is 96.1%.

Zhao et al.'s 2017 [71] research focuses on the challenges in intrusion detection brought on by a significant volume of duplicated data, a protracted training period, and the simplicity of sliding into a local optimum. We suggest a probabilistic neural network- and deep belief network-based intrusion detection system (PNN). The high dimensional data are transformed into low dimensional data using DBN nonlinear learning while preserving the fundamental characteristics of the original data. Then, to get the optimum learning performance, the number of hidden nodes in each layer is optimized using the particle-swarm optimization method. PNN is used to categorize low-dimensional data. For testing, the KDD CUP 99 dataset was used. The experimental results had 99.14% accuracy, 93.25% precision, and 0.615% FAR, respectively.

Alrawashdeh et al. [72] implemented their method for optimizing the deep network in 2017. The method relies on a soft-max Logistic Regression with a deep belief network as its foundation. Using the enhanced pre-trained data, the multi-class Logistic Regression layer was trained across 10 epochs to enhance the performance of the network as a whole. On the whole 10% KDD Cup 99 test dataset, our technique produced a low false negative rate of 2.47% and a detection rate of 97.9%.

Vishwakarma et al. [73] presented research on the effectiveness of the KNN-ACO, BP Neural Network, and Support Vector Machine for comparative comparison utilizing conventional performance evaluation criteria in 2017. Studies on the effectiveness of these algorithms, the AkNN intrusion detection approach based on the KDD Cup 99 dataset, and pre-training the dataset using ACO. The method's accuracy rate is 94.17%, and the FAR as a whole is 5.82%. This approach makes use of a very little dataset.

In their research, Hajisalem et al. [74] 2018 developed a hybrid classification strategy using an artificial bee colony (ABC) and an artificial fish swarm (AFS). To choose features, they applied Fuzzy C-Means Clustering (FCM) and Correlation-based Feature Selection (CFS) methods. To differentiate between normal and anomalous records, they built If-Then rules using the CART technique in the last stage. They used the NSL-KDD and UNSW-NB15 data sets to test their approach, and they found that it had a 99% accuracy rate.

Karimipour et al. [75] proposed in 2019 the unattended identification of anomalies based on the statistical correlation between readings. The goal of the authorized model was to provide huge intelligent networks with a configurable anomaly detection engine that could differentiate between a real breakdown, a disorder, and a cunning hack. The suggested method employs symbolic dynamic filtering to lower computational complexity and reveal causal relationships between subsystems. The effectiveness of the technique under a range of operating conditions is supported by simulation results for the IEEE 39, 118, and 2848 bus designs. Less than 2% of positive and false-positive rates, which make up 99% of all positive rates, are indeed positive, according to the findings.

Kanimozhi et al. [76] categorized the CSE-CIC-IDS 2018 data set in 2019 using ANN, RF, k-NN, SVM, ADA BOOST, and NB machine learning approaches. He proposed a feature selection method based on the Non-Dominated Sorting Genetic Algorithm II and logistic regression (NSGA-II). The suggested method was put to the test using the Non-Dominated Sorting Genetic Algorithm Binomial Logistic Regression (NSGA2-BLR) and Non-Dominated Sorting Genetic Algorithm Multinomial Logistic Regression (NSGA2-MLR) techniques. The best subsets might be classified using C4.5, Random Forest (RF), and Naive Bayes (NB) algorithms. The study made use of the NSL-KDD, UNSW-NB15, and CIC-IDS2017 data sets. The categorization had a 99.97% success rate.

Defu et al (2019) [77] developed ML-centric attack detection meant for power systems, which were trained by deploying data along with logs acquired by Phasor Measurement Units (PMUs). The accuracy might be maximized by the data processing; in addition, 37 diverse kinds of power grid behaviors might be detected by the AWW. The feature development engineering was accomplished. With the RF being chosen as AdaBoost's simple classifier, the data was sent to several ML models. For equating the presented system to other ones, several comparison criteria were deployed. For accuracy and identification rate, the system could attain 93.91% and 93.6%, which is superior to the '8' depicted methodologies.

Wei et al. devised a recovery technique for the optimal re-closure of the trickling transmission lines in 2020 [78]. To enable the approach to adapt to unexpected attack situations and to adopt real-time decision-making skills, a framework for deep reinforcement learning (RL) has been built. During the assault-recovery phase, an environment has been developed for simulating energy device dynamics and producing training data. This data was used to train the sophisticated RL algorithm to calculate the

ideal lock-up time. Numerical results show that, depending on the situation, the strategy used would reduce the impacts of a cyberattack.

To identify and mitigate LR-DDoS attacks in SDN systems in the year 2020, Perez et al. [79] suggested a flexible modular framework. Six machine learning models were used to train the intrusion detection system (IDS) in the framework, and the DoS dataset from the Canadian Institute of Cybersecurity was used to evaluate the system's overall efficacy. The results of the investigation indicate that, despite the difficulties in identifying LR-DoS assaults, this strategy has a 95 percent detection rate. The Mininet digital system's OS controller is utilized to keep the simulated environment and actual production networks as similar as is practical. The intrusion prevention detection device mitigates any attack that the intrusion detection system detects inside the testing topology. This shows how proficient the system is at identifying and shielding against LR-DDoS attacks.

Ban Mohammed Khammas (2020) [80] proffered a fresh technique grounded on static analysis for detecting ransomware. Dispensing of the disassembling process by direct extraction of features as rare bytes with the utilization of common pattern mining that maximizes the detection speed is an important characteristic. A gain Ratio approach was used for FS that suggested that 1000 features were the ideal number for detection. In the proposed investigation, the impact of the tree effect and seed numbers on ransomware detection was thoroughly reviewed. In terms of time and accuracy, the 100-number trees with a seed of 1 generated the best results. This technique has a high accuracy rate for ransomware detection of 97.74%.

Yasir Ali Farrukh et al (2021) [81] presented a 2-layer hierarchical ML with 95.44 % precision for enhancing cyber-attack detection. For distinguishing betwixt the '2' modes of operation, the 1st layer is deployed; normal state or cyber-attack. For categorizing the state into various kinds of cyber-attacks, the 2nd layer is deployed. To target the aimed layer's task, an opportunity was offered; thus, enhancement is done.

An SVM-centric PHY-layer authentication was created by Sumathy S et al in 2021 [82] to identify potential security breaches in 5G wireless communication at the physical layer. For maximizing the rate of authentication, it is deployed with test features. With test statistic features, the detection rate is enhanced. On Multiple-Input Multiple-Output (MIMO), the system was applied. On every attack, the presented system attains the highest detection rate.

Iqbal H Sarker et al (2021) [83] evolved “Cyber Learning”, an ML-centric CS modeling with correlated- FS, along with a comprehensive empirical evaluation of several ML-centric security models’ efficacy. Binary classification and multi-class classification models were taken into consideration to identify abnormalities as well as various types of cyber-attacks. The "10" ML methods, including linear discriminant analysis, NB, LR, stochastic gradient descent, KNN, SVM, DT, RF, and intensive Gradient Boosting, were used to improve the system. Various hidden layers were regarded by the ANN-centric security model. By employing UNSW-NB15 and NSL-KDD, the efficacy is computed by carrying out experiments. They sought to act as a reference point for data-driven security modeling through experimental analysis and discoveries in the context of CS.

Jatinder Manhas and Shallu Kotwal (2021) [84] provided many machine learning (ML) approaches, including KNN, multilayer perceptron, DT, NB, and SVM, which have been assessed for use in IDS implementation to categorize network connections as legitimate or malicious in table 2.5. To assess the ability of ML techniques, accuracy, sensitivity, precision, and F-score were deployed. The DT is the best classifier for IDS.

Table 2.5: Performance Comparison of ML Models Applied in Cyber Security

Author	Dataset	Detection	Accuracy	Disadvantages
Muhammad Shakil Pervez et al. (2014) [85]	NSL-KDD	Hybrid based	82.37%	When analogized to the current accuracy, accuracy would be more if there was a grouping of mining classifiers with SVM.
Preeti Mishra et al (2019) [86]	KDD	Misuse-based	99.96%	Detecting low-frequency attacks just by examination of network features is tedious.
Donghwoon Kwon et al (2019) [87]	NSL-KDD	Anomaly-Based	90.40%	For enhancing ADNIDS, the labeled or else trained traffic dataset as of real

				network traffic wasn't present.
Ayyaz-Ul-Haq Qureshi et al (2019) [88]	NSL-KDD	Anomaly-Based	94.50%	In attack detection methods, NSL-KDD did not play a significant part.
Ying Gao et al (2019) [89]	KDD	Anomaly-Based	99.95%	Since attackers frequently alter the kinds along with techniques of attacks, it wasn't extremely effectual in DDoS; thus, determining the pattern was tedious.
Mrutyunjaya Panda et al (2007) [90]	DARPA	Misuse-based	99.90%	There was a low FPR in the misuse detection; however, fresh attacks can't be detected.
W. A Awad et al (2011) [91]	Spam base	Email spam	96.90%	The built classifier was not as effective at identifying genuine messages.
RamaniSagar et al. (2020) [92]	Twitter	Spam tweets	98.88%	With recent technological advancements, the scope of security applications was broad, which couldn't be limited to a few applications.

Karthika Renuka D (2015) [93]	Spam base	Email spam	84.00%	The metric determined the features' rank along with eradicating every feature, which doesn't attain a sufficient score by feature ranking techniques.
Vivek Nandan Tiwari et al (2016) [94]	KDD CUP99	Anomaly-Based	-	The evaluation was challenging; in addition, to evaluate the data for security policy violations, network administrators do not have the resources.
Vinayakumar R et al (2019) [95]	NSL-KDD	Hybrid-Based	75.30%	The established system lacked specific information on the malware's structure and features.
Anna L Buczak et al (2016) [96]	DARPA	Anomaly-Based	80.00%	Finding the boundaries betwixt known and unknown categories is a challenge in anomaly detection.
Gary Stein et al (2005) [97]	KDD	Hybrid based	99.85%	Since it was tedious to engender common behavior profiles, most prevailing techniques had a false alarm rate for protected systems.
Yara Rizk et al (2019) [98]	Spam base	Email spam	89.2%	Data was not transmitted by network connection and

				they were not explicitly shown
Sang Min Lee et al (2010) [99]	Spam base	Email spam	95.43%	Since irrelevant features not only increase time and sources but also decrease classification rates, every feature was not essential for classifying emails.
Megha Rathi and Vikas Pareek et al (2013) [100]	Spam base	Email spam	99.54%	Acquiring 100% accuracy was tedious; however, RT and RF were very nearby.

2.6 Review of Deep Learning Methods for Cybersecurity

In 2015, Wang et al. [101] used DL to categorize the data using stacked auto-encoders and a sigmoid layer to determine the kind of traffic. The dataset Wang utilized consisted of the payload bytes of each session and the TCP traffic statistics from an internal network. This dataset had 58 different protocol types, however as HTTP is easily recognizable and makes up the great majority of the data, it was left out. A three-layer stacked auto-encoder is used to extract the features, which are then fed into a sigmoid layer for classification. This network, eliminating HTTP, had a recall range of 90.9% to 100% and a precision range of 91.74% to 100% for the 25 most popular remaining protocols.

Cox et al. [102] used DL in 2015 to recognize and classify various file types using DBNs. They did this by utilizing a signal processing method. Three separate feature types are created using the data. Take the Shannon entropy across a 256-byte window with a 50% overlap as an illustration. Then, to give it a predetermined length, the Shannon entropy values are cubically interpolated into a regular grid of 256 points. By first interpreting the byte sequence as a signal and then translating it into frequency space, the second feature set is produced. A histogram of the bytes makes up the third feature set. A four-layer DBN with stacked demising auto encoders served as the classifier. The total number of files in

the dataset was 4500, with 500 of each of the nine types and 100 of each type kept aside for testing. Overall, nine different file types could be accurately categorized in 97.44% of cases.

Javaid et al. developed a deep-learning-based IDS in 2015 [103] that builds two distinct models using sparse auto-encoder layers followed by a variety of supervised softmax layers. The first model separates network traffic into two groups: beneficial and detrimental. The second approach splits regular traffic or attack traffic into four different types. The sparse auto-encoder part of the model contains two hidden layers. This output is fed into three softmax layers to create a DNN with four hidden layers.

With 88.4% accuracy against 79.1% accuracy, the two-class classifier performed better than the five-class classifier. Additionally, Ma et al. [104] utilized comparable methods and had comparable outcomes.

Tang et al. (2016) [105] demonstrate a software-defined networking-based IDS system that makes use of deep learning. The SDN controller, which can track all OpenFlow switches and request all network data, is where the advised IDS system is installed. The four kinds of attacks were DoS attacks, R2L attacks, U2R attacks, and Probe attacks in the NSL-KDD dataset that was used in the study. It was classified into two classes (normal and anomaly class) for analysis. According to the experimental findings, the learning rate of 0.001 outperforms others and has the highest receiver operating characteristic curve (AUC).

A five-layer deep belief network (DBN) intrusion detection model was employed by Chawla [106] in 2017, particularly for the Internet of Things. Each hidden layer in the suggested model is an auto encoder's encoding layer. The author's experiment yielded the characteristics, which also included metadata about the packet and data from the IPv6 header. Twelve distinct attack types were used to represent the harmful data. A TPR of 95.4% and overall accuracy of 95.03% were produced by the model. In a related experiment by Diro and Chilamkurti [107], they were able to obtain 99.2% accuracy on a binary classification task and 98.27% accuracy on a four-class issue using a different dataset and an auto encoder with three hidden layers.

Wang's work was expanded upon in 2017 by Lotfollahi et al. [108], who looked at traffic characterization and application identification. To characterize network traffic, it must first be classified (e.g., FTP). The sort of application being utilized is identified by application identification. Lotfollahi et al. [108] claim that their technology can identify encrypted

communication and distinguish between VPN and non-VPN traffic. Combining an auto encoder, a CNN, and a classification layer allowed them to do this. The traffic classification job obtained an F1 score of 93% while the application identification assignment received a score of 98%.

In 2017, Chawla [106] used a five-layer deep belief network (DBN) intrusion detection model designed for the Internet of Things. Each hidden layer in the suggested model is an auto encoder's encoding layer. The author's experiment yielded the features, which also included metadata about the packet and data from the IPv6 header. Twelve different attack types were used to represent the harmful data. The model generated a TPR of 95.4% and an overall accuracy of 95.03%. In a comparable experiment, Diro and Chilamkurti [107] used a different dataset and an auto encoder with three hidden layers to achieve 99.2% accuracy on a task involving binary classification and 98.27% accuracy on a four-class problem.

A method that uses a deep neural network model to help categorize cyberattacks was proposed by Zhou et al. (2018) [109]. The system primarily uses three processes: data collection, data pre-processing, and deep neural network categorization. The system achieves an accuracy of 0.963 using an SVM model with a learning rate of 0.01, 10 training epochs, and 86 input units. The results reveal that the k-nearest neighborhood, linear regression, and random forest classical machine learning techniques outperform each other marginally.

A multi-channel intelligent attack detection system using recurrent neural networks with long short-term memory is described by Jiang et al. (2018) [110]. Using the NSL-KDD dataset, the effectiveness of the proposed intelligent attack detection system is evaluated. The long short-term memory recurrent neural network's performance parameters include a 99.23% detection rate, 9.86% false alarm rate, and 98.94% accuracy.

By moving processing from the cloud to the edge of the network, which is transmitted across the network backbone and is located closer to the user and devices, Diro and Chilamkurti [111] examined the capacity of a DL algorithm to identify intrusion in IoT. They developed a DNN with three hidden layers using the NSL-KDD dataset, outperforming shallow learning techniques with accuracy rates of 99.2%, detection rates of 99.27%, and false alarm rates of 0.85%. Diro and Chilamkurti [112] conducted this

experiment in 2018 and got the same results using stacked autoencoders with two hidden layers.

Wang et al (2018) [113] exhibited a scenario-centric 2-stage sparse cyber-attack for smart grids with total as well as biased network details in 2018. The verified cyber-attacks were detected; in addition, a security mechanism grounded on Interval State Estimation (ISE) was applied freshly. For increasing the function variable's variance cycles, the upper along with lower limits of every state variable were modeled as a dual optimization challenge. For gathering nonlinear and non-stationary features in electric load results, the stacked auto-encoder (SAE), a well-known DL, was deployed. For maximizing the predictive performance of electric loads, those features were wielded; thus, state variables with a narrow width. For developing the forecasting error's variance, a parametric Gaussian distribution was wielded. For depicting the current cyber-attack models' validity and security mechanisms, comprehensive research on various IEEE benchmarks was deployed.

Fan Zhang et al. (2019) [114] developed a CDS based on the defense-in-depth principle and deployed network traffic data, host system data, as well as measured process parameters. The AD system offered multi-layer protection by limiting the defenders' crucial time before irreversible repercussions occurred in the physical system. In the traditional intrusion prevention layer, which is the 1st layer, firewalls, data diodes, along with gateways were included. Grounded on network traffic and system data, data-driven models were encompassed by the 2nd defense system, for cyber-AD. The classification model denoted by M1 together with big data analytics models signified by M2 is also included. When behavior deviation from normal operation was produced by the attacks, early identification of attackers was offered by M1 and M2. If malicious activities couldn't be recognized by the secondary layer, the processed data will be monitored by the last defense line. Due to the cyber-attack, the empirical models (indicated by M3) were deployed by the last defense line, which considerably recognized the abnormal operations. Before considerable consequences occurred, impactful cyber-attacks could be identified. However, the scheme was ineffective for the advanced cyber-attacks.

Convolutional neural networks were used by Basumallik et al. (2019) [115] to identify packet-data anomalies in a state estimator based on phasor measurement units. The data is analyzed and characteristics from the phasor measurement units are extracted using convolutional neural networks. The phasor measurement unit buses are the IEEE-30 bus and IEEE-118 bus systems. From the study, 512 neurons in a coupled layer may provide

an accuracy of 98.67% and a probability of 0.5. According to the authors, a convolutional neural network-based filter outperforms those based on recurrent neural networks, huge short-term memory, support vector machines, bagged filters, and boosted filters.

Nevius Kaja et al (2019) [116] developed 2-stage intelligent IDS, which were recognized and protected from such malicious attacks. It was encompassed by the approach centered on ML algorithms. Its usage in the design of IDS after a 4-step effective data pre-processing was fresh. K-Means was utilized by the IDS that identified the attacks in the 1st stage. In the 2nd stage, supervised learning was utilized, which categorized such attacks and removed the number of false positives. By applying the approach that was capable of detection and also the classification of attacks with higher accuracy, effective IDS were produced. The number of false positives was reduced. The IDS's performance was superior when contrasted to the prevailing system. Nevertheless, low detection rates along with higher FP were possessed.

A Network Intrusion Detection (ID) technique that combines hybrid sampling and a Deep Hierarchical Network (DHN) was described by Kaiyuan Jiang et al. in 2020 [117]. At first, One-Side Selection (OSS), which reduced the noise samples in the common category, was used. The Synthetic Minority Over-sampling Technique was then used to increase the minority samples. In that manner, a balanced dataset was determined. Due to this, the minority samples' features were fully learned by the model, and also the model's training time was significantly decreased. Secondly, to extract spatial features, a CNN was utilized. For extracting temporal features, Bi-directional long short-term memory (Bi-LSTM) was employed, which created a DHN model. The experiments upon the NSL-KDD along with UNSW-NB15 datasets verified the Network ID algorithm. The model with excellent classification performance was attained. But, the disadvantage of high packet loss was possessed by the scheme and it was also ineffective in handling network overhead.

Abdulrahman Al-Abassi et al (2020) [118] developed a DL technique, which engendered imbalanced datasets' balanced representations. The representations were accepted as the input by an ensemble DL AD, which has been particularly modeled for an ICS environment. The DL, which learned fresh representations of imbalanced datasets, encompassed various unsupervised SAEs. The SAE AD, which extracted fresh representations of the unlabelled data, deployed enormous Auto Encoders (AEs); hence, disparate patterns were achieved. Fresh representations of each SAE were given to a DNN by utilizing a super vector. By using a fusion activation vector, it was concatenated. By the

DT which was employed as a binary classifier, the attacks were detected as of the newly merged representations. This system surpassed the prevailing models. Nevertheless, there was poor backup capability.

In the year 2020, Ismail et al [119] .'s investigation focused on energy theft within the dg domain. In this assault, malicious customers hack the smart meter to keep track of their renewable energy sources and use their data for the system to declare more power. As a way of identifying such detrimental conduct, deep system learning has been researched. This study found that when dg smart meters, environmental reports, and SCADA metering parameters were integrated, the best detection rate (99%) and the lowest false alarm rate were attained.

Moshe Kravchik et al. (2022) [120] engendered a methodology to recognize anomalies and cyber-attacks in physical-level ICS data by employing 1 Dimensional Convolution Neural Networks (CNNs), which shallowed under complete AE, variational AE, and PCA. An FS method was performed by employing the Kolmogorov-Smirnov test. By using short-time Fourier transform and energy binning, the time-domain signals were converted into frequency representation. The system was modeled in time along with frequency domains. On threes popular public datasets, the system was analyzed. The method was robust toward such evasion attacks. For evading detection, the attacker was compelled to forfeit the desired physical impact. However, there was high energy consumption.

Table 2.6 Various Deep Learning Models in Cyber-Attack Detection and Mitigation

Author	Adopted Methods	Features	Challenges
Zhe et al (2020) [121]	RNN Model	<ul style="list-style-type: none"> • Tiny divergence • Reliable correction • Maximal destabilizing effects 	The initial state reconstruction wasn't constrained.

<p>Georgios et al (2020) [122]</p>	<p>ANN Classifier</p>	<ul style="list-style-type: none"> • Improved classification accuracy • Low energy failure • Less pocket dropped failure 	<p>The classification findings will benefit from the addition/removal of features from the illustrative datasets.</p>
<p>Huaizhi Wanget al (2018) [123]</p>	<p>SAE Model</p>	<ul style="list-style-type: none"> • High detection accuracy • MAPE • Robustness 	<p>To resolve L0-norm minimization, the enhancement must be prioritized.</p>
<p>Defu et al (2019)[124]</p>	<p>AWV Model</p>	<ul style="list-style-type: none"> • Enhanced classification cause • High precision • Enhanced precision • Maximal recall • Superior F1 score 	<p>The associated data should be maximized; in addition, progress on a DL, which is incorporated with Big Data analysis, should be done.</p>
<p>Jesus Arturo Perez-Diaz et al. (2022) [125]</p>	<p>SDN Model</p>	<ul style="list-style-type: none"> • Maximal exactness • False alarm rate • High exactitude • Enhanced recall • Maximal f1 measure 	<p>The recent ML and DL strategies weren't integrated by the proffered system.</p>

Karimipour et al (2019) [82]	DBN Model	<ul style="list-style-type: none"> • Enhanced accuracy • True positive rate • Minimized FPR 	The proffered technique success rate doesn't rely on the attack scenarios.
Fanrong Wei et al (2020) [129]	Deep RL Framework	<ul style="list-style-type: none"> • Reduced cyber-attack impacts • Minimized MSE • Enhanced system stability 	The statistics engendered in scenario 1 along with state of affairs 2 weren't encompassed by the training facts.
Muhammad Ismail et al (2020) [128]	Hybrid C-RNN detector Model	<ul style="list-style-type: none"> • Highest detection rate • Lowest false alarm 	The next detector's resistance to a fresh cyber-attack, which wasn't present, was tested throughout the detector's training.

2.7 Research Gap

For businesses and individual users, the internet has emerged to be a vital infrastructure; in addition, its security has become a huge concern. In inspiring the required purchaser confidence, protection is an important component for attaining commercial success for the fresh methodologies, which are evolving recently. For resolving fraud detection in CS, regression might be wielded. Once a system is determined as of the historical transaction it detects fraudulent transactions, especially grounded on recent transactions' observable attributes. For resolving several CS problems, system evaluation techniques are wielded. For offering viable answers to CS challenges, there is a potential for advances in the realm of device understanding together with deep mastery. Nevertheless, for specific usefulness, recognizing which set of rules is appropriate. Multi-layered processes are essential for keeping the solution resistant to malware attacks along with attaining superior detection rates. The choice of a selected version is vital while solving CS problems. For resolving malicious attack detection, online data sets are analyzed by ML techniques, which were

completed by employing NB. By deploying constrained specified data points that are extremely costly to attain, active learning permits the issue to be resolved. When minimizing latency and enhancing detection efficiency, IDS should detect along with feedback network traffic in real-time. For enhancement, the accuracy along with the generalization of ID has much room. Several kinds of attacks can be detected by a good scheme with could enhance the IDS's performance. The establishment of IDS might be affected by the incorrectly classified attack data. Moreover, for justifying the objective, a summary of the literature is furnished at the review's end.

2.8 Conclusion

The cyber-attacks dynamic along with the intricate environment wasn't dealt with in the major present ID system. Thus, green adaptive strategies like several gadget researching methodologies could cause minimized false alarm rates, and high detection costs, along with reasonable calculation as well as verbal exchange fees. For mitigation, a fresh DL-centric CAD System with a Bait-centric system was presented. For effectual cyber-attack detection, various operations were included. The prevailing systems were surpassed by the CAD; in addition, it is more reliable and robust.

CHAPTER 3

METHODOLOGY

3.1 Introduction

ICSs are hugely deployed for partial or full automation control [129-130]. On the environment like the safety as well as people's health, the economy, along with national security, their operation has a straight effect [131]. They are highly susceptible to being corrupted by malicious attackers since the data are usually transmitted over a wired or wireless network in ICS [132]. For leveraging the system vulnerabilities toward launching cyber-attacks, the inclusion of the IoT in ICSs opens up opportunities for cybercriminals [133-134]. DoS, Man in middle attacks, SQL injections, Password attacks, Phishing, etc, are encompassed in typical cyber-attacks against ICSs [135]. Causing damage or catastrophe like hazardous accidents or production loss by manipulating along with disrupting the physical process is the key aim of cyber-attacks on ICSs [136]. Attack detection systems are created to expertly track the activities taking place in an information system and spot the warning signals of security problems [137]. Anomaly detection, which is the act of discovering abnormal occurrences or unexpected behavior, is utilized for attack detection [138–139]. Just on a particular kind of attack, those techniques are trained along with unseen or new types of attacks that aren't detected by them [140]. Defense of computer systems as of risks to confidentiality, integrity, along with availability is termed computer security. Records revealed honestly feasibility policy is called Confidentiality; records are not mislaid or else spoilt along with the device operations exactly are termed integrity; device offerings are present while they're required is termed availability. The monitoring is done by computer structures, computer networks, and data. By those dangers, the maximization of CAD structures has been initiated along with others that are expected to emerge lately. Industrial control systems are aimed at cyber-criminals. Complex methodologies and key infrastructures, which offer power, water, shipping, production, as well as other crucial services, are exhibited by the people who work in those areas [132]. Early, these systems were fundamentally dumb and automated by deploying protocols, which were elite to the device and dwell on networks outdoors. Business management systems that are in usage attach to the internet either directly or else indirectly since the landscape has shifted. Thus, vulnerabilities are caused as with any other connected device.

Gigantic outages, several affected consumers, or else even a national tragedy might be caused by the downtime or invasion of an ICS network.

Thus, several anomaly detection algorithms are presented for surpassing the challenges and vulnerabilities faced during attack detection. By deploying several ML techniques, those approaches are incorporated and applied [141]. However, the imbalanced natures of ICS datasets aren't regarded by the prevailing system; thus, low detection rates or high false-positive in real scenarios are caused [142]. If the entire system was attacked simultaneously, a few current methodologies might be insufficient [143]. On fault-tolerant control that could offer tools for attack-resilient control, enormous research was conducted [144]. However, there are significant variations between fault-tolerant and attack-resilient control when it comes to attacking detection and isolation, which drive the need for distinct techniques to address security issues in ICSs [145]. Thus, a system that guarantees the accurate detection of cyber-attacks and retains more authenticity termed BReLU-ResNet -centric CAD System with a Bait-centric approach was proposed for mitigation.

3.2 Advanced Encryption Standard Algorithm

The AES algorithm is a symmetric block cipher that uses 128, 192, and 256-bit keys to transforming plaintext stored in 128-bit blocks into ciphertext [146]. Since the AES algorithm is regarded as secure, it is a component of the international standard. AES uses a 128-bit symmetric or single-key block cipher to encrypt and decode data. The ciphertext is produced by the AES encryption procedure. A human-readable and intelligible version of unencrypted data has been transformed into something practically impossible to read. It is not possible to read the AES ciphertext, which is the result of the encryption process until it has been decoded with the AES private key.

To transform plaintext into ciphertext and ciphertext back into plaintext, the encryption and decryption process can use keys of lengths of 128 bits, 192 bits, or 256 bits [146]. Encryption and decryption are the terms used to describe these procedures. The identical AES private key is provided to both the sender and the recipient during AES encrypted communication. The data is transformed into plaintext that can be read and ciphertext using this private key. Without the AES private key, a hacker attempting to access this data would be unable to do so.

3.2.1 Operation of Advanced Encryption Standard Algorithm

In contrast to Feistel encryption, AES uses iterative encryption. A "substitution-permutation network" forms the basis of it. It comprises some related processes, some of which move bits around while others replace specific outputs for inputs (permutations). It's noteworthy to notice that AES does all of its calculations using bytes rather than bits. AES treats a plaintext block's 128 bits as 16 bytes as a result [147]. These 16 bytes are organized into four columns and four rows for matrix processing. The AES key length affects how many rounds are used. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each of these rounds uses a unique 128-bit round key that is obtained from the first AES key. The following graphic 3.1 provides a schematic of the AES structure.

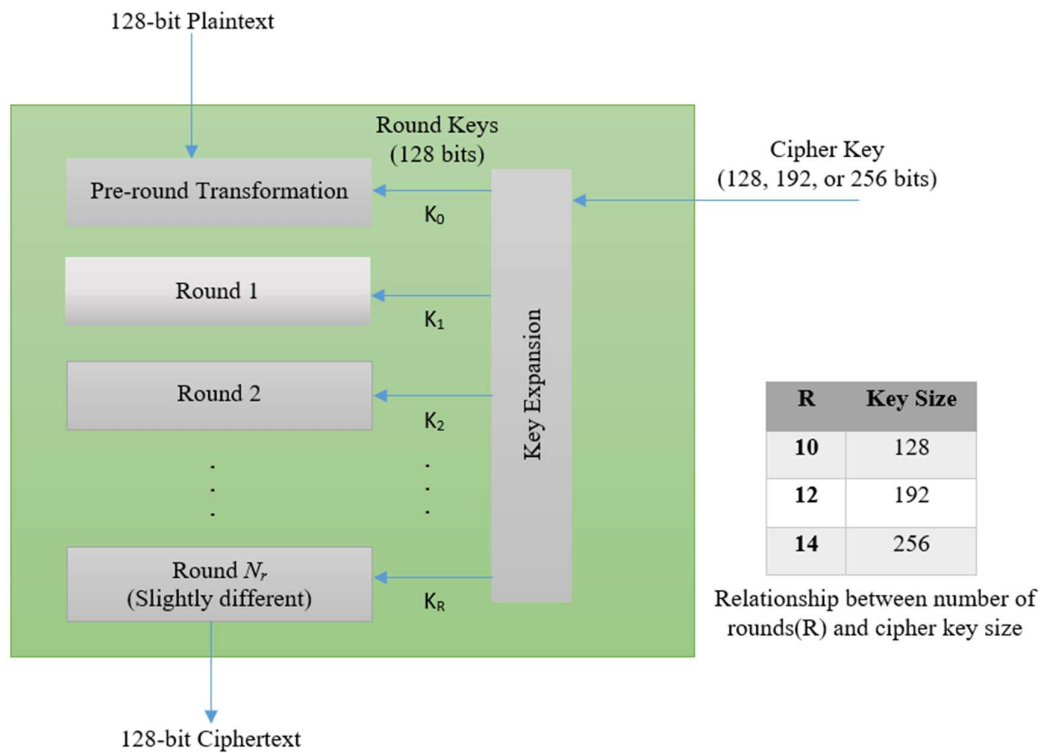


Fig 3.1: Advanced Encryption Standard Algorithm Structure [147]

3.2.1.1 Encryption Process

Each cycle has four sub-processes. Below figure 3.2, the process' first stage is depicted.

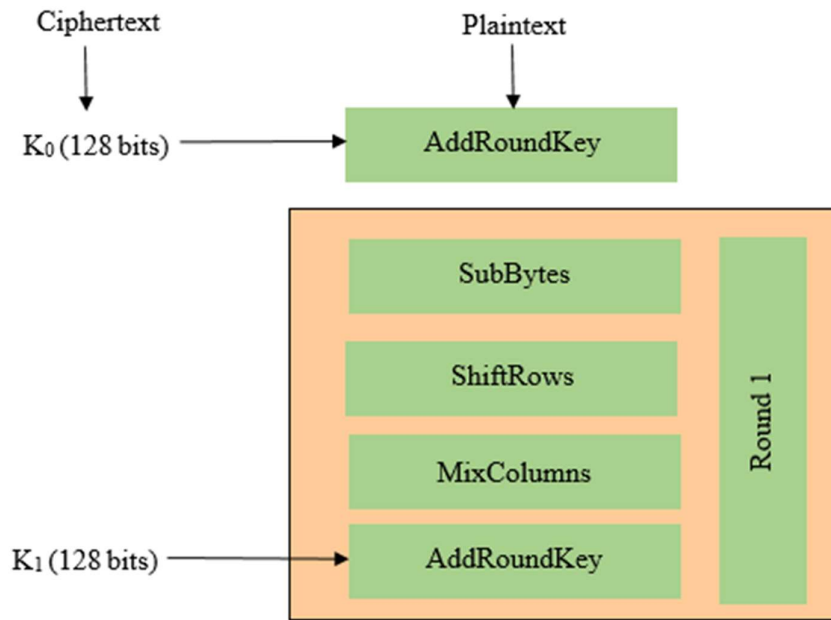


Fig 3.2: Advanced Encryption Standard Algorithm Encryption Process [148].

- **Byte Substitution (Sub Bytes):** To replace the 16 input bytes, a fixed table (S-box) provided in the design is looked up. A matrix with four rows and four columns represents the outcome.
- **Move rows:** The four rows of the matrix are all shifted to the left. Any entries that "slide off" are reinserted on the right side of the row. For shift, the subsequent processes apply [149]:
 - i. The top row remains in place.
 - ii. The second row has been moved to one (byte) position to the left.
 - iii. The third row has been shifted left two places.
 - iv. Three spaces to the left, in the fourth row.
 - v. The result is a new matrix with the same 16 bytes but in different places.
- **Mix Columns:** For each four-byte column, a different mathematical function is employed to alter it [150]. This method takes the four bytes of one column and produces four completely new bytes that replace the original column. The result is a second, new matrix with 16 additional bytes. It should be noted that this stage is not part of the final round.
- **Add round key:** The 16 bytes of the matrix, which are now regarded as 128 bits, are XORed with the 128 bits of the round key. If this is the last round, the output is

the encrypted text. If not, 16 bytes are translated from the resultant 128 bits, and the operation is repeated.

3.2.1.2 Decryption Process

The process for decrypting an AES cipher text is very identical to that for encrypting it. Each round involves doing the four steps in reverse order [151].

- Round key added
- Mix columns
- Move rows
- Byte replacement

Despite being extremely closely related, the encryption and decryption algorithms must be implemented independently since the sub-processes in each round operate in reverse, unlike a Feistel Cipher.

3.3 Rivest-Shamir-Adleman Encryption Algorithm

Rivest-Shamir-Adleman is an asymmetric encryption technique that is extensively utilized in a variety of goods and services (RSA). Data is encrypted and decrypted using a pair of keys that are mathematically related in asymmetric encryption. The creation of a key pair results in the creation of a private and public key, with the private key remaining a secret known only to the key pair's inventor [152]. The public key or the private key can be used to encrypt or decrypt data using RSA, respectively. The fact that RSA is the most used asymmetric encryption method is due in part to this.

Users of RSA can choose to encrypt using the private or public key, which has many benefits. If the content has been encrypted with the public key, it must be decoded with the private key. When the data recipient provides the data sender their public key, sensitive data can be sent securely through a network or Internet connection [153]. The data sender then encrypts sensitive data before transferring it using the recipient's public key. Only the owner of the private key can decrypt sensitive information since the data was encrypted using the public key. Even if the data were intercepted in route, only the intended receiver will be able to decipher it.

The alternate asymmetric encryption method using RSA is message encryption using a private key. In this illustration, the sender encrypts the data using their private key before sending it to the receiver along with their public key. By utilizing the sender's public key to decrypt the data, the recipient may then confirm that the sender is who they say they are [154]. The data might be intercepted and read while in transit using this method, but the

main goal of the encryption is to determine the source. The recipient would be aware if the data had been altered while in route due to the public key's inability to decrypt the altered message.

The technical components of RSA are based on the notion that factoring the output back into the underlying prime numbers is very challenging, even though multiplying two sufficiently big integers together is easy. Two numbers—one of which is a composite of two enormous prime numbers—make up the public and private keys [155]. The same pair of prime numbers serve as the source of both values. It is exceedingly challenging to factorize RSA keys because of their average length of 1024 or 2048 bits, though 1024-bit keys are rumored to be breakable soon [156]. The RSA algorithm ensures that the keys in the aforementioned example are as secure as feasible. The following examples show how it operates:

The steps below are used by the RSA algorithm to create public and private keys [157]:

1. p and q , two big prime numbers, should be chosen.
2. Find $n = p * q$ by multiplying these values, where n is referred to as the modulus for encryption and decoding.
3. Select a value e smaller than n such that n is roughly equal to $(p - 1) * (q - 1)$. This indicates that the only factor in common between e and $(p - 1) * (q - 1)$ is 1. Select " e " such that $1 < e < \varphi(n)$, e is prime to $\varphi(n)$

$$\gcd(e, \varphi(n)) = 1$$

4. The public key is $\langle e, n \rangle$ if $n = p * q$. Public key $\langle e, n \rangle$ is used to encrypt a plaintext message m . The following formula is used to obtain cipher text C from the plain text.

$$C = m^e \bmod n$$

In this case, m must be lower than n . Each message in a larger message ($>n$) is handled as a separate communication and is encrypted independently.

5. We calculate the d according to the formula below to get the private key:

$$d_e \bmod \{(p - 1) * (q - 1)\} = 1$$

Or

$$d_e \bmod \varphi(n) = 1 \quad (3.1)$$

6. $\langle d, n \rangle$ is the private key. The private key $\langle d, n \rangle$ is used to decipher the cipher text message c . The following formula is used to calculate plain text m from the cipher text c .

$$m = c^d \text{ mod } n$$

Let us consider an example to encrypt plaintext 9 using the RSA public-key encryption algorithm.

Step 1: Select two prime numbers p and q as 7 and 11 respectively.

Step 2: Multiply these numbers to find $n=p*q$, where n is called the modulus for encryption and decryption.

$$n = p*q$$

$$n = 7*11$$

$$n = 77$$

Step 3: Chose a number e less than n , such that n is relatively prime to $(p-1)*(q-1)$. It means that e and $(p-1)*(q-1)$ have no common factor except 1. Choose e such that $1 < e < \varphi(n)$, e is prime to $\varphi(n)$, $\text{gcd}(e, \varphi(n)) = 1$.

$$\text{Calculate } \varphi(n) = (p-1)*(q-1)$$

$$\varphi(n) = (7-1)*(11-1)$$

$$\varphi(n) = 6*10$$

$$\varphi(n) = 60$$

Choose relative prime e of 60 as 7.

Thus the public key is $(e,n)=(7,77)$.

Step 4: A plain Text message m is encrypted using the public key (e,n) . The following formula is used to obtain cipher text C from the plain text.

$$C = m^e \text{ mod } n$$

$$C = 9^7 \text{ mod } 77$$

$$C = 37$$

Step 5: The private key is (d,n) . To determine the private key, we use the following formula

$$d_e \text{ mod } \{(p - 1) \times (q - 1)\} = 1 \text{ or } d_e \text{ mod } \varphi(n) = 1$$

$$7d \bmod 60 = 1$$

$$d = 43$$

The private key $(d,n) = (43,77)$

Step 6: A cipher text message c is decrypted using the Private key (d,n) . To calculate plain text m from the ciphertext c we use the following formula

$$m = c^d \bmod n$$

$$m = 37^{43} \bmod 77$$

$$m = 9$$

So, Plain text is 9 and Cipher text is 37.

3.4 Elliptic Curve Cryptography Algorithm

The Rivest-Shamir-Adleman (RSA) cryptographic algorithm can be replaced by elliptical curve cryptography (ECC), a public key encryption technique based on elliptic curve theory [158]. ECC is most frequently used for one-way email, data, and software encryption as well as digital signatures in cryptocurrencies like Bitcoin and Ethereum.

An elliptic curve is a looping line that connects two axes, or lines on a graph that indicate where a point is located, rather than an oval form. The curve is fully symmetrical, or mirror imaged, along the x-axis of the graph. Data is encrypted and decrypted using public key cryptography systems like ECC, which combine two separate keys through a mathematical process [159]. One is a public key that is known to everyone, while the other is a private key that is only known by the data's sender and receiver. ECC creates keys by mimicking the properties of an elliptic curve equation, as opposed to the traditional method of obtaining keys as the product of large prime integers.

ECC is similar to the majority of other public key encryption techniques, including RSA and Diffie-Hellman [160]. The idea of a one-way, or trapdoor, function is used by each of these cryptographic techniques [159]. This suggests that employing a mathematical equation with a public and private key to travel from point A to point B is straightforward [161]. Traveling from point B to point A is difficult, if not impossible, without knowing the private key and depending on the key size used.

As seen in the picture below with the green line and three blue dots designated A, B, and C, ECC is based on the properties of a group of values, where operations may be performed on any two members to give a third member, which is derived from positions where the line crosses the axes. To acquire another point on the curve, multiply one curve point by a certain quantity (C). Point C is moved to the mirrored point on the other side of the x-axis to produce point D. A line is formed from this spot back to point A, where it crosses at point E. There is a maximum number of times this process can be finished that is specified. The private key value, or n, specifies how many iterations of the equation should be performed before arriving at the final result that may be used to encrypt and decrypt data [162]. The key size employed has an impact on the equation's maximum defined value. The following equation can be used to represent the points on the graph from a cryptographic standpoint:

$$y^2 = x^3 + ax + b$$

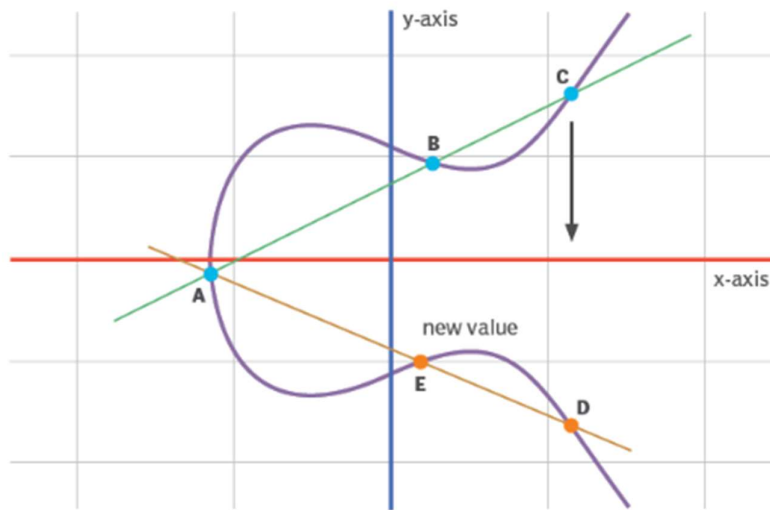


Fig 3.3: Elliptic curve cryptography graph [155].

3.4.1 Key Generation

Input the parameters are 'a', 'b' and 'q' where 'q' is a prime number the points on the curve has been generated as 'G' which order is larger the n [163]. The public key of user A is selected and represented as n_A which is less than 'n'. The public key of user B is selected which is represented as n_B which is less than 'n'. The public key of user B has been calculated with product of n_B and 'G'. which is stored in P_B . The public key of user A has

been calculated with product of n_A and 'G' which is stored in P_B . The private key of user A is represented as P_A . and the public key of user B has been represented as an P_B [164].

Step 1: Input the parameters as a,b and q, Where q is a prime with an integer of the form 2^m .

Step 2: Compute the generator G as a point on the curve whose order is larger value as n.

Step 3: Select the Public key as n_A .

$$n_A < n \text{ where } A \text{ is an User A}$$

Step 4 : select the Public key as n_B .

$$n_B < n \text{ where } B \text{ is an User B}$$

Step 5: Calculate the Public key P_A

$$P_A = n_A * G, \text{ where } A \text{ is an User A}$$

Step 6: Calculate the Public key P_B

$$P_B = n_B * G, \text{ where } B \text{ is an User B}$$

Step 7: Return Public Key P_A .

Step 8: Return Public Key P_B .

Let us consider a numerical example to key exchange using Elliptic Curve Cryptography algorithm

Consider a Prime number $q=8209$, $a=2$, $b=7$, $G=(4, 1313)$, $h=1\%$ of secret key (ie.K(x)), for encoding and decoding of message in elliptic curve. Based on global parameters, the elliptic curve's equation becomes:

$$y^2 \text{ mod } 8209 = (x^3 + 2x + 7) \text{ mod } 8209$$

Step 1: Private key of A is a random value: $d_A=4706$

Step 2: Public Key of A is

$$\begin{aligned} P_A(x,y) &= d_A * G(x,y) \\ &= 4706 * (4, 1313) \end{aligned}$$

$$= (7926, 5458)$$

Step 3: Private Key of B is a random value:

$$d_B = 4802$$

Step 4: Public Key of B is:

$$\begin{aligned} P_B(x, y) &= d_B * G(x, y) \\ &= 4802 * (4, 1313) \\ &= (6866, 15) \end{aligned}$$

Step 5: Calculation of secret-key by A is:

$$\begin{aligned} K(x, y) &= d_A * P_B \\ &= 4701 * (6866, 15) = (1846, 3967) \end{aligned}$$

Step 6: Calculation of secret-key by B is:

$$\begin{aligned} K(x, y) &= d_B * P_A \\ &= 4802 * (7926, 5458) = (1846, 3967) \end{aligned}$$

3.4.2 Encryption and Decryption

The first task in this system is to encode the plaintext message m to be sent as an x - y point P_m . It is the point P_m that will be encrypted as a ciphertext and subsequently decrypted. As with the key exchange system, an encryption/decryption system requires a point G and an elliptic group $Eq(a, b)$ as parameters. Each user A selects a private key n_A and generates a public key $P_A = n_A * G$.

To encrypt and send a message P_m to B , A chooses a random positive integer k and produces the cipher text C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B 's public key P_B . To decrypt the cipher text, B multiplies the first point in the pair by B 's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

A has masked the message P_m by adding kPB to it. Nobody but A knows the value of k , so even though P_b is a public key, nobody can remove the mask kPB . However, A also includes a “clue,” which is enough to remove the mask if one knows the private key nB . For an attacker to recover the message, the attacker would have to compute k given G and kG , which is assumed to be hard.

As an example of the encryption process take $p = 751$; $E_p(-1, 188)$, which is equivalent to the curve $y^2 = x^3 - x + 188$; and $G = (0, 376)$.

Suppose that A wishes to send a message to B that is encoded in the elliptic point $P_m = (562, 201)$ and that A selects the random number $k = 386$.

B’s public key is $P_B = (201, 5)$.

We have $386(0, 376) = (676, 558)$, and

$(562, 201) + 386(201, 5) = (385, 328)$.

Thus, A sends the cipher text $\{(676, 558), (385, 328)\}$.

3.5 Data Encryption Standard Algorithm

The Data Encryption Standard (DES) technique, which was created by the IBM team in the 1970s, is nothing more than a block cipher with a symmetric key that converts all plain 64-bit text data blocks into 48-bit keyed cipher text blocks [165]. The National Institute of Standards and Technology, or NIST, now recognizes this standard. As implied by the term “symmetric-key,” the technique encrypts/decrypts data using the same 48-bit key [166]. Typically, asymmetrical algorithms require two keys one for encryption and the other for decryption.

Initial Permutation (IP): Smaller, 64-bit-sized segments of the plain text are separated. Before the opening round, the IP is conducted. The execution of the transposition procedure is described in this phase. The 58th bit, for instance, substitutes the first bit, the 50th bit, the second bit, and so forth. The resulting 64-bit text is divided into Left Plain Text (LPT) and Right Plain Text, which are each equal halves of 32 bits (RPT) [167].

Step 1: Key Transformation: The 56-bit key required by the DES algorithm is created by removing every bit from a 64-bit key's eighth place. A 48-bit key is produced in this stage. The 56-bit key is split into two equal portions, and the number of rounds determines how

many times the bits are rotated to the left. The bits in the key are thus all rearranged [167]. A 48-bit key is created after some bits are lost during the shifting procedure. Compression permutation is the procedure in question.

Step 2: Expansion Permutation: Assume RPT is produced during the IP stage and is 32 bits in size. This step enlarges it from 32 to 48 bits. The 32-bit RPT is divided into 8 chunks of 4 bits each, with an additional 2 bits added to each chunk. The pieces are then each subjected to a permutation operation to yield 48-bit data [167]. The 48-bit key obtained in step 1 is combined with the 48-bit extended RPT using an XOR function.

The following steps comprise the algorithmic process [168]:

1. The 64-bit plain text block is given to the initial permutation (IP) function to start the procedure.
2. The plain text is then subjected to the initial permutation (IP).
3. The initial permutation (IP) creates Left Plain Text (LPT) and Right Plain Text (RPT), two-half of the permuted block (RPT).
4. The encryption method consists of 16 cycles for each LPT and RPT.
5. The LPT and RPT are then reunited, and the newly combined block is subjected to a Final Permutation (FP).
6. This procedure produces the appropriate 64-bit cipher text as a result.

The steps for data encryption are as follows [168]:

1. Split the plain text's 64 bits into two equally sized halves by permuting them.
2. Several rounds of operations will be performed on these 32-bit data pieces.
3. Use an XOR operation between the 48-bit compressed key and the extended right plain text.
4. S-box substitution is the next step once the resultant output is sent.
5. Next, combine the output with the left plain text using the XOR function, and then save the result in the right plain text.
6. Keep the left plain text copy of the first right plain text.
7. The LPT and RPT halves are both sent to the following rounds for additional procedures.
8. Swap the data in the LPT and RPT after the previous round.
9. Use the inverse permutation step in the last step to obtain the encrypted text.

The procedures for data decryption include the following steps:

1. Key 16 becomes Key 1, and so on, with the order of the 16 48-bit keys reversed.
2. The cipher text is subjected to the encryption process.

3.6 Artificial Neural Network Algorithm

In information technology (IT), an artificial neural network (ANN) is a system of hardware and/or software that is based on how neurons in the human brain work. An example of deep learning technology that falls under the artificial intelligence (AI) umbrella is artificial neural networks (ANNs), sometimes referred to as neural networks [169]. These technologies are frequently applied in the business world to solve complex signal processing or pattern recognition problems. Since 2000, some prominent commercial applications have included facial recognition, speech-to-text transcription, data analysis for oil exploration, check processing using handwriting recognition, and weather forecasting. A large number of parallel, tier-arranged processors are often used in an ANN. The first layer is where the raw input data is received, much like the optic nerves in the processing of human vision. Each consecutive layer receives the output from the tier before it rather than the raw input, much as how neurons farther from the optic nerve receive signals from those closest to it. The last layer generates the output of the system.

Artificial neural networks are renowned for their ability to adapt, which means that they change as they gain knowledge from initial training and additional data from later runs. The most fundamental learning model is based on the concept of input stream weighting, where each node assigns a value to the significance of the input data from each of its predecessors. Higher weights are assigned to inputs that help in obtaining the correct responses.

The capacity of artificial neural networks to adapt, or to alter as they learn from initial training and extra data from subsequent runs, is well known [169]. The simplest basic learning model uses the idea of input stream weighting, in which each node rates the importance of the incoming data from each of its forebears. The importance of inputs that support accurate responses is increased.

An Artificial Neural Network is typically fed or trained on a lot of data at first. Training involves providing input to the network and defining the expected outcome. To build a network that can distinguish actor faces, for instance, the first training can include a collection of photos with the faces of actors, non-actors, masks, sculptures, and animals. Each input contains the accompanying identification, such as information stating that they are not actors or people or the names of the actors [170]. The model can adjust its internal

weightings and perform better by reacting. An artificial neural network has three layers as shown in figure 3.4.

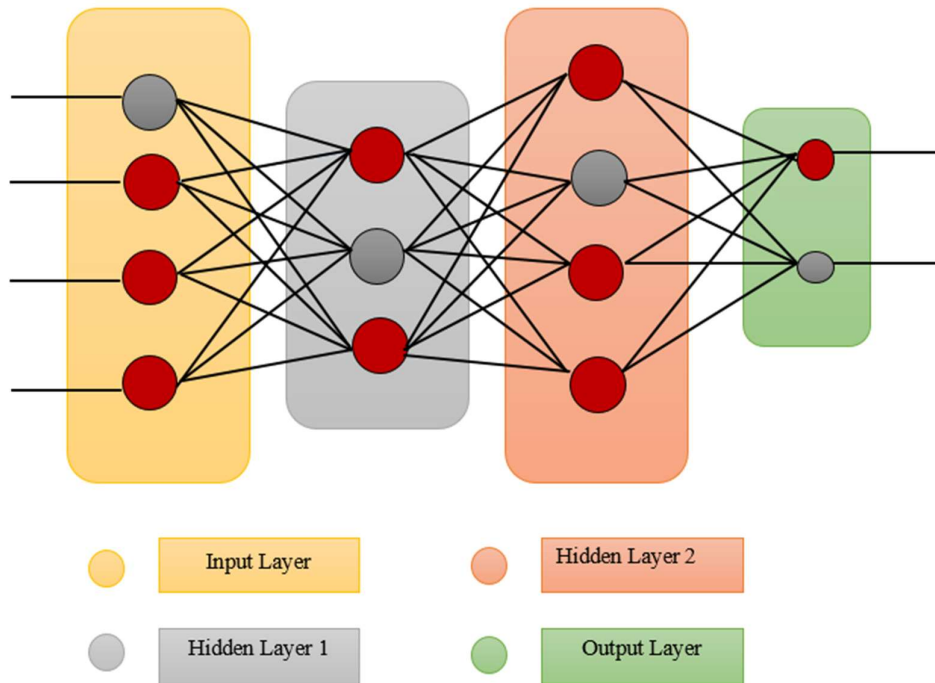


Fig 3.4: layers of artificial neural network [170].

- **Input layer:** As its name suggests, the information layer allows programmers to submit input in a variety of different formats.
- **Hidden layer:** Displayed between the input and output layers, the hidden layer is opaque. It does all the calculations required to find hidden patterns and features.
- **Output Layer:** After the input has undergone several changes in the hidden layer, this layer is utilized to convey the output.

The artificial neural network computes the weighted sum of the inputs and includes a bias when provided input. This algorithm is shown using a transfer function [170].

$$\sum_{i=1}^n W_i * X_i + b \quad (3.5)$$

It feeds the weighted total as an input to an activation function, which outputs the result. The activation functions of a node control whether it should fire or not. Only those who are fired have access to the output layer. Numerous activation functions can be employed, depending on the kind of task we are working on.

3.6.1 Types of neural networks

The "hidden layers" of the model, or the number of layers between the input and output, are frequently used to define the depth of neural networks. As a result, the phrases "deep learning" and "neural network" are sometimes used interchangeably. Alternative ways to define them include the number of hidden nodes in the model or the number of inputs and outputs that each node possesses. Utilizing modifications to the conventional neural network design, different forms of information may be carried forward and backward among layers.

There are several types of artificial neural networks, including:

1. **Feed-forward neural networks:** The feed-forward network is one of the most basic varieties of neural networks. Information is transmitted in a single direction, traveling via some input nodes before it is received at the output node. The network may or may not include hidden node layers, which helps to understand how the network works [171]. It can withstand a lot of noise. This type of ANN computational model is also used in computer vision and facial recognition systems.
2. **Recurrent neural networks:** They keep track of the output from processing nodes and include it in the model. This is how the model is claimed to learn to anticipate the outcome of a layer. Each node acts as a memory cell in the RNN model, continuing computation and operation implementation. This neural network starts with front propagation and then saves all of the processed input so it may repeat it in the future, similar to a feed-forward network [172]. When a network predicts incorrectly, the system self-learns and uses backpropagation to keep trying to anticipate correctly. This type of ANN is frequently used in text-to-speech conversions.
3. **Convolutional neural networks:** one of the most popular models in use today. One or more convolutional layers in this computational model of a neural network may be pooled or linked. A subset of multilayer perceptrons serves as its foundation. Before the picture is finally split into rectangles and sent for nonlinear analysis, these convolutional layers generate feature maps that capture a portion of the image. Numerous of the most advanced AI applications, like facial recognition, text digitization, and natural language processing, use the CNN model [173]. It is very well-liked in the photo recognition industry. Signal processing, picture classification, and phrase identification are other uses.

4. **Deconvolutional neural networks:** Employing a reversed CNN model approach. They look for characteristics or signals that may have been lost or dismissed as irrelevant to the CNN system's goal. This network model may be used for picture creation and analysis.

5. **Modular neural networks:** These networks consist of many separate neural networks. The networks do not communicate with one another or interfere with one another's actions during the calculation. Thus, lengthy or complex computational operations may be carried out more successfully.

3.7 Convolutional Neural Networks Algorithm

Multi-layer neural networks called convolutional neural networks (CNN, or ConvNet) are used to extract visual patterns from pixel pictures [174]. The mathematical function is referred to as "convolution" on CNN. In a specific kind of linear operation, you can combine two functions to show how the shape of one function can be altered by another. Simply said, to extract information from an image, two images that are represented as two matrices are multiplied to produce the output. While CNNs are similar to other neural networks, they complicate the equation by using a series of convolutional layers. Without convolutional layers, CNN is unable to operate.

A convolutional neural network utilizes a backpropagation algorithm to learn spatial hierarchies of data automatically and adaptively [175]. It has many layers, including convolution layers, pooling layers, and fully connected layers. Figure 3.5 shows a typical CNN building.

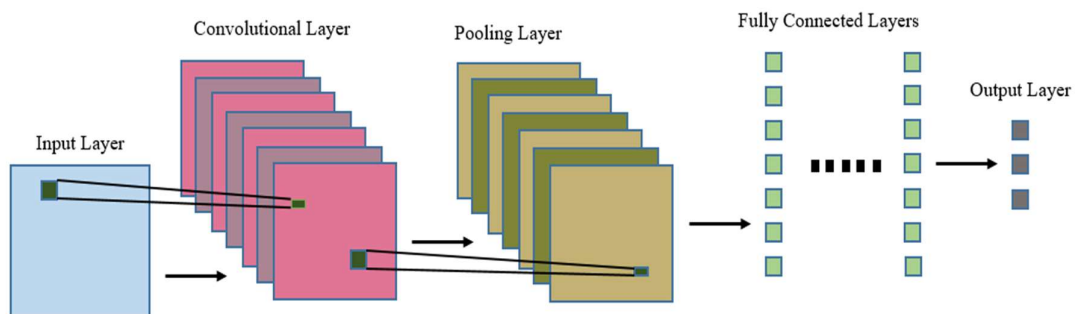


Fig 3.5: CNN building architecture [176].

Definitions of the various layers can be found in the architecture above:

- **Convolutional layer:** When applied to an input image, convolutional layers are made up of several filters (also known as kernels). A feature map, a representation

of the input image with the filters applied, is the result of the convolutional layer. Convolutional layers can be combined to build more sophisticated models that can extract finer details from photos.

- **Pooling layer:** In deep learning, pooling layers are a subset of convolutional layers. By pooling layers, the input's spatial dimension is reduced, which facilitates processing and uses less memory. Pooling speeds up training and also contributes to a decrease in the number of parameters. Max pooling and average pooling are the two primary types of pooling [177]. While average pooling uses the average value from each feature map, max pooling uses the maximum value. To minimize the size of the input before it is fed into a fully connected layer, pooling layers are often utilized after convolutional layers.
- **Fully connected layer:** In a convolutional neural network, fully-connected layers are among the most fundamental types of layers (CNN). Each neuron in a completely connected layer is entirely connected to every other neuron in the layer below, as the name suggests. In the final stages of a CNN, when it is desired to leverage the features discovered by the prior layers to make predictions, fully linked layers are frequently employed [178]. To classify a picture as including an animal, such as a dog, cat, bird, etc., the last fully connected layer of a CNN may employ the characteristics identified by the prior layers.

CNN's are extensively used for picture identification and classification applications. For example, CNNs may be used to identify objects in a photo or classify an image as either a dog or a cat. CNN's may also be used for more challenging tasks, like describing pictures or identifying their focus points. CNN may also be used with time-series data, like audio or text data. CNN's are powerful deep-learning tool that has been used to achieve cutting-edge results in a variety of applications.

3.8 Proposed Cyber-Attack Detection and Mitigation System

For people using the Internet and computers, Cyber-attacks and CS are the challenges. Even for people who aren't using them directly, the problems are increasing. Society hugely relies on networks and computers. With sensors and actuators, they haven't closed within cyberspace anymore and have interaction with the real world. These systems are termed Cyber-Physical Systems (CPS), IoT/Everything (IoT/E), Industry 4.0, Industrial Internet, M2M, et cetera. Serious influence might be caused in real life by the exploitation of any of these systems no matter what they are called; in addition, to mitigate those risks, suitable

countermeasures must be taken. The concern for CS of ICS is increased by the evolving attacks against CPS. On firewalls, data diodes, along with other intrusion preventions that aren't apt for rising cyber threats as motivated attackers, the present efforts of ICS CS are dependent. To detect the attacks with the aid of a DL system, the prevailing system presented an approach. The attack wasn't eradicated even though they are identified. A developed and powerful adversary should be offered as a solution to that issue.

For attack node mitigation, which is proffered employing a new Classification and Encryption methodology, a fresh framework was developed. For training along with testing data, the input data is split into 80% and 20%. Initially, the entire training data is pre-processed. From the input training dataset, features are extracted. To select the significant features, the feature is optimized by employing TWMA. By deploying the BReLU-ResNet the feature is trained. Implementing the skip connection for offering input for the layer indiscriminately for merging the data flow for eradicating data loss and gradient vanishing problems is the goal of Residual neural networks (ResNet). Reducing noise is averaging this system; in addition, training accuracy and generalization are maintained by it. Achieving enhanced training accuracy and approximate level of traversal is the proficient way of enhancing maximum label data. The data is classified into attack and normal data. By employing Bait, the Source IP Address is saved into a secure log file if the data is attack data. The data is ready for transmission if it is normal data. By utilizing the ESHP-ECC, the data is encrypted in Data Transmission. By employing ED, the shortest path distance is analyzed. By deploying the DSHP-ECC, the data is decrypted in the Destination. In the Security Log File (SLF), the testing data is checked in testing. The data is blocked, or attack detection is done if the data's source IP address is present already. In figure 3.6, the proposed framework's block diagram is depicted.

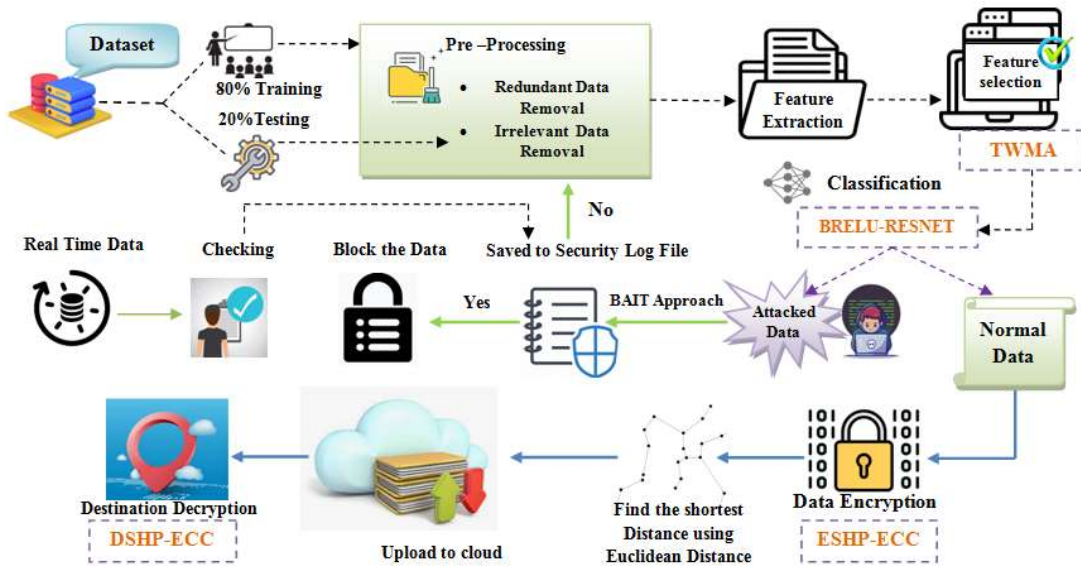


Fig 3.6: Structural Designs of the Proposed CAD and Mitigation System [179].

3.9 Pre-Processing

The input dataset is split into training as well as testing data to initiate the process of the CAD system. For converting the raw data into clean data, the data is pre-processed in the training phase. For enhancing the classification accuracy along with minimizing the training time, pre-processing is carried out. Redundant data removal and irrelevant information removal are deployed as pre-processing steps.

- Storing of same data in multiple locations is termed redundant data. A technique to remove duplicate data from the dataset is called redundant data removal. This reduces the computational complexity and results in better generalization for the classifier.
- The process of removing the data that are not required for the detection of cyber attacks is termed irrelevant information removal. The processing time might be increased by the presence of such unrelated information and may result in an inaccurate attack detection rate. Hence, to improve the performance, the dissimilar data present in the input dataset is removed. Then, the features are extracted from the pre-processed data.

3.10 Feature Extraction

It is the procedure of extracting the number of features by generating novel features as of the prevailing ones. Most information in the original feature sets is included in the novel

features. The feature extraction/selection relies on a representative feature set as of the input patterns in training. To train the classifier, these features are deployed. For allocating the test patterns to one of the pattern classes under selected features' consideration as of the training phase, the trained classifier is implemented in the classification phase.

- Common data reduction, that is, limiting storage needs along with maximizing system speed;
- The feature set reduction, that is, saving resources in the data collection or during usage's next round;
- Performance expansion, that is, gaining predictive precision;
- Data understanding, that is, gaining knowledge about the process engendered by the data or simply visualizing the data's feature set as input patterns.

From the pre-processed dataset, the features like (1) source IP address, (2) source port number, (3) destination IP address, (4) destination port number, (5) transaction protocol, (6) source bits per second, (7) destination bits per second, etc are extracted. The set of extracted features $x_{(i)}$ is equated as,

$$x_{(i)} = x_{(1)}, x_{(2)}, \dots, x_{(n)} \quad (3.6)$$

Here, the number of extracted features is depicted by n .

3.11 Feature Selection by TWMA

The significant features are selected using the novel Taxicab Woodpecker Mating Optimization (WMA) (TWMA) [180]. By the mating behavior of red-bellied woodpeckers, WMA, which is a nature-inspired optimization, is presented. Woodpeckers, which deploy an effectual strategy of communication called drumming for attracting the other gender to mate, are wonderful birds; in addition, there are 200 different species of them. In structural optimization, WMA applies to tedious issues. Attaining optimal values meant for the parameters as of every possible value for maximizing or minimizing its result is termed optimization. In various engineering systems, the WMA is deployed for resolving real-world issues. The WMA's efficacy is examined in which it attains enhanced outcomes in diverse benchmark functions in figure 3.7.

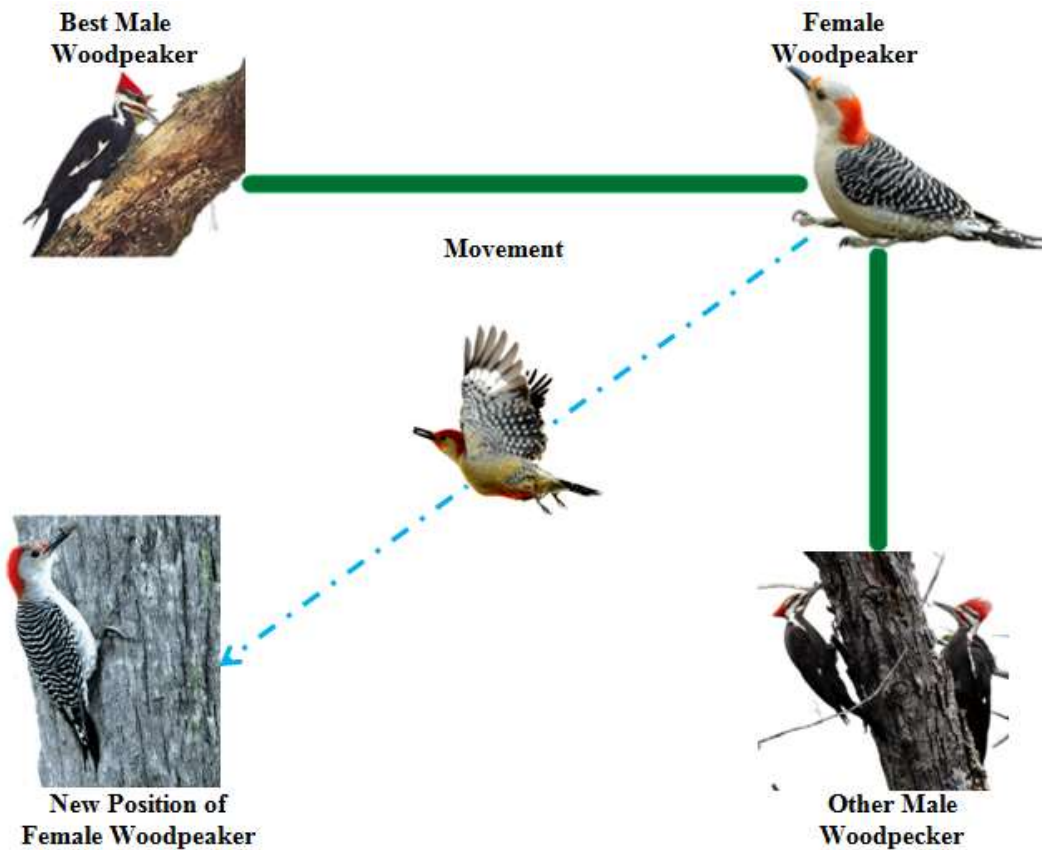


Fig 3.7: Position of Female Woodpecker [180].

Inspiration for WMA: By the red-bellied woodpeckers' intelligent mating behavior, WMA is inspired. The population is categorized into male and female groups. For communication, they deploy a particular strategy termed drumming or pecking the trees' trunks. For constructing nests along with feeding on insects, they make holes into the tree's trunk. Nevertheless, attracting mates in the mating season is the goal of drumming.

The Male starts drumming during the mating season. The enhanced sound by the male attracts the female; in addition, the male tries to attract along with selecting the best mate. In drumming, birds that have high capability could generate stronger, higher-quality drums; in addition, are considered ideal mates (their drums can be heard long along with could attract more females) [181]. For females, more powerful sound connects the male's higher capability of discovering food, and a nest, along with reproducing, making them an improved option as a mate. Grounded on the sound quality the female hears, the female size movement toward a male woodpecker takes place. At various intervals or several days, that procedure is repeated; the female gets closer to the male each time [182]. Sound waves are broadcast; thus, the other female might hear them as per the physics laws. The sound

intensity on which sound is received by a listener depends is termed the physical quantity. For the WMA, such kinds of concepts offered inspiration [183].

Sound Intensity of Woodpecker: By sound waves physics concept, the sound intensity was inspired. The quality or frequency of the sound produced along with received as waves are termed sound intensity in physics [180]. Relying on the producing sound waves' nature, the sound intensity might be low or high. For attracting females to mate, the drumming or pecking tree sound is generated by the male in WMA [182]. The female selects the male with the high sound intensity; while the male with low sound intensity isn't selected.

Distinguish between Male & female Red Bellied Woodpecker: For mating, the Population is classified into males and females. Regarding females, the male population is high initially. The population will be maximized by successful mating. Hence, diverse characteristics are included in males and females, which are as follows,

- **Male:** It has a red crown and nape, medium-sized black along with a white bar with a pale belly.

Female: It has a red nape, absence of the red crown, medium-sized black, together with white barred with a pale belly.

3.11.1 Proposed TWMA

The population is categorized into male and female in WMA. By pecking the trees' trunks termed drumming, the male communicates with females. The females are attracted by relying on the sound quality produced by the male. Thus, the male's sound intensity drum indicates its ability to attract more females. The female move toward the male birds; in addition, communication and flow of information betwixt them takes place by hearing the sound. The female will attract the male along with a move toward it if the male's sound intensity is closer to the female. Nevertheless, slow or premature convergence due to the loss of diversity within the population is a disadvantage in WMA. To update the female woodpecker's position during movement, Taxicab geometry is used; thus, the woodpecker population falling into local optimum could be avoided and also eliminates the slow or premature convergence in figure 3.8 TWMA is the enhancement made in general WMA.

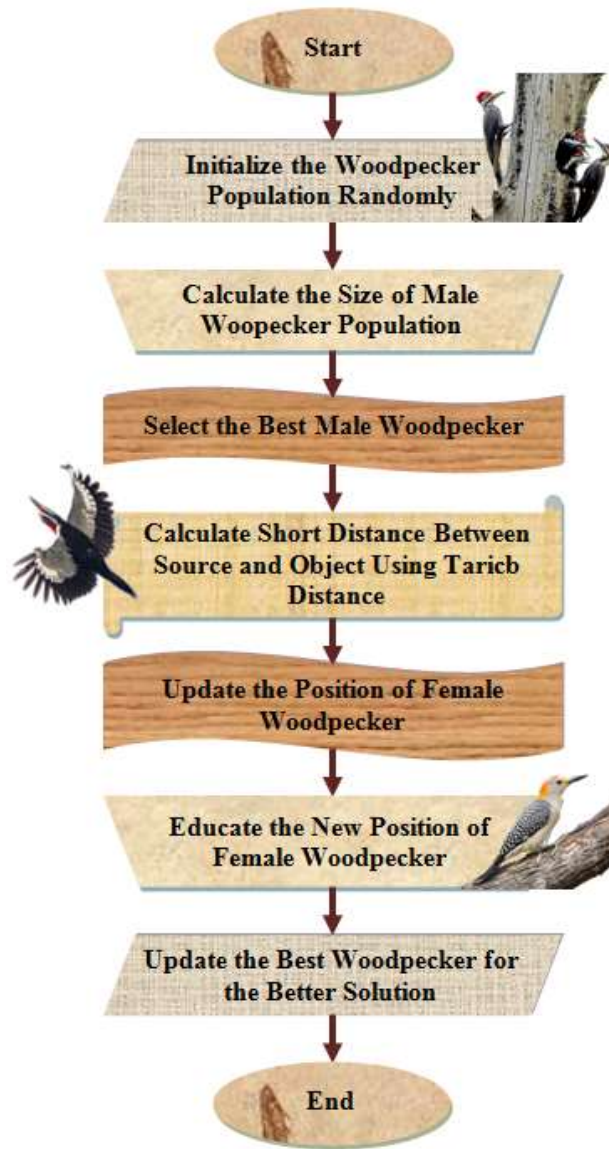


Fig 3.8: Flowchart of TWMA [179].

The steps of TWMA are detailed as follows.

Step 1: Initially, the woodpecker population (extracted features) is initialized as,

$$x_{(i)} = x_{(1)}, x_{(2)}, x_{(3)}, x_{(4)}, \dots \dots \dots, x_{(n)} \quad (3.7)$$

Here, the woodpecker population is depicted by $x_{(i)}$ and the woodpeckers in the population are signified by n .

Step 2: The fitness of each woodpecker is calculated for detecting the best woodpecker after population initialization. The woodpecker population is separated into male and female groups. The male becomes the search agent and the one with the uppermost fitness

is regarded as \mathcal{X}^* (the global best solution). Regarding classification accuracy, the fitness is calculated. The fitness evaluation $f(x_{(i)})$ is,

$$f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)}) \quad (3.8)$$

Step 3: By employing the below equation, the woodpecker's sound intensity is estimated.

$$\delta = \frac{2\pi^2 \gamma^2 A^2 DS}{\Psi} \quad (3.9)$$

Where, the sound intensity is signified by δ , the sound frequency is depicted by \mathcal{Y} , the sound amplitude is mentioned by A , the density of the medium by which sound is traveling is delineated by D , the sound speed is described by S , and the area of sound is expounded by Ψ .

Step 4: Grounded on the source's sound, the sound intensity of the woodpecker may change. A few sources may emit the sound in one direction. Consider a sphere in the region of a source with a radius ι . Via the sphere's surface, the sound waves will pass. The sound intensity (δ) is equated as,

$$\delta = \frac{2\pi^2 \gamma^2 \chi DS}{\psi \cdot 4\pi\iota^2} \quad (3.10)$$

Where the propagation rate of sound waves is signified by χ and the area of the sphere is depicted by $4\pi\iota^2$. Sound intensity depends on the distance betwixt the source and the object.

Step 5: The better sound quality received by the female woodpecker is signified by the shortest distance between the source and the object. For estimating the distance betwixt the source and object, the Taxicab distance is deployed; thus, the problem of premature convergence is surpassed along with obtaining the global best solution.

$$\iota = \sqrt{(x_m - y_f)} \quad (3.11)$$

Here, the sound source position (male woodpecker) is depicted by x_m and the listener position (female woodpecker) is mentioned by y_f .

Step 6: Regarding the male bird's sound intensity, the female updates its position. The position updating process ($y_{f,j}^{\tau+1}$) is equated as,

$$y_{f,j}^{\tau+1} = y_{f,j}^{\tau} + r * \frac{\alpha_{f,j}^{\tau} \langle \beta^{x^*} (y_{x^*}^{\tau} - y_{f,j}^{\tau}) + \beta_{m,i} (x_{m,i}^{\tau} - y_{f,j}^{\tau}) \rangle}{2} \quad (3.12)$$

Here, the female woodpecker population is depicted by $j=1,2,\dots,m$, the current position of j -th woodpecker in τ th iteration is signified by $y_{f,j}^\tau$, the position of the best woodpecker is delineated by $y_{x^*}^\tau$, the position of i -th male woodpecker is expounded by $x_{m,i}^\tau$, a random number uniformly distributed in the interval $[0, 1]$ is indicated by r , a self-tuned random factor of j -th woodpecker is mentioned by $\alpha_{f,j}^\tau$, the attractiveness of the female bird to the male bird is depicted by β^* and $\beta_{m,i}$.

Step 7: The self-tuning random factor $\alpha_{f,j}^\tau$ is estimated by using the below equation.

$$\alpha_{f,j}^\tau = r * \eta \quad (3.13)$$

$$\eta = ts \left(1 - \frac{\tau}{\tau^{\max}} \right) \quad (3.14)$$

Where the tangent sigmoid function is depicted by ts , the current, and the maximum number of iterations is modeled by τ, τ^{\max} , a random value in the interval $[-2\eta, 2\eta]$ be delineated by α . The search agent deviates from the target, which leads to exploration if $|\alpha| > 1$, and the female bird joins with the male bird, which leads to exploitation if $|\alpha| < 1$.

Step 8: The attractiveness (β) of male and females woodpeckers is equated as,

$$\beta = (1 + \delta(i, j))^{-1} \quad (3.15)$$

Where the sound intensity of i -th male woodpecker heard by the j -th female woodpecker is depicted $\delta(i, j)$. It is also termed the step size of the female woodpecker since it specifies the closeness of the female woodpecker towards the male, β lies in the interval $[0, 1]$, and the accurate movement of the female toward the male woodpecker is delineated by the lower β value.

Step 9: The male woodpecker population decreases at each cycle, and finally, only one woodpecker will remain. In the initial phase, a large male population increases the exploration. Thus, the exploitation and accuracy of the solution are maximized by the decreasing population. The population size ($x_{m,i}$) in each iteration is equated as,

$$x_{m,i} = \left[\text{round} \left(\frac{n}{2} * \left(1 - \frac{\tau}{\tau^{\max}} \right) \right) + 1 \right] \quad (3.16)$$

Here, the total woodpecker population is depicted by n , and the current and maximum number of iterations is signified by τ, τ^{\max} .

Step 10: In the end, one woodpecker and the global best woodpecker X^* is encompassed in the decreased population of woodpeckers. Thus, equation (3.12) can be modified as,

$$y_{f,j}^{\tau+1} = y_{f,j}^{\tau} + r * \langle \alpha_{f,j}^{\tau} \cdot (y_{x^*}^{\tau} - y_{f,j}^{\tau}) \cdot \beta_{m,i} \rangle \quad (3.17)$$

Step 11: There is a possibility of deviation in direction during the movement of the female woodpecker towards the male; in addition, by other woodpeckers or hunting birds, the female birds might be attacked. To protect itself from danger, the female bird may change their path. This random change in the pathway is termed Run Away. This random escaping movement of the woodpecker consists of two types of movements, which are based on the sound intensity of x^* male bird. The two types of movements (μ) are,

$$\mu = \begin{cases} R & \beta \geq \xi \\ P & \text{else} \end{cases} \quad (3.18)$$

Here, the runaway movement and X^* runaway movement are depicted as R, P .

$$\xi = 0.8 \cdot \frac{\sum_{j=1}^{m-1} \beta_{x^*}^j}{m-1} \quad (3.19)$$

Where the threshold for the sound intensity x^* is signified by ξ .

Step 12: The female's position obtained from the runaway is equated as,

$$\tilde{y}_{f,j} = L - (L - U) * r \quad (3.20)$$

Where the position of j -th the woodpecker after the runaway is delineated by $\tilde{y}_{f,j}$, a random number in the uniform distribution [0, 1] is indicated by r and the upper and lower bounds of variables are denoted by L, U .

Step 13: The X^* runaway movement is denoted further,

$$P = \phi * \left(1 - \frac{\tau}{\tau^{\max}} \right) \quad (3.21)$$

Here, the runaway coefficient is depicted by ϕ . The position of a female woodpecker from x^* the runaway movement ($y_{f,j}^{x^*}$) is equated as,

$$y_{f,j}^{x^*} = y_{f,j}^{\tau} + P^{bit} \langle y_{x^*}^{\tau} - y_r \rangle \cdot B \quad (3.22)$$

$$P^{bit} = \begin{cases} 1 & r \leq P \\ 0 & else \end{cases} \quad (3.23)$$

Where, a random number in the uniform distribution [0, 1] is depicted by r and a random number [-1, 1] is signified by B . Until the stopping criterion is met by comparing the position of i -th woodpecker with the former position together with the position of the best woodpecker, the process continues. Next, the better position is replaced with the other position. In the end, the optimal solution is obtained, i.e., the selected best features ($X^{(k)}$) are equated as,

$$X^{(k)} = X^{(1)}, X^{(2)}, \dots, X^{(K)} \quad (3.24)$$

Here, the number of features selected for further classification is signified by K . In figure 3.9, the proposed TWMA's pseudo-code is depicted.

Pseudocode for Proposed TWMA

Input: Extracted Features $x_{(i)}$

Output: Selected features $(X^{(k)})$

Begin

Create the initial population of woodpeckers

Compute $f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)})$

Obtain x^* based on $f(x_{(i)})$

While (stopping condition is not satisfied) **do**

Partition $x_{(i)}$

For $1 \leq i \leq n$

Determine the sound intensity δ

Compute Taxicab distance

Choose $x_{m,i}$ (i -th male woodpecker)

Evaluate β^{x^*} and $\beta_{m,i}$

Analyze $\alpha_{f,j}^z = r * \eta$

Update woodpeckers' position $(y_{f,j}^{z+1})$

Calculate sound intensity threshold ξ

If $\beta^{x^*} > \xi$

Estimate $\tilde{y}_{f,j} = L - (L - U) * r$

Else

Find out x^* runaway movement $(y_{f,j}^{x^*})$

End if

Appraise the new position of $y_{f,j}$

Renew x^*

End for

$\tau = \tau + 1$

End while

Obtain global best solution $(X^{(k)})$

End

Fig. 3.9 Pseudo-code of the Proposed FS Technique [184].

3.12 Classification using BReLU-ResNet

ANN's structural design is CNN. The visual cortex's several features are deployed by CNN. Estimating the input images' class labels is a significant role in image classification. In the sequence of convolutional (Conv), nonlinear, pooling, together with Fully Connected (FC) layers, the images are accepted; then, the result is generated. The CNN's initial layer

is the Conv layer [185]. Via the pixel value, an image is depicted as a matrix. Fewer matrixes are selected, which is termed a filter (neuron or core). Convolution is engendered by the filter where the input image is presented. Develop the values with actual pixel values; in addition, each multiplication is added. It goes additional right with 1 unit executing the same function since the filters have interpreted the image from the upper left corner. A matrix is attained behind passing the filter; nevertheless, when weighed against the input matrix, it is reduced. Detecting edges and colors are analogous. Several Conv networks differed by nonlinear and pooling layers are encompassed in the system. The initial layer's outcome will become the 2nd layer's input if the image exceeds 1 Conv layer; in addition, it takes place with every further Conv layer. Every convolution function is followed by the nonlinear layer. The activation function, which deploys nonlinear property, is included in it. Then, the pooling layer is implemented. By employing width and height, it has functioned; in addition, executes the sampling function. The image volume is eradicated due to the result. A definite image won't require the extra procedure if it is applied while some features are analyzed in the prevailing Conv function; in addition, it could be minimized to lesser definite pictures. In networks, the resultant data is achieved in the FC layer. An N-dimensional vector is offered by connecting an FC layer to the final stage in which the number of classes as of which the desired classes could be enhanced is signified by N.

The 1st single-channel Residual Networks (ResNets) were exhibited in 2015. It is now extensively accepted as one of the modern DL techniques. Easy network optimization along with higher accuracy was provided by that technique. For the ILSVRC competition, the network called ResNet was the baseline of submissions in which, for the task of ImageNet detection along with localization, it won the 1st prize. Initial operations like convolution and max-pooling are performed by every ResNet after stacked convolutions. It solved the vanishing gradient issue.

Instead of investigating the unreferenced changes, it learns the residual operations concerning input layers, which is the key factor of ResNet. The aspects of ResNet are high accuracy, better optimization, and computational efficiency. One of the key advantages is that by using knowledgeable low-level frame extractors as an alternative to initialize with random weight.

The ultra DNN's training is stimulated since the ResNet is productive along with developing accuracy [186]. From CNN's depth, the ResNet is evolved, which caused degradation problems. While enhancing the depth and minimizing the accuracy, the

accuracy is maximized; in addition, it is regarded as a demerit. The error might be discarded that is deeper along with doesn't provide maximal training samples error while a shallow network suffers the accuracy of saturation along with includes congruent mapping layers [187]. Conveying the prevailing outcome to the upcoming layer with the assistance of congruent mapping is the goal. To solve the degradation and gradient vanishing problem, the residual block is implemented by ResNet. Under the input inclusion and residual block's output, those blocks in ResNet perform the left-over ones. In figure 3.10, the structure of the ResNet is depicted.

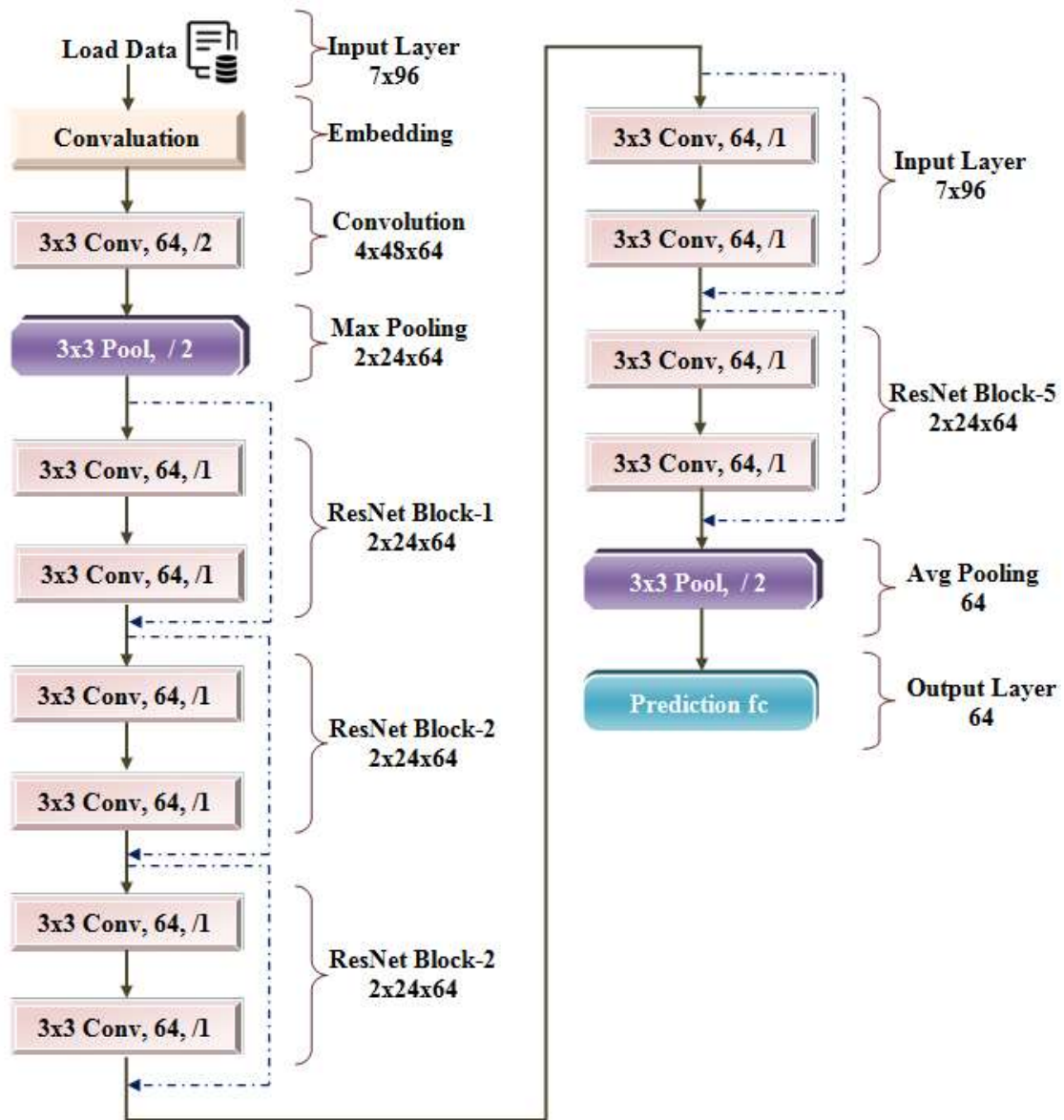


Fig 3.10: RESNET Architecture [184].

By presenting a “Residual block” that features a “skip connection”, that inserts the output of the current layer to the front layer, the ResNet handles those issues. For equalizing the dimensions of the short-cut connection along with the output layer, x is multiplied by a linear projection W if x and (x) below do not have the same dimension. Even with far more layers than typical CNN, the network can maintain stability in figure 3.11.

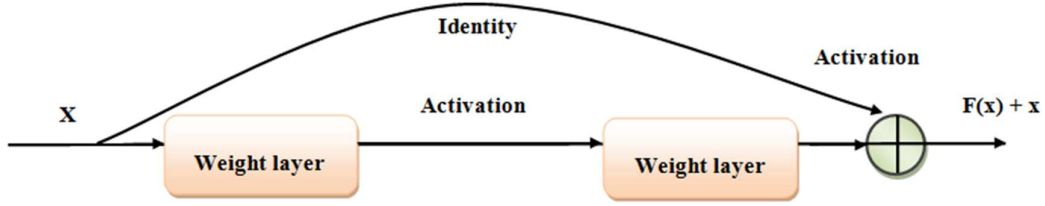


Fig 3.11: Residual Network Building Block [184].

3.12.1 Proposed BReLU-ResNet

For categorizing the attacked data from the on-attacked data, the selected features $(X^{(k)})$ are fed into the BReLU-ResNet. Since ResNet surpasses the degradation caused due to the rise in network depth, it is wielded for classification. Convolutional, batch normalization, max pooling, flattening, and activation layers are encompassed in the ResNet. Initially, the selected features are inputted to the ResNet, the input is convoluted with the $2*2$ filter in the convolutional layer, and it produces the output with reduced feature dimension. The result achieved as of the convolutional layer is given to the batch normalization layer in which the network time is stabilized along with epochs minimized. In convolutional and batch normalization, there are ‘3’ layers. The data is given to the max-pooling layer, which down-samples the data. For categorizing the results, the FC layer includes the average pooling and softmax layer. Nevertheless, owing to the activation function’s randomized nature, ResNet has an over-fitting issue. In the ResNet, Bernoulli’s value is used in the Leaky Rectified Linear Unit activation function instead of a random value. This modification in baseline ResNet is called BReLU-ResNet

Let $(X^{(k)})$ be the input features and a filter (Γ) of size (a,b) is used in the convolution layer, which is equated as,

$$conv(X^{(k)} * \Gamma) = \sum_{k=1}^K (X^{(k)} - a, X^{(k)} - b) \cdot \Gamma(a,b) \quad (3.25)$$

- A significant part of neural networks is the activation function. The BERLU activation function $(f(X^{(k)}))$ is equated as,

$$f(X^{(k)}) = \max(0, b(X^{(k)})) \quad (3.26)$$

Here, Bernoulli's distribution function is delineated by $b(X^{(k)})$.

$$b(X^{(k)}(p, o)) = p \cdot o + (1 - p)(1 - o) \quad (3.27)$$

Where the probability and the possible outcome $(X^{(k)})$ is signified by p, o .

- In the BERLU-RESNET, the network layers are capable of approximating any function asymptotically. The approximation of residual function $\partial X^{(k)}$ is,

$$\partial X^{(k)} = f(X^{(k)}) * X^{(k)} \quad (3.28)$$

Where the target function is depicted by $f(X^{(k)})$.

$$f(X^{(k)}) = \partial X^{(k)} + X^{(k)} \quad (3.29)$$

The attacked data is separated from the normal data by the classifier's output; then, by employing the Bait, the attacked data is stored in the SLF. By deploying the Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC), the normal data is encrypted. To transfer data in the cloud effectively, the shortest path betwixt every node is estimated.

3.13 Data Encryption Using ESHP-ECC

By employing the Hashed ECC, the data is securely accessed. In retrieving the info, security is significant. The secure access utilizing hashed ECC is delineated further.

3.13.1 Secure Access ECC

To deploy Elliptic Curve (EC) Cryptography (ECC) as the baseline for discrete logarithm-centric cryptosystems was presented by Victor Miller and Neal Koblitz [188-189] at the University of Washington 1985. In several cryptographic contexts like integer factorization and primarily proving, elliptic curves were deployed already. The science of keeping information secure is termed cryptography in a nutshell; thus, for cloud computing security, it is a helpful tool. To transmit over the Internet to the rightful recipients, encryption and decryption of messages were encompassed. To encrypt and decrypt the transmitted data information, any cryptographic scheme's secrecy is significant usage. Even though a few organizations believe in having the algorithmic key a top secret via encryption, most cryptographic algorithms are openly accessible. In the elliptic curve, the ECC discrete

points over a finite field are deployed as a cyclic group. By employing ECC, every kind of public cryptography-centric scheme could be implemented as analogous. When weighed against other cryptosystems, the popularity of ECC is owing to the determination, which is grounded on a harder mathematical issue. For the conventional public-key cryptosystem like RSA and DSA, it is an alternative in which the factorization or the discrete log issue could be resolved in sub-exponential time. When analogized to competitive systems like the RSA and DSA, the smaller parameters could be wielded in ECC.

With a smaller key size, the same SL is provided by ECC; thus, in limited environments such as mobile phones, sensor networking, and smart cards, enhanced performance is caused. While considering RSA with a key size of 1024 bits, the ECC with a key size of 160 bits offers the same SL. Scalar multiplication is encompassed by the main agreement, signature generation, and signing, together with verification; in addition, they are the elliptic curve's key operations. In the entire system's efficacy, scalar multiplication plays a significant role. In a few environments like limited devices, and central servers, rapid multiplication is significant in which a large number of key agreements, signature generations, along with verification take place. On the complexity of the EC Discrete Logarithm Problem (ECDLP), the ECC's security strength depends. Point doubling and adding operations are encompassed in scalar multiplication, which was adopted by ECC that are computationally more effectual when weighed against RSA exponentiation. For understanding the ECC along with breaking the security key, the ECC's complexity puts the attacker in difficulty.

ECC helps to develop equal security with less battery usage and computing power. The category of security mechanism, which creates a hash value, checksum value, or message digest for specific data, is signified by the hash function. For increasing the security strength, hashing is integrated with ECC. A kind of mechanism, which is espoused in public-key cryptography employment, is termed ECC. With the utilization of a prime number function, that methodology is grounded on a curve with specific base points. In figure 3.12, the functions are deployed as a maximal limit.

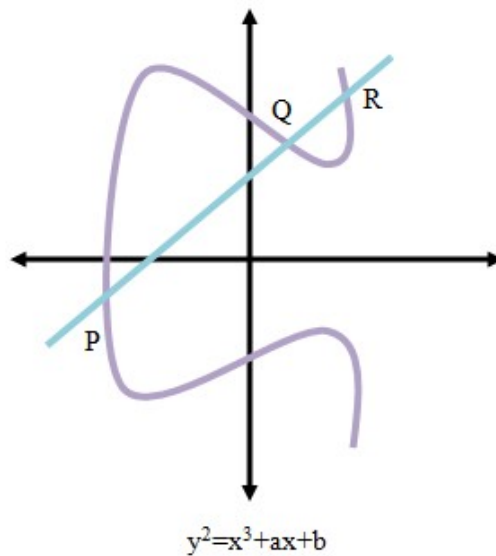


Fig 3.12: Elliptic Curve [154].

By employing the hashed ECC system, the data is accessed securely. Hashed ECC, which is a public key encryption method, grounded on the EC theory could be deployed for generating faster, smaller, and more efficient cryptographic keys. Rather than the prevailing technique, keys are generated via the properties of the EC equation by hashed ECC as the product of very large prime numbers.

3.13.2 Encrypted Secure Hash Probability

Secure Hash Algorithm (SHA) is the name of a series of hash algorithms; in 1993, the SHA-1 was presented [141]. A 160-bit hash value was generated by SHA-1. SHA-1 also has weak collision avoidance similar to MD5. In 2001 SHA-2 was developed [190]. SHA-224, SHA-256, SHA-384, along with SHA-512 are termed after the length of the MD each creates is encompassed in SHA-2.

From an arbitrary length string, a 160-bit hash value is generated by SHA-1. Huge applications namely SSH, SSL, and S-MIME (Secure / Multipurpose Internet Mail Extensions), together with IPsec are deployed by it similar to MD5. It is computationally infeasible of detecting a message, which relates to a given MD or to detect '2' messages, which generate a similar message digest, which is the basis behind the security of SHA-1. Nevertheless, this principle is no longer valid. For replacing the present 160-bit version, more secure variations of SHA-1 are verified when there are no successful attacks on SHA-

1. With the numbers reflecting the strength of the MD engendered on the application, SHA-256, SHA-384, together with SHA-512 are encompassed in it.

The superior version of the previous hash system termed SHA 0, SHA 1, SHA 256, as well as SHA 384 is this system. A function, which gathers the input data of any size along with generates the Message Digest (MD) of 512-bit size along with 1024-bit block length is termed the SHA-512. To form various 1024 bits, the message bits are enlarged with an extra system. This block is categorized into smaller parts of 1024 bits. With the generated hash code, the key block is incorporated with the initializing vector. With the previously created hash codes, further blocks are incorporated. Concerning the generated hash values allied with the closed frequent patterns, the hash tree is constructed. To index in a hash tree, hash values are utilized significantly. The closed frequent patterns indexed with a related hash value are depicted by every leaf node.

Hashing algorithms, which is also termed one-way encryption, deploy no key. For authenticating messages, digital signatures, and documents, hashing is employed. MD is referred to as a hash function that accepts a variable-length block of data as input and produces a fixed-length hash value. A function, which produces MD 512-bit size together with 1024-bit block length, is termed SHA 512 hash function. To accept input in the form of a message with any length or size, the cryptographic system operates with the SHA 512; in addition, MD, which has a fixed length of 512 bits, is generated. SHA- 512 works on a message in 1024-bit blocks along with generating a 512-bit MD. 2^{128} bits is the maximal message length acceptable.

3.13.3 Proposed ESHP-ECC Algorithm

A public-key cryptosystem grounded on the EC hypothesis that is secure asymmetric encryption deployed for data security is termed the ECC. Via EC properties, public along with private keys are produced for every user. For encrypting and decrypting the data, those keys are employed. The keys are generated randomly in ECC. Hence, the main information might be hacked easily. Grounded on the engendered key value, the probability of ones and zeros is produced. By employing secured hashing, the key values are converted into a hash value in figure 3.13. The proffered system is termed the ESHP-ECC owing to the modifications in the general ECC. The ESHP-ECC's encryption process is detailed below,

- Initially, for key generation, the EC equation was used.

$$Y^2 = X^3 + aX + b \quad (3.30)$$

a, b signifies the integers.

- Next, a random number (η) is generated $[1, n-1]$ and the probability of ones and zeros of this random number is calculated as the private key. the public key (ρ) is equated as,

$$\rho = \eta * B \quad (3.31)$$

Where the point on the EC is signified by B .

- Then, by using secure hashing, these public and private keys are converted into a hash value. A cryptographic hash function, which considers the keys as the input together with produces a 160-bit (20-byte) is termed SHA. The private and public keys are represented as η'' and ρ'' .
- Let, the message to be transmitted is depicted by M and it has the point Q on the EC. Randomly select σ from $[1, n-1]$. '2' cipher-texts $(C^{(1)}, C^{(2)})$ are calculated using the below equations.

$$C^{(1)} = \sigma * B \quad (3.32)$$

$$C^{(2)} = Q + \sigma * \rho \quad (3.33)$$

Here, the encrypted message, which is transmitted to the cloud server via the shortest path, is delineated by $(C^{(1)}, C^{(2)})$.

Input: Attack free message M
Output: Encrypted data $(C^{(1)}, C^{(2)})$

Begin
For each M
 Perform key generation
 Define the elliptic curve equation $Y^2 = X^3 + aX + b$
 For $1 \leq \eta \leq n - 1$
 Generate (η)
 Compute the probability of ones and zeros of (η)
 Estimate the public and private keys $\rho = \eta * B$
 For each η, ρ
 Carry out SHA hashing
 Attain η'' and ρ''
 End for
 End for
 Execute data encryption
 Select randomly σ from $[1, n - 1]$
 Calculate $C^{(1)} = \sigma * B$
 Attain the cipher text $C^{(2)} = Q + \sigma * \rho$
End for
Recognize the encrypted message $(C^{(1)}, C^{(2)})$
End

Fig 3.13: Pseudo-codes for Proposed ESHP-ECC [149].

For example consider a text message Hello World.

Its equivalent ASCII values are: {104, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100}

Using the formula $Y^2 = X^3 + aX + b$ the keys are generated. Consider $a=0$, $b=7$ and the number which is converted above is considered as X .

Using the randomly selected values from the above converted value and product of the probability of the ones and zeros of the binary values of the number is private key and the multiplication of the private key with the randomly selected number is now our public key.

Using the SHA 256 and the public key the Hash code will be generated. The generated hash will be b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9.

And using the decryption technique the hash b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9 will be decrypted to get the original message Hello World.

3.14 Shortest Pathway Calculation

The number of sensor nodes available to transmit the encrypted message is signified by $(x_i = x_1, x_2, \dots, x_N)$. For efficient data transmission and for minimizing the computational time, the shortest path between each sensor node is identified. Thus, for calculating the distance, ED $E^{(d)}$ is wielded.

$$E^{(d)} = \left\| (x_i - x_j) \right\|^2 \quad (3.34)$$

Where the j -th node is depicted by x_j . The shortest pathway obtained is used to transmit the encrypted message after distance computation. By employing DSHP-ECC, this encrypted message is decrypted at the receiver side.

3.15 Decryption through DSHP-ECC

The encrypted message is decrypted using the below equation,

$$Q = C^{(2)} - \eta * C^{(1)} \quad (3.35)$$

Here, the original message is depicted by Q .

3.16 Attack Mitigation System Based on Bait Approach

For sending a fake Route Request (RREQ) to the Bait RREQ, the Bait is deployed for enticing a Malicious Node (MN). Attack node detection along with the mitigation process is done by this process. Amongst source and destination, secure routing is required in the transmission process. For transmitting the packets to the destination, routing protocol helps; in addition, collaborative black hole attacks also affect them. Collaborative attacks are the MN that performs together and drops the packets. By transmitting Bait RREQ to the suspicious node, the confirmation of the suspicious node as an MN is done by confirming the node. It is marked as an MN along with its buffered route reply is leftover if it replies

to the Bait RREQ or else, it is forwarded to the source node. Hence, the forged route reply sent as an MN is discarded along with securing the route discovery process. For reaching the target, the MN publicized them as the optimal and shortest path. The RREQ packets that aren't legal are sent to the source by the malicious nodes. Thus, via the closest neighbor nodes, the source node sends the Bait request to the destination address. Though it is not the destination node, it replies to the request once the request reaches the malicious node. This request serves as the lookup's input for the flow table. Both the detection and mitigation of the assault take place. Getting the response from the malicious node, the source node compares it to the destination address. The source node considers it as the MN and rejects the reply request if the addresses are not matched. The data transfer occurs effectively if an attacker node is found. While the intermediary, non-attacker nodes get the RREQ packets, it is passed to the target node with their address. The data transmission takes place as the shortest path between the source and the destination is found. The Bait's architecture is seen in figure 3.14.

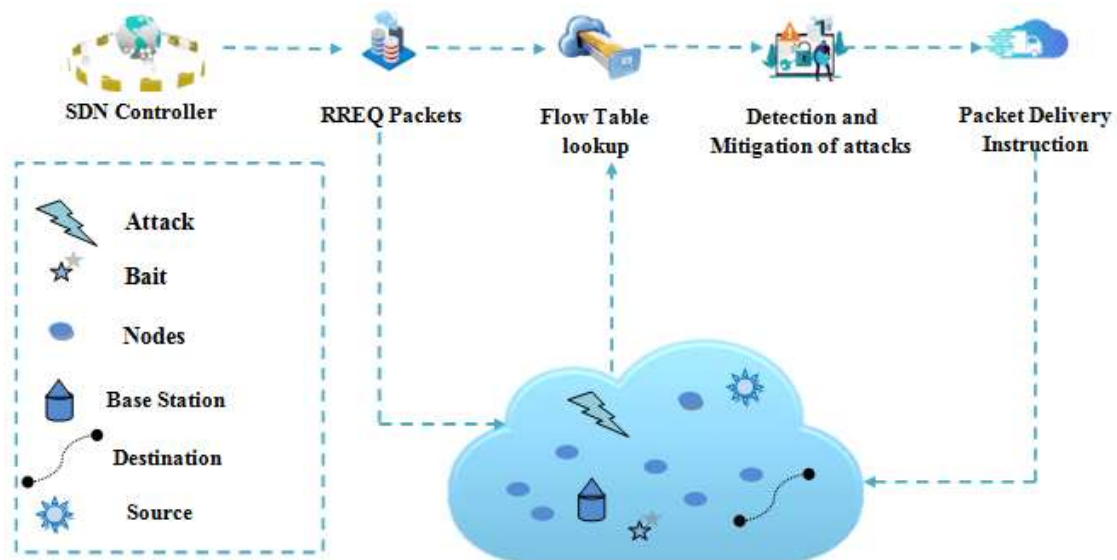


Fig 3.14: General Structure of Bait [184].

The test data is first checked with the security log file during testing. The data is blocked from further processing if the source IP address of the data is already present in the security log file. Cyber-attack detection and mitigation are done if it is not present in the security log file.

3.17 Conclusion

This chapter deals with the conceptual model of the proposed design and explains the different parts of the model. The chapter explain the algorithms used to compare the proposed model with the prevailing systems. The chapter also deals with how the features are extracted, how the features are selected using TWMA algorithm. The chapter also includes how classification of attack and normal data are made using proposed BReLU-ResNet algorithm. The chapter also explains how the data is encrypted and decrypted using proposed SHP-ECC algorithm and also explains the identification of shortest path to transfer the data in-between the source and destination using Euclidian distance algorithm. The chapter describes how the attacks are mitigated using Bait approach.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Introduction

It is a challenging task to detect such threats in a wireless network. Current wireless attacks are highly sophisticated and passive; in addition, highly persistent to evade traditional security systems. It is a huge challenge to investigate targeted and sophisticated attacks via statistical modeling. It is tedious to recognize those attacks by employing the prevailing detection methodology. The novel features of the attackers and attack behaviors aren't regarded by the analytical strategies deployed in the prevailing IDS.

For enhancing resilience along with warranting constant production with the required specifications, precise CAD in modern industrial systems is indispensable. Nevertheless, to detect malicious attacks, basic IDS grounded on shallow ML are constrained. The suspicious activities' related features could be studied by the proffered stacked DL along with could determine them as usual activities.

The proposed technique's complete examination of the outcome is delineated. To prove the efficacy, the performance along with comparative evaluation is done. The system is implemented by using MATLAB. The data are attained from the UNSW-NB15 dataset that is openly available. Further, the implementation of the intended method with the prevailing algorithm is discussed elaborately.

4.2 Programming Background

By employing a superior performance estimating platform, which deployed the power of a Central Processing Unit (CPU) along with a Graphical Processing Unit (GPU) with the Radeon Vega Mobile Gfx graphics card's multicore structure, experiments were performed for analyzing the system's performance. In the working platform of MATLAB, SAR Image Change detection methodology is deployed with machine configuration.

- Processor: AMD Ryzen 5 3500U
- CPU Speed: 2.10 GHz
- OS: Windows 10
- RAM: 8GB

4.3 Database Description

To generate a hybrid of real modern ordinary activities together with synthetic contemporary attack behaviors, the UNSW-NB 15 dataset's actual network packets were produced in the Australian Centre for CS (ACCS) Cyber Range Lab by utilizing the IXIA Perfect Storm tool. In 2015, the UNSW-NB15 computer network security dataset was made public. 2,540,044 realistic modern normal and anomalous (commonly known as attack) network events comprise this dataset. IXIA traffic generator used three virtual servers to compile these records. Two servers were set up to distribute regular network traffic, while a third was set up to produce unusual network traffic.

Argus and Bro-IDS initiatives collaborated to extract 49 features from the raw network packets, including both flow-based and packet-based characteristics. The packet header and its payload (also known as packet data) are used to extract packet-based characteristics. In contrast, flow-based characteristics are created by sequencing packets as they go across the network from a source to a destination. The three most crucial properties in the formulation of a flow-based feature are direction, inter-packet length, and inter-arrival times: Two illustrations of flow-based characteristics are the overall duration and the destination-to-source-time-to-live. The features are divided into three groups: the fundamental features (6–18), the content features (19–26), and the time features (27–35). Features 36 through 40 and 41 through 47 are referred to as connection features and general-purpose features, respectively. While connection characteristics show the characteristic of the relationship of 100 consecutively arranged records, general purpose features are those attributes meant to illustrate the purpose of a certain record. The final two aspects are labels and attack categories.

Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, and Worms are the different types of attacks. 2,218,761 records are used to represent typical assaults, whereas 24246, 2677, 2329, 16535, 44525, 215481, 13987, 1511, and 174 records are used to represent fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, and worms signatures, respectively. As a result, there is a significant lack of balance in the dataset as Normal records make up 87% of it while Worms records make up just 0.007%. The dataset's creators additionally subsampled and divided it into training and testing subsets, as shown in Table 4.1, a technique used by other researchers.

Table 4.1: UNSW-NB15 Dataset [53].

Category	Testing Set	Training Set
Normal	37000	56.000
DoS	4089	12.264
Generic	18.871	40.000
Backdoor	583	1.746
Shellcode	378	1.133
Reconnaissance	3.496	10.491
Worms	44	130
Exploits	11.132	33.393
Analysis	677	2.000
Fuzzers	6.062	18.184
Total Records	82.332	175.341

The UNSW website has access to the dataset. Compared to previous benchmark datasets like DARPA98, KDDCUP 99, and NSL-KDD, among others, this dataset's structure is more complicated. As a result, the UNSW-NB15 is enhanced to provide a more thorough assessment of the current network intrusion detection technologies.

4.4 Performance Metrics

Evaluation of a machine learning model's performance is one of the key stages in its development. The efficiency or caliber of the model is evaluated using a variety of measures, sometimes referred to as performance metrics or evaluation metrics. These

performance metrics allow us to assess how successfully our model processed the given data. We can improve the model's performance by modifying the hyper-parameters. Performance indicators provide a way to gauge how effectively a machine learning (ML) model generalizes to fresh or unstudied data.

To evaluate the performance, performance metrics like precision, F-score, TPR, recall, precision, and accuracy, together with False Positive (FP) Rate (FPR) are deployed [191]. By recognizing the performance parameters' discrete numbers, the performance analysis is done. True Positive (TP), FP, False Negative (FN), along with True Negative (TN), which are usually deployed for comparison are encompassed in the confusion matrix. In table 4.2, the detailed description of each of these parameters is elucidated in figure 4.1.

Table 4.2: Confusion Matrix Analysis

		Predicted class	
		Normal	Attack
Actual Class	Normal	True Negative (TN)	False Positive (FP)
	Attack	False Negative (FN)	True Positive (TP)

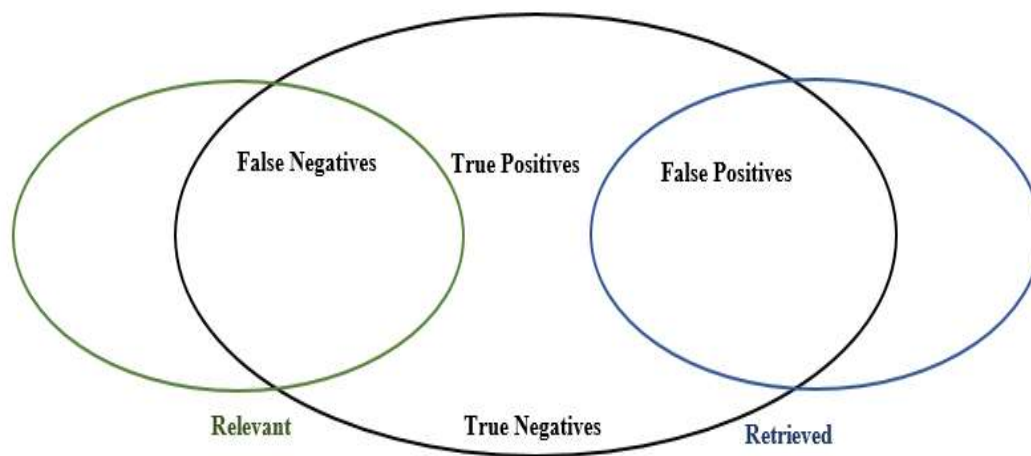


Fig 4.1: Diagrammatic Representations of TP, TN, FP, and FN Regarding Relevant and Retrieved Docs.

For estimating performance evaluation metrics that have less significance when analogized to the accuracy metric like the classification accuracy (detection rate) (the percentage of associated instances (for example., attacks) amongst the retrieved instances); the classification recall (sensitivity) (positive instances percentage, which is labeled correctly); the F1-score (the average score like the precision) and recall (that is., deploys FN and FP); FRR (the percentage of misclassified normal instances detected), the confusion matrix parameters like TN, TP, FN, along with FP were wielded.

In this matrix:

- True Positive (TP): The number of instances that are correctly classified as "attack."
- False Positive (FP): The number of instances that are incorrectly classified as "attack" when they are actually "normal."
- True Negative (TN): The number of instances that are correctly classified as "normal."
- False Negative (FN): The number of instances that are incorrectly classified as "normal" when they are actually "attack."

Each cell in the matrix represents a count of instances, indicating the number of samples that fall into each category based on their actual and predicted class labels. The confusion matrix provides crucial information for evaluating the performance of a classification model in distinguishing between attack and normal data.

The general performance metrics were espoused to discriminate cyber-attacks for monitoring the investigated schemes' detection performance.

Precision:

It is the degree to which common measurements under unaltered conditions reveal the same results [192].

$$\rho = \frac{TP}{TP + FP} \tag{4.1}$$

Recall:

The percentages of positive patterns, which are suitably retrieved by the cloud server with the request from the data user, are calculated [192].

$$\gamma = \frac{TP}{TP + FN} \tag{4.2}$$

F-Score:

It is a measure, which merges precision as well as recall. The F1-score combines the accuracy and recall of a classifier into one statistic by computing their harmonic means

[193]. It is mostly used to contrast the potency of two classifiers. Assume the recall and accuracy of classifiers A and B are greater. It is possible to determine which classifier produces better results in this scenario by comparing their F1 scores.

The following formula is used to determine a classification model's F1 score [192]:

$$F - Score = 2 \left(\frac{\rho \cdot \gamma}{\rho + \gamma} \right) \quad (4.3)$$

Sensitivity:

It is the proportion of true positives, which are suitably determined by an attack. How better the system is at retrieving the search outcomes is depicted by it. Sensitivity is used to evaluate model performance since it allows us to see how many situations the model correctly identified [191]. A model with high sensitivity may be missing some of the positive cases if there are few false negatives. In other words, sensitivity evaluates how effectively a model can distinguish between good data. This is critical because our models must be able to recognize all of the positive examples to provide accurate forecasts. The sum of the false negative rate and the sensitivity is one. The model performs better at correctly detecting positive cases the greater the true positive rate. The following formula can be used to calculate sensitivity or true positive rate mathematically [192]:

$$Sensitivity = \frac{TP}{TP + FN} \quad (4.4)$$

A high sensitivity means the model is correctly detecting the majority of the positive findings, whereas a low sensitivity means the model is missing a substantial chunk of the positive discoveries. A higher true positive and a smaller false negative would be indicative of greater sensitivity. A lower sensitivity number would result in a higher false negative and a lower true positive value.

Specificity:

When evaluating model performance using sensitivity, sensitivity and specificity are typically compared. It is the percentage of accurately recognized true negatives. Specificity is the proportion of genuine negatives that the model successfully identifies [192]. This means that more real negatives, often known as false positives since they were originally believed to be positive, would be recorded. A True Negative Rate is another name for this proportion (TNR). The sum of the specificity (real negative rate) and false positive rate would always be one. High specificity implies that the model is properly recognizing the bulk of the negative outcomes, whereas low specificity suggests that the model is

mislabeling a significant percentage of negative findings as positive. Mathematically, specificity may be computed as follows [192]:

$$\text{Specificity} = \frac{TN}{FP + TN} \quad (4.5)$$

A very high specificity or true negative rate would be ideal for the model. Greater specificity would lead to a higher real negative value and a lower false-positive rate. Higher false positive and lower true negative values would follow from a lower specificity number.

Accuracy:

It is the proportion of true outcomes, either TP or true negative. The degree of exact response is depicted by it [192].

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (4.6)$$

False Acceptance Rate:

The gauge of the likelihood in which the system would wrongly respond with unpredicted outcomes is termed the False Acceptance Rate (FAR). The false acceptances divided by the identification attempts are termed the system's FAR.

False Rejection Rate:

The gauge of the chance in which the system will wrongly reject the attempt of the request made by the data user is termed the False Rejection Rate (FRR). The ratio of false rejections alienated by the recognition attempts is termed the system's FRR [193].

$$MCC = \frac{(TP * TN) - (FP * FN)}{(TP + FP)(TP + FN)(TN + FP)(TN + FN)} \quad (4.7)$$

False Positive Rate:

The computation of the fraction of the measures of negative events imperfectly classified as positives to the aggregate measure of TN trials is termed the FPR [193].

$$FPR = \frac{FP}{FP + TN} \quad (4.8)$$

The exact detection proportion is appraised by the accuracy. Extremely satisfying overall ID is signified by superior accuracy. The ability to detect cyber-attacks precisely is called sensitivity. In binary classification, recall is similar to sensitivity. The proportion of actual negatives, which are detected precisely, is termed specificity. The ability to discriminate typical observations precisely is specificity. The relevance of the detected positives is signified by precision. The harmonic average of precision and sensitivity is depicted by the F1 score.

Matthews Correlational Coefficient:

The Matthews correlation coefficient is used in machine learning to assess the precision of binary and multiclass classifications. Because it takes into account both accurate and inaccurate positives and negatives, it is generally viewed as a balanced measure that can be used even when the classes are of drastically different sizes. The MCC is just a correlation coefficient with a value between -1 and +1 [191]. Inverse prediction is represented by a coefficient of -1, perfect prediction by a coefficient of 1, and random prediction at random by a coefficient of 0. The phi coefficient is another name for the statistic.

Following are the calculations for Matthew's correlation coefficient [191]:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \quad (4.9)$$

4.5 Confusion Matrix of ANFIS algorithm

ANFIS, which is a hybrid model composed of a fuzzy and artificial neural network, aims to determine the behavior of imprecisely complex dynamic systems and to deal with engineering problems. The confusion matrix is a performance evaluation tool used to assess the accuracy of classification algorithms, including the Adaptive Neuro-Fuzzy Inference System (ANFIS). The confusion matrix presents the actual and predicted class labels in a tabular format, making it easier to understand the model's performance in a binary classification problem, such as distinguishing between "attack" data and "normal" data.

Let's consider an example where we want to use ANFIS to classify network traffic data as either "attack" or "normal."

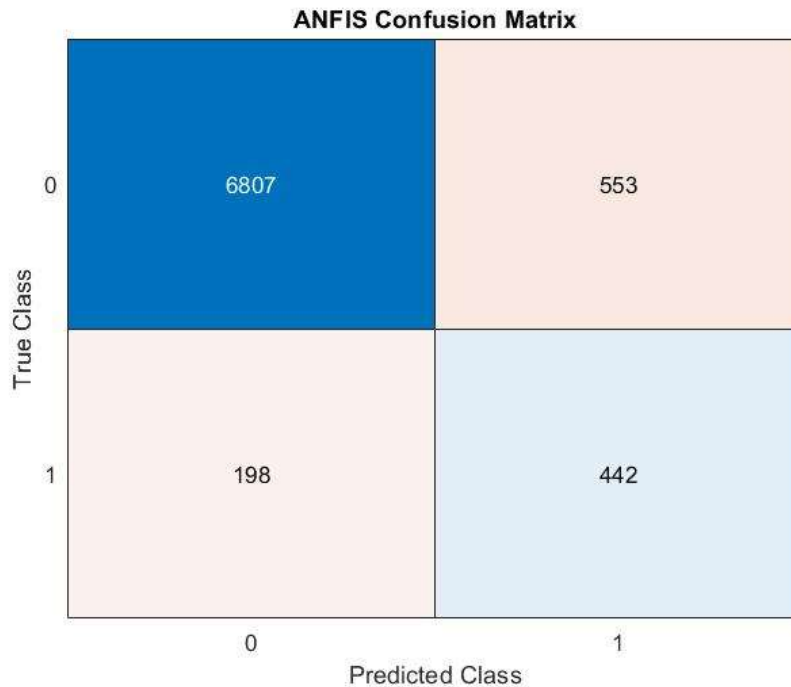


Fig 4.2: Confusion matrix of ANFIS algorithm over attack and normal data.

Suppose we have a dataset of 8000 network traffic instances, and we use ANFIS to classify them as either "attack" or "normal." After training and testing the ANFIS model, we obtain the following results:

- True Positive (TP): 442 instances correctly classified as "attack."
- False Positive (FP): 553 instances incorrectly classified as "attack" when they are "normal."
- True Negative (TN): 6807 instances correctly classified as "normal."
- False Negative (FN): 198 instances incorrectly classified as "normal" when they are "attack."

Now, we can calculate various performance metrics using the values in the confusion matrix:

1. Accuracy: $(TP + TN) / \text{Total} = (442 + 6807) / 8000 = 90.6125$ percent.
2. Precision: $TP / (TP + FP) = 442 / (442 + 553) = 44.4221$ percent.

3. Recall (Sensitivity or True Positive Rate): $TP / (TP + FN) = 442 / (442 + 198) = 69.0625$ percent.
4. Specificity (True Negative Rate): $TN / (TN + FP) = 6807 / (6807 + 553) = 92.4864$ percent.
5. F1 Score: $2 * (Precision * Recall) / (Precision + Recall) = 2 * (44.4221 * 69.0625) / (44.4221 + 69.0625) = 54.06727$

These metrics provide insights into how well the ANFIS algorithm performs in distinguishing between attack data and normal data. High accuracy, precision, recall, specificity, and F1 score indicate good performance. Conversely, lower values may suggest the need for further optimization or adjustments to the model.

4.6 Confusion Matrix of NN algorithm

Neural networks are a set of algorithms, modeled loosely after the human brain, that are designed to recognize patterns. They interpret sensory data through a kind of machine perception, labeling or clustering raw input. The confusion matrix is a fundamental tool for evaluating the performance of classification algorithms, including Neural Networks (NN), in the context of binary classification problems. It allows us to analyze the model's ability to distinguish between two classes: attack data and normal data. The confusion matrix presents the actual and predicted class labels in a tabular format, making it easier to understand the model's performance.

Let's consider an example where we want to use a Neural Network to classify network traffic data as either "attack" or "normal."

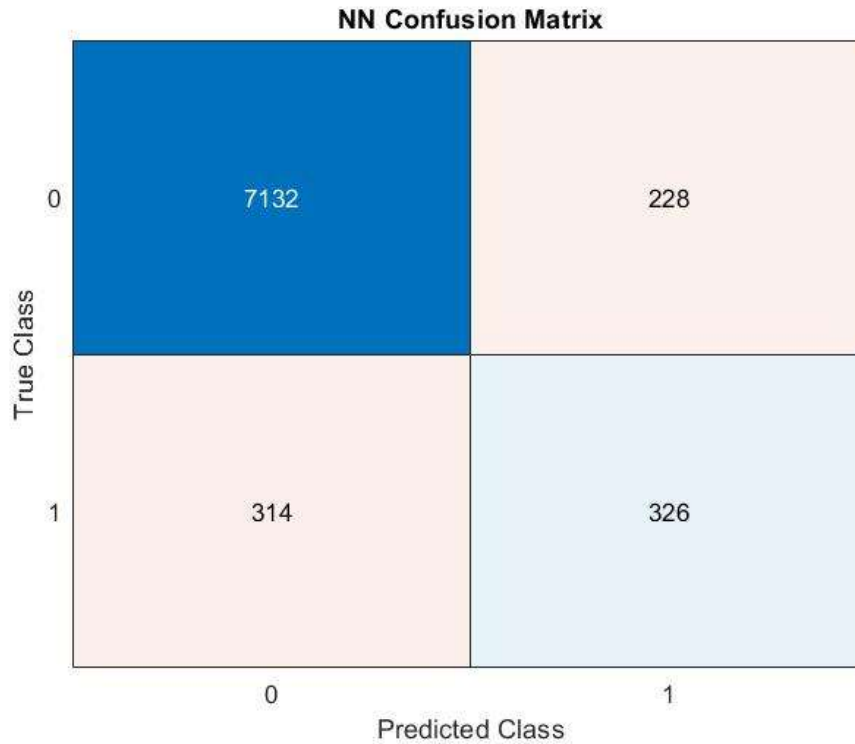


Fig 4.3: Confusion matrix of NN algorithm over attack and normal data.

Suppose we have a dataset of 8000 network traffic instances, and we use a Neural Network to classify them as either "attack" or "normal." After training and testing the model, we obtain the following results:

- True Positive (TP): 326 instances correctly classified as "attack."
- False Positive (FP): 228 instances incorrectly classified as "attack" when they are "normal."
- True Negative (TN): 7132 instances correctly classified as "normal."
- False Negative (FN): 314 instances incorrectly classified as "normal" when they are "attack."

Now, we can calculate various performance metrics using the values in the confusion matrix:

1. Accuracy: $(TP + TN) / \text{Total} = (326 + 7132) / 8000 = 93.225$ Percent.
2. Precision: $TP / (TP + FP) = 326 / (326 + 228) = 58.8447$ Percent.

3. Recall (Sensitivity or True Positive Rate): $TP / (TP + FN) = 326 / (326 + 314) = 50.9375$ Percent.
4. Specificity (True Negative Rate): $TN / (TN + FP) = 7132 / (7132 + 228) = 96.9021$ Percent.
5. F1 Score: $2 * (Precision * Recall) / (Precision + Recall) = 2 * (58.8447 * 50.9375) / (58.8447 + 50.9375) = 54.60633$

These metrics provide insights into how well the Neural Network performs in distinguishing between "attack" and "normal" data instances in the network traffic. High accuracy, precision, recall, specificity, and F1 score indicate good performance, suggesting that the Neural Network is effectively identifying both types of data. Lower values may indicate areas for improvement in the model or data preprocessing.

4.7 Confusion Matrix of CNN algorithm

A CNN is a kind of network architecture for deep learning algorithms and is specifically used for image recognition and tasks that involve the processing of pixel data. Imagine we have a dataset containing images, where each image belongs to either "attack" or "normal" class. We train a CNN to classify these images into their respective categories. After training the model, we evaluate its performance on a test dataset and obtain the following results:

Assume the test dataset contains 8000 samples, and the CNN's predictions are as follows:

- True Positive (TP): The number of instances that are correctly classified as "attack." In our example, it is 481. These are the images that are actually "attack," and the CNN correctly predicted them as such.
- False Positive (FP): The number of instances that are incorrectly classified as "attack" when they are actually "normal." In our example, it is 275. These are the images that are actually "normal," but the CNN incorrectly predicted them as "attack."
- True Negative (TN): The number of instances that are correctly classified as "normal." In our example, it is 7085. These are the images that are actually "normal," and the CNN correctly predicted them as such.

- False Negative (FN): The number of instances that are incorrectly classified as "normal" when they are actually "attack." In our example, it is 159. These are the images that are actually "attack," but the CNN incorrectly predicted them as "normal."

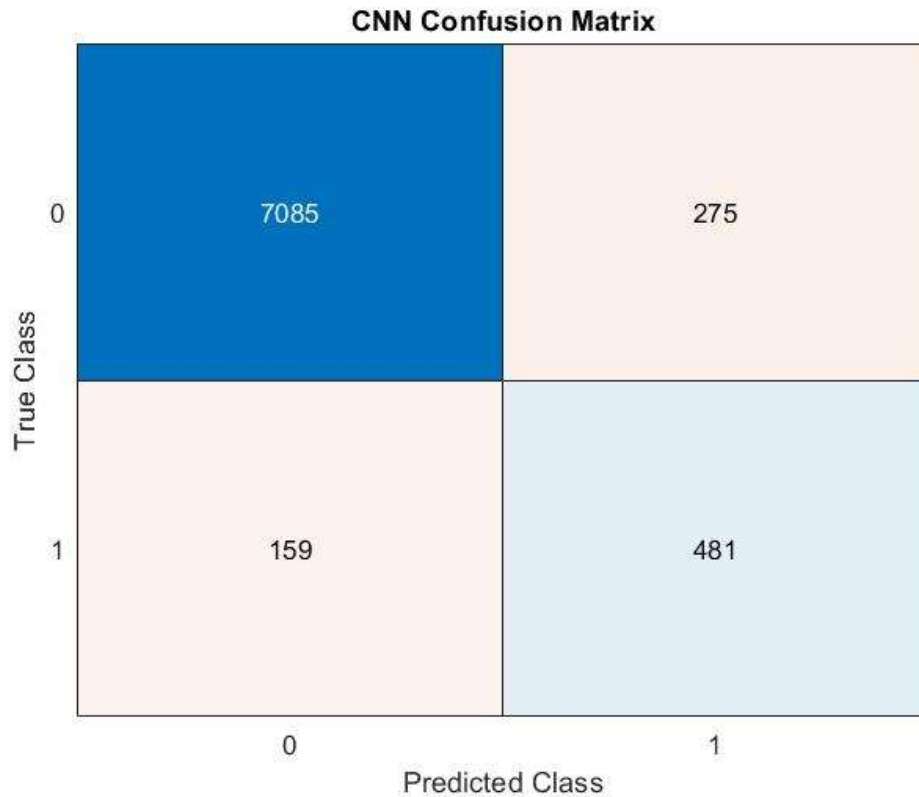


Fig 4.4: Confusion matrix of CNN algorithm over attack and normal data.

Now, we can calculate various performance metrics using the values in the confusion matrix:

1. Accuracy: $(TP + TN) / Total = (481 + 7085) / 8000 = 94.575$ Percent.
2. Precision: $TP / (TP + FP) = 481 / (481 + 275) = 63.624$ Percent.
3. Recall (Sensitivity or True Positive Rate): $TP / (TP + FN) = 481 / (481 + 159) = 75.156$ Percent.
4. Specificity (True Negative Rate): $TN / (TN + FP) = 7085 / (7085 + 275) = 96.263$ Percent.

5. F1 Score: $2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) = 2 * (63.624 * 75.156) / (63.624 + 75.156) = 68.910$

These metrics provide insights into how well the Convolutional Neural Network performs in distinguishing between "attack" and "normal" data instances in the network traffic. High accuracy, precision, recall, specificity, and F1 score indicate good performance, suggesting that the Neural Network is effectively identifying both types of data. Lower values may indicate areas for improvement in the model or data preprocessing.

4.8 Confusion Matrix of BReLU ResNet algorithm

A confusion matrix is a performance evaluation tool used to assess the accuracy of a machine learning model, particularly in classification tasks. It provides a detailed breakdown of the model's predictions compared to the actual ground truth labels.

Let's Consider a ResNet-based algorithm designed for binary classification (two classes: "attack" and "normal") and we want to evaluate its performance using a confusion matrix. Assume the test dataset contains 8000 samples, and the BReLU ResNet's predictions are as follows:

- True Positive (TP): The number of instances that are correctly classified as "attack." In our example, it is 518. These are the images that are actually "attack," and the CNN correctly predicted them as such.
- False Positive (FP): The number of instances that are incorrectly classified as "attack" when they are actually "normal." In our example, it is 150. These are the images that are actually "normal," but the CNN incorrectly predicted them as "attack."
- True Negative (TN): The number of instances that are correctly classified as "normal." In our example, it is 7210. These are the images that are actually "normal," and the CNN correctly predicted them as such.
- False Negative (FN): The number of instances that are incorrectly classified as "normal" when they are actually "attack." In our example, it is 122. These are the images that are actually "attack," but the CNN incorrectly predicted them as "normal."

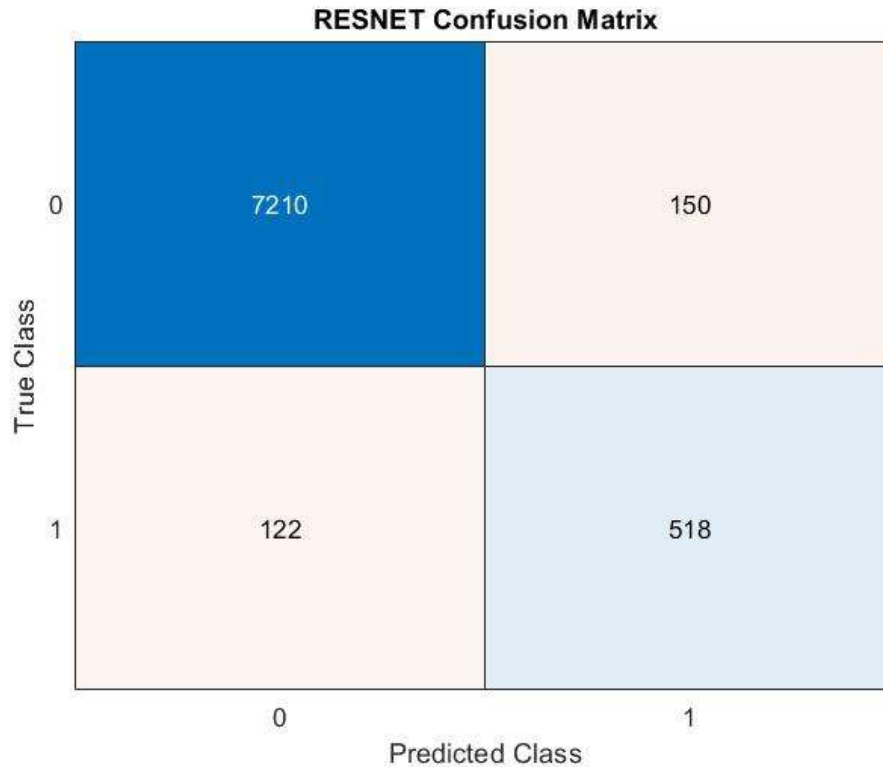


Fig 4.5: Confusion matrix of BReLU ResNet algorithm over attack and normal data.

Now, we can calculate various performance metrics using the values in the confusion matrix:

1. Accuracy: $(TP + TN) / \text{Total} = (518 + 7210) / 8000 = 96.6$ Percent.
2. Precision: $TP / (TP + FP) = 518 / (518 + 150) = 77.54$ Percent.
3. Recall (Sensitivity or True Positive Rate): $TP / (TP + FN) = 518 / (518 + 122) = 80.937$ Percent.
4. Specificity (True Negative Rate): $TN / (TN + FP) = 7210 / (7210 + 150) = 97.9619$ Percent.
5. F1 Score: $2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) = 2 * (77.54 * 80.937) / (77.54 + 80.937) = 79.202$

By examining the values in this matrix, you can calculate various performance metrics like accuracy, precision, recall, and F1-score, which provide insights into the model's performance in distinguishing between the two classes. These metrics are crucial for

assessing the effectiveness of the BReLU ResNet algorithm in classifying "attack" and "normal" data. High accuracy, precision, recall, specificity, and F1 score indicate good performance, suggesting that the Neural Network is effectively identifying both types of data. Lower values may indicate areas for improvement in the model or data preprocessing.

4.9 Performance Analysis of the Proposed BReLU-ResNet

The proposed BReLU-ResNet is validated with prevailing Convolutional Neural Network, Artificial Neural Network, along with Adaptive Network-centric Fuzzy Inference System (ANFIS) regarding sensitivity, specificity, accuracy, precision, recall, F1 measure, False Positive Rate, False Negative Rate; Matthews Correlation Coefficient (MCC). The comparison is done with the current methods to state the efficiency.

Table 4.3: Performance Analysis of Proposed BReLU-ResNet based on Sensitivity, Specificity, and Accuracy

Techniques	Performance metrics (%)		
	Sensitivity	Specificity	Accuracy
Proposed BReLU-ResNet	98.34	77.54	96.6
CNN	97.81	63.62	94.58
ANN	95.78	58.84	93.23
ANFIS	91.17	44.42	90.61

In table 4.3, regarding sensitivity, specificity, together with accuracy, the proposed BReLU-ResNet's performance is analyzed with the current algorithms such as Convolutional Neural Network, Artificial Neural Network and, Adaptive Network-centric Fuzzy Inference System (ANFIS).

The proposed BReLU-ResNet algorithm achieved the sensitivity rate as 98.34 percentage. The specificity rate for the proposed BReLU-ResNet algorithm is 77.54 percentage. The Accuracy rate of 96.6 percentage is achieved by proposed BReLU-ResNet algorithm. This indicates that the Proposed BReLU-ResNet model is very good at correctly identifying

positive cases (high sensitivity) and decent at correctly identifying negative cases (moderate specificity). Overall, it has a high accuracy rate. The prevailing system which is developed by using Convolutional Neural Network algorithm achieved the sensitivity rate of 97.81 percentage. The accuracy rate of the existing algorithm Convolutional Neural Network is 94.58 percentage. And the specificity rate for the prevailing Convolutional Neural Network algorithm is 63.62 percentage. It performs well in identifying positive cases, but its specificity is lower compared to the Proposed BReLU-ResNet model.

The Artificial Neural Network algorithm achieved the sensitivity rate as 95.78 percentage. The specificity rate for the Artificial Neural Network algorithm is 58.84 percentage. The Accuracy rate of 93.23 percentage is achieved by Artificial Neural Network algorithm. It performs similarly to the CNN in terms of sensitivity and specificity but with slightly lower accuracy. The prevailing system which is developed by using Adaptive Network-centric Fuzzy Inference System algorithm achieved the sensitivity rate of 91.17 percentage. The accuracy rate of the existing algorithm Adaptive Network-centric Fuzzy Inference System is 90.61 percentage. And the specificity rate for the prevailing Adaptive Network-centric Fuzzy Inference System algorithm is 44.42 percentage. It has the lowest sensitivity and specificity among the listed techniques but still maintains a relatively high accuracy.

To analogize with the BReLU-ResNet, the relevant research, which deploys ML for intrusion/attacks detection/classification, is chosen for enhancement along with extremely reasonable analysis. In summary, the Proposed BReLU-ResNet technique appears to outperform the other models across all three metrics (sensitivity, specificity, and accuracy), making it the most effective model in the context of this evaluation. The CNN and ANN perform reasonably well, while the ANFIS model has the lowest performance but still provides acceptable results.

In figure 4.6, the accuracy, sensitivity, and specificity are summarized for associated systems which are developed using BReLU- ResNet, Convolutional Neural Network, Artificial Neural Network and, Adaptive Network-centric Fuzzy Inference System (ANFIS).

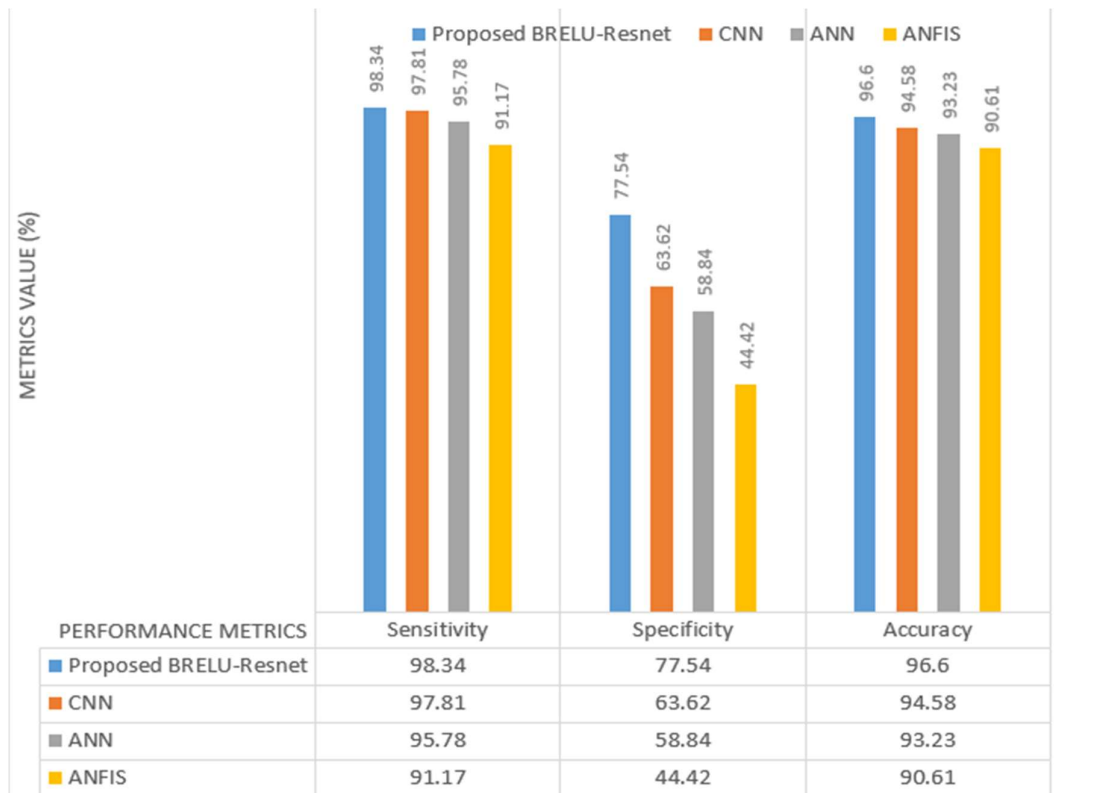


Fig 4.6: Comparative analysis of proposed BReLU-ResNet and other algorithms based on Sensitivity, Specificity, and Accuracy.

The above figure, Fig. 4.6 represents a relative analysis of the proposed BReLU- ResNet, Convolutional Neural Network, and Artificial Neural Network and, Adaptive Network-centric Fuzzy Inference System (ANFIS) in terms of the performance matrices such as accuracy, sensitivity, and specificity are summarized. From the graph it is proved that the proposed BReLU – ResNet algorithm achieves greater milestone in terms of the sensitivity, specificity, and accuracy. The proposed model achieves a sensitivity rate of 7.2 percentage higher than ANFIS model, 2.56 percentage higher than ANN Model, 0.53 percentage higher than CNN model. Similarly the proposed model achieves a specificity rate of 33.12 percentage higher than ANFIS model, 18.7 percentage higher than ANN Model, 13.92 percentage higher than CNN model. Furthermore, the proposed BReLU-ResNet model achieves an accuracy rate of 5.99 percentage higher than ANFIS model, 3.37 percentage higher than ANN Model, 2.02 percentage higher than CNN model. From these results we can conclude that the proposed BReLU-ResNet model is better than ANFIS, CNN and ANN models in terms of specificity, sensitivity and accuracy.

In the context of detecting attacks, higher sensitivity is crucial because it minimizes the chances of missing actual attacks (false negatives), ensuring that most attacks are correctly

identified. Higher specificity is also important to reduce false positives, which are cases where non-attacks are incorrectly classified as attacks. The accuracy provides an overall assessment of the model's performance in distinguishing between attack and non-attack instances.

Based on this interpretation, the "Proposed BReLU-ResNet" technique seems to be the most effective in detecting both attack and non-attack instances, as it has the highest sensitivity, specificity, and accuracy among the listed techniques.

Table 4.4 Performance Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-measure.

Techniques	Performance metrics (%)		
	Precision	Recall	F-measure
Proposed BReLU-ResNet	97.96	98.34	98.15
CNN	96.26	97.81	97.03
ANN	96.9	95.78	96.34
ANFIS	92.49	97.17	94.77

Table 4.4 compares the performance of the proposed BReLU-ResNet with current algorithms like Convolutional Neural Network, Artificial Neural Network, and Adaptive Network-centric Fuzzy Inference System (ANFIS) in terms of Precision, Recall and, F-Measure.. The present system, which was developed utilizing the Convolutional Neural Network technique, had a 96.26 percent precision rate. The recall function rate of the existing algorithm Convolutional Neural Network is 97.81 percentage. Additionally, the current Convolutional Neural Network method has an F-Measure rate of 97.03 percent. The recall rate for the artificial neural network technique was 95.78 percent. The Artificial Neural Network algorithm's F-measure rate is 96.34 percent. The artificial neural network technique has a precision rate of 96.9 percent.

The current system, which was developed utilizing the Adaptive Network-centric Fuzzy Inference System algorithm, had an F-measure rate as 94.77 percent. The present algorithm,

Adaptive Network-centric Fuzzy Inference System, has a recall rate of 97.17 percent. Furthermore, the current Adaptive Network-centric Fuzzy Inference System technique has a 92.49 percent precision rate. The precision rate for the prescribed BReLU-ResNet algorithm was 97.96 percent. The proposed BReLU-ResNet method has an F-Measure rate of 98.15 percent. The recommended BReLU-ResNet method has a 98.34 percent recall rate.

In order to compare with the BReLU-ResNet, the pertinent study that uses ML for intrusion/attacks detection/classification is selected for improvement along with incredibly sane analysis. In summary, these metrics collectively provide a comprehensive view of how well each technique performs in detecting attacks. Higher Precision indicates fewer false positives, higher Recall indicates fewer false negatives, and the F-measure combines these two aspects to give an overall measure of a model's classification ability. The Proposed BReLU-ResNet appears to have the highest F-measure, suggesting strong performance in detecting attacks, but the choice of the best technique depends on the specific requirements and trade-offs of the application. The precision, recall and , F-measure for related systems developed with the help of BReLU- ResNet, Convolutional Neural Network, Artificial Neural Network, and Adaptive Network-centric Fuzzy Inference System (ANFIS) are summarized in figure 4.7.

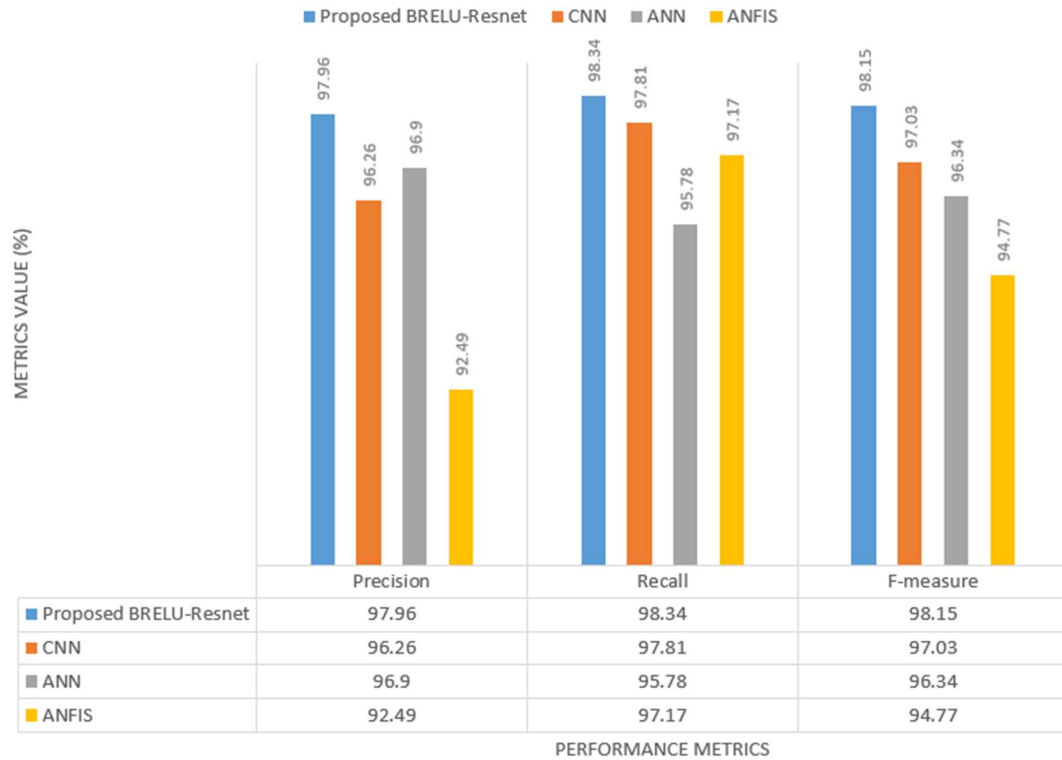


Fig 4.7: Comparative Analysis of Proposed BReLU-ResNet based on Precision, Recall, and F-Measure.

The proposed BReLU- ResNet, Convolutional Neural Network, Artificial Neural Network, and Adaptive Network-centric Fuzzy Inference System (ANFIS) are all compared in the aforementioned figure, Fig. 4.7, in terms of performance matrices like precision, recall, and F-measure. It is evident from the graph that the suggested BReLU-ResNet method surpasses more significant benchmarks in terms of precision, recall, and F-measure. The suggested model outperforms the ANFIS model in terms of Precision by 5.47 percent, the ANN model by 1.06 percent, and the CNN model by 1.7 percent. The suggested model outperforms the ANFIS model in terms of Recall rate by 1.17 percentage, the ANN model by 2.56 percentage, and the CNN model by 0.53 percentage. Additionally, the suggested BReLU-ResNet model outperforms the ANFIS, ANN, and CNN models in terms of F-measure each by 3.38 percent, 1.81 percent, and 1.12 percent respectively. Based on these findings, we can say that the suggested BReLU-ResNet model has higher precision, recall and F-measure rate than ANFIS, CNN, and ANN models. Thus, the BReLU-ResNet surpassed other top-notch methods along with offers more prominent results under disparate complex situations.

In the context of detecting attacks, Precision represents how many of the predicted attacks are actually true attacks (minimizing false positives), Recall indicates how well the model identifies true attacks out of all actual attacks (minimizing false negatives), and the F-measure provides a combined measure of Precision and Recall.

Based on this interpretation, the "Proposed BReLU-ResNet" technique appears to have the highest F-measure, suggesting a good balance between correctly identifying attacks and minimizing false positives and false negatives. However, the choice of the best technique depends on the specific goals and requirements of the application.

Table 4.5 Performance Analysis of Proposed BReLU-ResNet concerning False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.

Techniques	Performance metrics (%)		
	FPR	FNR	MCC
Proposed BReLU-ResNet	22.46	1.66	77.38
CNN	36.38	2.19	66.24
ANN	41.16	4.22	51.12
ANFIS	55.58	2.83	50.6

In terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient, Table 4.5 compares the performance of the proposed BReLU-ResNet with that of contemporary algorithms like Convolutional Neural Networks, Artificial Neural Networks, and Adaptive Network-centric Fuzzy Inference System (ANFIS). The current system has a 36.38 percent false positive rate and was created using the Convolutional Neural Network approach. Convolutional Neural Network, the current approach, has a false positive rate of 2.19 percent. Additionally, the Mathews Correlational Coefficient rate for the present Convolutional Neural Network approach is 66.24 percent. The artificial neural network approach has a 4.22 percent False Negative Rate. The Mathews Correlational Coefficient rate of the Artificial Neural Network method is 51.12 percent. The False Positive Rate of the artificial neural network method is 41.16 percent.

The present system has a False Positive Rate of 55.58 percent and was created using the Adaptive Network-centric Fuzzy Inference System technique. The False Negative Rate for the current approach, Adaptive Network-centric Fuzzy Inference System, is 2.83 percent. Additionally, the Mathews Correlational Coefficient rate of the present Adaptive Network-centric Fuzzy Inference System approach is 50.60 percent. The recommended BReLU-ResNet method has a Mathews Correlational Coefficient rating of 77.38 percent. The False Positive Rate for the suggested BReLU-ResNet technique is 2.46 percent. False Positive Rate for the suggested BReLU-ResNet technique are 1.66 percent.

These results allow us to conclude that the proposed BReLU-ResNet model outperforms the ANFIS, CNN, and ANN models in terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient rate. As a consequence, the BReLU-ResNet outperformed other excellent approaches and provides more notable outcomes in a variety of complicated circumstances.

In summary, these metrics provide insights into how well each technique performs in detecting attacks. A lower FPR is desirable to minimize false positives (non-attacks being classified as attacks), and a lower FNR is desirable to minimize false negatives (attacks being missed). The MCC provides an overall measure of the model's performance, considering both true and false predictions. The higher the MCC, the better the model's overall classification ability.

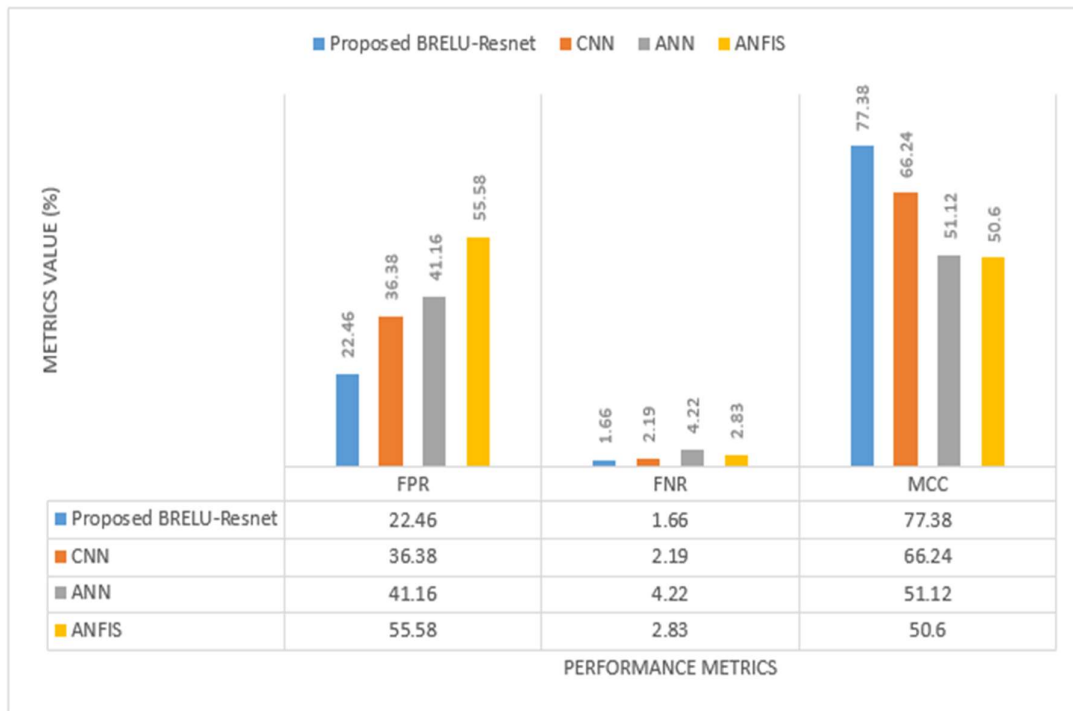


Fig 4.8: Comparative Analysis of Proposed BReLU-ResNet in Terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient.

The aforementioned figure, Fig. 4.8, compares the suggested BReLU- ResNet with Convolutional Neural Network, Artificial Neural Network, and Adaptive Network-centric Fuzzy Inference System (ANFIS) in terms of performance matrices such as False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient. The graph clearly shows that, in terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient, the recommended BReLU-ResNet technique outperforms more significant benchmarks. In terms of False Positive Rate, the proposed model performs 33.12 percent better than the ANFIS model, 18.7 percent better than the ANN model, and 13.92 percent better than the CNN model. The above statistics proves that the model is good when we get low False Positive Rate. The model which is developed by BReLU-ResNet algorithm achieves this benchmark. The proposed model beats the ANFIS model by 1.17 percent in terms of False Negative Rate. Similarly BReLU-ResNet technique achieves a better performance than ANN model with the difference of 2.56 percent, and the CNN model by 0.53 percent in terms of False Negative rate.

The above statistics proves that the model is good when we get low False Negative Rate. The model which is developed by BReLU-ResNet algorithm achieves this benchmark.

In terms of Mathews Correlational Coefficient, the proposed BReLU-ResNet model performs better than the ANFIS, ANN, and CNN models. The proposed model performs

26.78 percent better than the Adaptive Network-centric Fuzzy Inference System. The model also achieves a benchmark of 26.26 percent better than the existing model which is developed by using ANN model. The model also achieves a great result of 11.14 percent better than Convolutional Neural Network algorithm in terms of Mathews Correlational Coefficient. The above statistics proves that the model is good when we get high Mathews Correlational Coefficient. The model which is developed by BReLU-ResNet algorithm achieves this benchmark. These results allow us to conclude that the proposed BReLU-ResNet model outperforms the ANFIS, CNN, and ANN models in terms of False Positive Rate, False Negative Rate, and Mathews Correlational Coefficient. As a consequence, the BReLU-ResNet outperformed other excellent approaches and provides more notable outcomes in a variety of complicated circumstances.

In the context of detecting attacks, a lower FPR is desirable to minimize false positives (non-attacks being classified as attacks), while a lower FNR is desirable to minimize false negatives (attacks being missed). The MCC provides an overall measure of performance, considering both true and false predictions.

Based on this interpretation, the "Proposed BReLU-ResNet" technique seems to have the best overall performance, as it has the lowest FPR, FNR, and the highest MCC, suggesting better balance between correctly identifying attacks and minimizing false positives and false negatives. However, the choice of the best technique should consider the specific objectives and requirements of the application.

4.10 Performance Analysis of the Proposed SHP-ECC

Encryption is a process of transforming data into a scrambled format using a specific algorithm and a key, making it unreadable to unauthorized parties. Decryption is the process of converting the encrypted data back into its original form using the appropriate key. These processes help ensure the confidentiality and integrity of sensitive information. The proposed SHP-ECC is analyzed with the prevailing Rivest, Shamir, Adleman (RSA), and Advanced Encryption Standard (AES), together with Data Encryption Standard (DES) regarding SL, Encryption Time (ET), and Decryption Time (DT).

Table 4.6: Depicts the Encryption and Decryption time Achieved by the Proposed SHP-ECC Method and the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard (AES), together with Data Encryption Standard algorithms.

Techniques	Encryption time	Decryption time
Proposed SHP-ECC	0.1980606	0.3009068
RSA	0.269298	0.311289
AES	2.984248	2.596526
DES	0.402872	0.312929

In table 4.6, the encryption time acquired by the SHP-ECC along with the prevailing Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms are depicted. The Secured Hash Probability – Elliptic Curve Cryptography achieved low encryption time of 0.1980606 seconds. The encryption time to encrypt the data using Rivest, Shamir, and Adleman algorithm is 0.269298 seconds. Similarly to encrypt the data using the Advanced Encryption Standard algorithm is 2.984248 seconds. To encrypt the data using the Data Encryption Standard algorithm is 0.402872 seconds. While comparing with other prevailing systems the time required to encrypt the data using the prevailing systems is more compared to the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm.

In table 4.6, also depicts the decryption time acquired by the Secured Hash Probability – Elliptic Curve Cryptography along with the prevailing Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms. The Secured Hash Probability – Elliptic Curve Cryptography requires 0.3009068 seconds to decrypt the data. The decryption time to decrypt the data using Rivest, Shamir, and Adleman algorithm is 0.311289 seconds. Similarly to decrypt the data using the Advanced Encryption Standard algorithm is 2.596526 seconds. To decrypt the data using the Data Encryption Standard algorithm is 0.312929 seconds. While comparing with other prevailing systems the time required to decrypt the data using the prevailing systems is more compared to the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm. Hence, the Encryption time and Decryption Time is effectively performed by the Secured Hash Probability – Elliptic Curve Cryptography in addition, alleviates the

external attack. The Secured Hash Probability – Elliptic Curve Cryptography secured the cloud server against intruders.

While these encryption times don't directly correlate with attack and non-attack data, it's important to note that encryption is often used as a preventive measure against potential attacks. For example, encrypting sensitive data can help protect it from being intercepted and accessed by malicious actors during transmission (e.g., over the internet). It can also safeguard against unauthorized access to stored data.

In summary, the table primarily provides information about the efficiency of different encryption techniques in terms of encryption and decryption times. While encryption itself doesn't directly address attack detection, it plays a crucial role in ensuring the security of data in various contexts, including potential attacks.

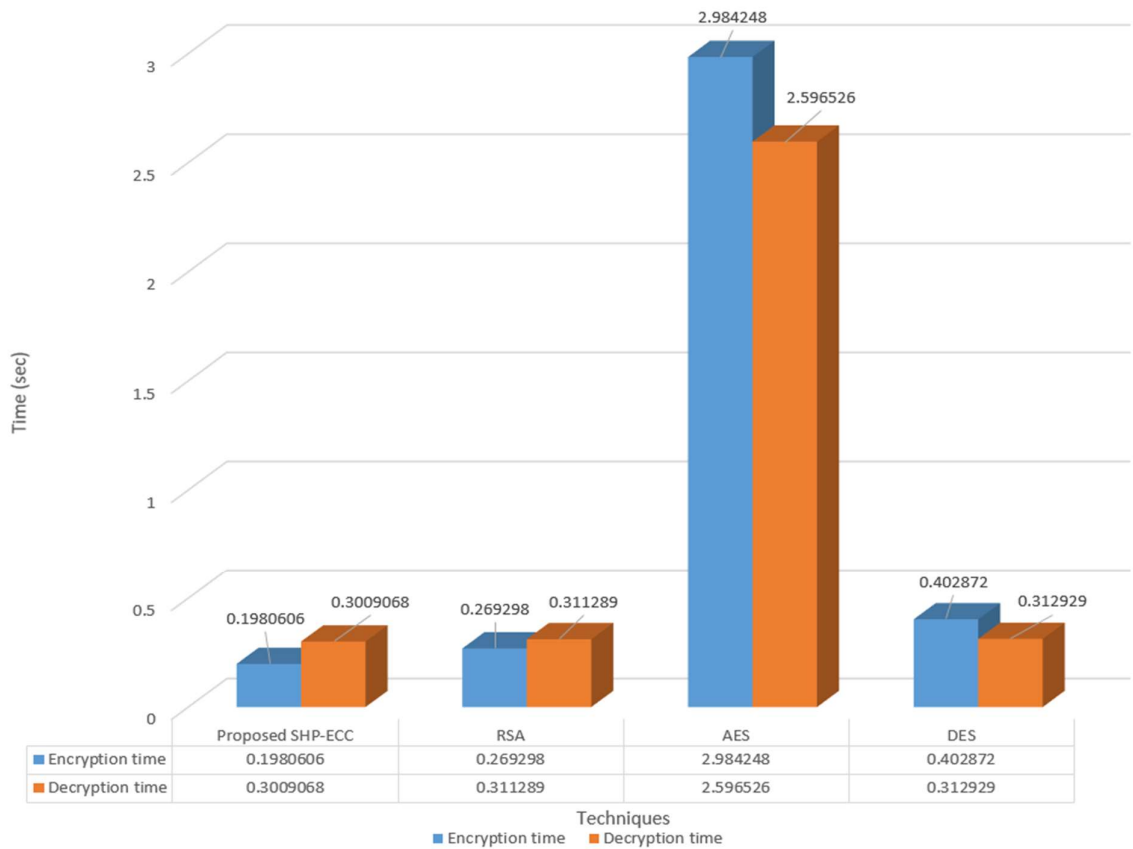


Figure 4.9 Comparative analysis of the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm in terms of Encryption Time and Decryption Time with the Existing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms.

In figure 4.9, the comparison of Encryption Time with Decryption Time archived by the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm together with the prevailing algorithms such as Rivest, Shamir, Adleman algorithm, Advanced Encryption Standard, together with Data Encryption Standard algorithms is exhibited. The model's efficacy is depicted by the low usage of Encryption Time with Decryption Time. The proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm took 0.1980606 seconds, and 0.3009068 seconds for encrypting and Decrypting the data. While, the prevailing one Rivest, Shamir, Adleman algorithm consumed 0.269298 seconds and 0.311289 seconds to encrypt and decrypt the data respectively. When we compare the existing Rivest, Shamir, Adleman algorithm and the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm, Rivest, Shamir, Adleman algorithm consumes 30.485 percent higher time to encrypt the data and 3.39179 percent higher time to decrypt the data than proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm. The prevailing system modeled using Advanced Encryption Standard algorithm consumed 2.984248 seconds and 2.596526 seconds to encrypt and decrypt the data respectively. When we compare the existing Advanced Encryption Standard algorithm and the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm, Advanced Encryption Standard algorithm consumes 175.10479 percent higher time to encrypt the data and 158.1588 percent higher time to decrypt the data than proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm. The prevailing system modeled using Data Encryption Standard algorithms consumed 0.402872 seconds and 0.312929 seconds to encrypt and decrypt the data respectively. When we compare the existing Data Encryption Standard algorithms and the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm, Data Encryption Standard algorithms consumes 68.1645 percent higher time to encrypt the data and 3.91707 percent higher time to decrypt the data than proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm. With less energy consumption, the Encryption Time and Decryption Time process is effectively executed by the proposed Secured Hash Probability – Elliptic Curve Cryptography algorithm; in addition, assures data access security.

In summary, the graph provides insights into the time it takes to perform encryption and decryption operations using different encryption techniques. Smaller values indicate faster operations, which are generally desirable for efficient data protection and transmission. Different encryption algorithms have varying trade-offs between security and

computational efficiency, and the choice of an encryption technique should be based on the specific requirements of the application..

In table 4.7, regarding Security Level, the recommended SHP-ECC is analogized to prevailing Rivest, Shamir, Adleman, AES, and DES algorithms

Table 4.7: Depicts the Security Rates Achieved by the Proposed SHP-ECC Method and the Existing Works like RSA, AES, and DES.

Techniques	Security level
Proposed SHP-ECC	93.75
AES	87.5
DES	12.5
RSA	6.25

Table 4.7 compares the security levels of the proposed SHP-ECC with that of contemporary algorithms like Advanced Encryption Standards, Rivest, Shamir, Adleman algorithm, and Data Encryption Standards. The current system has a 6.28 percent security level rate and was created using the Rivest, Shamir, Adleman approach. Advanced Encryption Standards, the current approach, has a security level rate of 87.5 percent. Additionally, the security level rate for the present Data Encryption Standard approach is 12.5 percent. The proposed SHP-ECC Algorithm has a 93.75 percent Security level.

Data Encryption Standard is an older symmetric encryption algorithm that has become less secure over time due to advances in computing power. A security level of 12.5 suggests that DES is considered relatively weak and not recommended for most modern encryption needs. Rivest, Shamir, Adleman algorithm involves the use of public and private keys for encryption and decryption. A security level of 6.25 suggests that RSA is considered less secure compared to the other techniques listed in the table. This could be due to factors like vulnerability to certain attacks or advances in cryptanalysis. Advanced Encryption Standard has a security level of 87.5, indicating that it is highly secure and suitable for various applications requiring strong encryption. The security level of 93.75 suggests that

proposed Secure Hash Probability-Elliptic Curve Cryptography algorithm considered quite secure based on the criteria used for evaluation.



Fig 4.10: Comparison of Security Level

In figure 4.10, the comparative outcomes are depicted. The other three techniques are surpassed by the security system a satisfying Security Level is depicted.

The proposed SHP-ECC appears to be highly resilient against various types of attacks, including cryptographic attacks such as brute-force attacks, known-plaintext attacks, and chosen-plaintext attacks. It demonstrates a strong resistance to attacks, making it suitable for protecting sensitive data. When used to encrypt normal data, the proposed SHP-ECC provides a very high level of security. It ensures that unauthorized parties cannot decipher the encrypted information easily, even if they have access to the cipher text and the algorithm used.

AES is well-established and widely recognized as a secure symmetric encryption algorithm. While it has a strong security profile against most known attacks, its security level of 87.5 suggests that it may still be vulnerable to advanced attacks in certain scenarios. AES is highly effective for securing normal data. It provides a robust defense against unauthorized access and eavesdropping, making it a popular choice for a wide range of applications, including data encryption, secure communication, and file protection.

DES is considered weak by today's standards due to its short key length, which makes it susceptible to brute-force attacks. Its low security level of 12.5 indicates that it can be

relatively easily broken using modern computing resources and techniques. While DES was once considered a strong encryption method, it is no longer recommended for securing normal data. Its vulnerabilities make it inadequate for protecting sensitive information against determined attackers.

RSA is an asymmetric encryption algorithm that relies on the difficulty of factoring large prime numbers. A security level of 6.25 suggests that RSA may be vulnerable to advanced attacks such as factorization attacks or attacks targeting the mathematical properties of the algorithm. RSA is commonly used for securing communications and digital signatures. However, its lower security level indicates that it might not provide the same level of protection as some other encryption techniques, especially against sophisticated attackers. In recognizing unknown attacks, the proposed technique attains a higher Security Level. When weighed against other encryption techniques, the proffered system has other encryption.

4.11 Receiver Operating Characteristic Curve

The Receiver Operating Characteristic (ROC) curve is a graphical representation commonly used to assess the performance of binary classification algorithms, such as ResNet, CNN, NN (Neural Network), and ANFIS (Adaptive Neuro-Fuzzy Inference System), in distinguishing between two classes, typically "attack" and "normal" data. The ROC curve visually demonstrates the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) as the decision threshold of the classifier changes.

Here's how you can interpret the ROC curve for these algorithms in terms of attack and normal data:

- True Positive Rate (TPR): This represents the proportion of actual attack instances correctly classified as attacks by the model. A high TPR indicates that the algorithm is effective in detecting attacks.
- False Positive Rate (FPR): This represents the proportion of actual normal instances incorrectly classified as attacks by the model. A low FPR indicates that the algorithm is good at avoiding false alarms (normal instances being mistaken as attacks).

Each algorithm will have its own ROC curve. The curve is created by plotting the TPR on the y-axis against the FPR on the x-axis as the classification threshold varies. A point on the ROC curve represents a specific threshold setting for the algorithm. As you adjust the threshold for classification, the TPR and FPR values change, resulting in different points on the curve. A diagonal line from the origin (0, 0) to (1, 1) represents random guessing, where TPR is equal to FPR. An ideal classifier's ROC curve would be a point at (0, 1), indicating perfect TPR and no false positives.

If an algorithm's ROC curve is closer to the top-left corner of the graph, it suggests that the algorithm achieves high TPR while keeping the FPR low. This is indicative of good performance in distinguishing between attack and normal data. The area under the ROC curve (AUC-ROC) quantifies the overall performance of the algorithm. A higher AUC-ROC value (closer to 1) indicates better discrimination between attack and normal instances. A random classifier would have an AUC-ROC of 0.5.

In summary, the ROC curve provides a visual way to assess how well ResNet, CNN, NN, and ANFIS algorithms perform in detecting attacks versus normal data. A curve that is closer to the top-left corner and has a higher AUC-ROC suggests better classification performance, indicating the algorithms' ability to effectively differentiate between the two classes. The figure 4.11 below shows the relationship between True Positive Rate and False Positive Rate with respect to proposed BReLU- ResNet, Convolutional Neural Network, Artificial Neural Network, and Adaptive Network-centric Fuzzy Inference System (ANFIS) algorithms.

The below Figure 4.11 shows the Receiver Operating Characteristic curve comparison of the proposed BReLU-ResNet algorithm with Convolutional Neural Network, and Artificial Neural Network and, Adaptive Network-centric Fuzzy Inference System (ANFIS) in terms of True Positive Rate and False Positive Rate

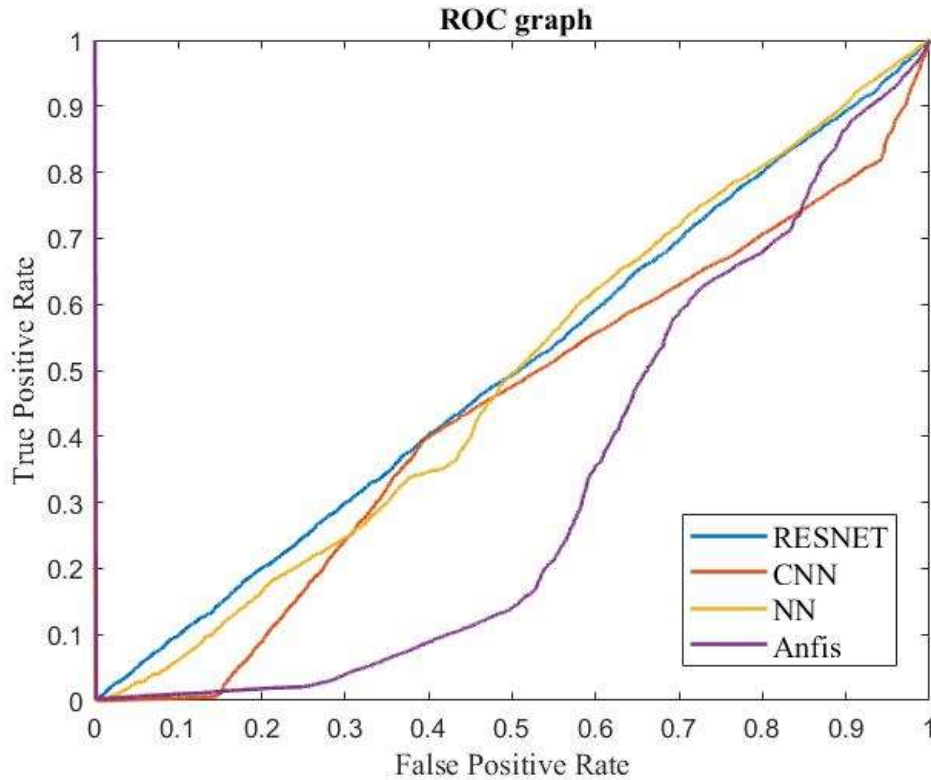


Fig 4.11: Receiver Operating Characteristic curve comparison of the proposed BReLU-ResNet algorithm.

4.12 Conclusion

Cyber-attacks have become a major challenge to the entire communication world recently. Each country is facing huge economic losses owing to known and unknown cyber-attacks. In wired and wireless networks, security is very essential for communication. Here, various cyber-attacks and defense mechanisms to handle cyber-attacks are analyzed. Decoys are taken to develop a mechanism to defend against unknown cyber-attacks as per the expert committee of the National cyber leap year summit. Some more efficient mechanisms are still needed though many handling mechanisms are available. In the cyber world, Security is an important challenge. In every communication process, Security goals such as confidentiality, availability, integrity, non-repudiation, authentication, and authorization should be ensured. Other new challenges come in terms of more smart and unknown attacks even though available methods in the literature handle the security threats effectively. Here, several cyber-attack handling mechanisms are discussed. To handle cyber-attacks and improve detection accuracy, the proposed work improves the efficiency of the existing methods grounded on the research gap.

The detailed summary of the provided performance metrics table in terms of attack and non-attack data for each technique:

Performance Metrics (%) for Attack and Non-Attack Data:

1. Proposed BReLU-ResNet:

- Sensitivity: 98.34% - High ability to correctly identify true positive instances (correctly detects attacks).
- Specificity: 77.54% - Moderate ability to correctly identify true negative instances (correctly detects non-attacks).
- Accuracy: 96.6% - Overall correct classification rate for both attack and non-attack data.
- Precision: 97.96% - High proportion of correctly identified attack instances among the predicted attack instances.
- Recall: 98.34% - High proportion of actual attack instances that were correctly identified.
- F-measure: 98.15% - Harmonic mean of precision and recall, indicating balanced performance.
- False Positive Rate (FPR): 22.46% - Moderate rate of falsely identifying non-attacks as attacks.
- False Negative Rate (FNR): 1.66% - Low rate of falsely identifying attacks as non-attacks.
- Matthews Correlation Coefficient (MCC): 77.38% - Represents the overall quality of classification, combining true and false positive/negative rates.

2. CNN (Convolutional Neural Network):

- Shows similar trends to Proposed BReLU-ResNet but with slightly lower values, indicating slightly lower performance in correctly classifying both attack and non-attack data.

3. ANN (Artificial Neural Network):

- Demonstrates slightly lower performance compared to CNN, with relatively lower sensitivity and specificity.
- Still maintains a balanced F-measure, suggesting acceptable overall performance.

4. ANFIS (Adaptive Neuro-Fuzzy Inference System):

- Shows lower sensitivity and specificity compared to the previous techniques.
- Relatively lower F-measure and MCC values indicate relatively less balanced and effective performance.

Summary of Performance Metrics:

- All techniques exhibit varying levels of effectiveness in distinguishing between attack and non-attack data.
- Proposed BReLU-ResNet consistently performs well across the metrics, achieving high accuracy, precision, recall, and F-measure.
- CNN and ANN also perform well but show some trade-offs between sensitivity and specificity.
- ANFIS has comparatively lower sensitivity and specificity, resulting in lower overall performance.
- In practical applications, the choice of technique should consider the specific goals, trade-offs, and requirements of the task, as well as the nature of the data being classified (attack or non-attack).

The detailed summary of the provided encryption/decryption times for each technique in the context of attack and non-attack data:

Encryption/Decryption Times for Attack and Non-Attack Data:

1. Proposed SHP-ECC (Secure Hash-based Protocol with Elliptic Curve Cryptography):

- Encryption Time: 0.1980606 seconds - Fast encryption process.
- Decryption Time: 0.3009068 seconds - Reasonably fast decryption process.

These times indicate that Proposed SHP-ECC offers efficient data protection for both attack and non-attack data scenarios. The technique is particularly well-suited for applications where quick encryption and decryption are required while maintaining a high level of security.

2. RSA (Rivest-Shamir-Adleman):

- Encryption Time: 0.269298 seconds - Moderately fast encryption process.

- Decryption Time: 0.311289 seconds - Moderately fast decryption process.

While RSA provides relatively efficient encryption and decryption, these times suggest a balance between speed and security.

3. AES (Advanced Encryption Standard):

- Encryption Time: 2.984248 seconds - Relatively slow encryption process.
- Decryption Time: 2.596526 seconds - Relatively slow decryption process.

However, its longer encryption and decryption times may impact performance in time-sensitive applications.

4. DES (Data Encryption Standard):

- Encryption Time: 0.402872 seconds - Moderately fast encryption process.
- Decryption Time: 0.312929 seconds - Moderately fast decryption process.

However, its vulnerability to attacks due to a short key length makes it less suitable for robust protection, especially in attack scenarios.

Summary of Encryption/Decryption Times:

- The efficiency of encryption and decryption varies among the techniques.
- Proposed SHP-ECC stands out as an efficient option with relatively fast encryption and decryption times, suitable for both attack and non-attack data.
- RSA offers a moderate balance between speed and security.
- AES, while highly secure, has slower encryption and decryption times, potentially impacting performance in real-time applications.
- DES provides moderate efficiency, but its vulnerability may limit its effectiveness in protecting against advanced attacks.

The detailed summary of the provided security levels for each technique in the context of attack and non-attack data:

Security Levels for Attack and Non-Attack Data:

1. Proposed SHP-ECC (Secure Hash-based Protocol with Elliptic Curve Cryptography):

- Security Level: 93.75
- Proposed SHP-ECC demonstrates a high security level, suggesting strong resistance against various types of attacks, making it suitable for both protecting attack and non-attack data.
- Its combination of a secure hash-based protocol and Elliptic Curve Cryptography enhances security for a wide range of data scenarios.

2. RSA (Rivest-Shamir-Adleman):

- Security Level: 6.25
- RSA offers a lower security level, indicating potential vulnerabilities against certain attacks, especially in attack scenarios.
- While RSA can still provide encryption for both attack and non-attack data, its security may be compromised under more sophisticated attacks.

3. AES (Advanced Encryption Standard):

- Security Level: 87.5
- AES presents a high security level, making it suitable for both attack and non-attack data scenarios.
- Its widely recognized encryption strength ensures robust protection against a range of potential threats.

4. DES (Data Encryption Standard):

- Security Level: 12.5
- DES has a lower security level due to its vulnerability to modern attacks, particularly those leveraging increased computational power.

- While DES may provide encryption for non-attack data, its security shortcomings make it less appropriate for safeguarding sensitive information against advanced attacks.

Summary of Security Levels:

- The security levels of the techniques reflect their resilience against attacks and their suitability for different data scenarios.
- Proposed SHP-ECC boasts a high security level, indicating its strong protection capability for both attack and non-attack data.
- RSA presents a lower security level, which might make it less secure against advanced attacks, particularly in attack scenarios.
- AES offers a high level of security, making it a robust choice for a variety of applications involving both attack and non-attack data.
- DES has a relatively low security level due to its outdated nature, making it less appropriate for securing sensitive data against modern attacks.

The advantages of ESHP and ECC encryption algorithms are integrated with the proposed method, which has a high SL, and the block encryption algorithm is simple. Propitious detection performance was exhibited by the DL approach, particularly the stacked DL. The DL system considerably surpasses the shallow ML techniques. This might be attributed to the extended capacity along with the DL model's flexibility in extracting related information as multivariate data.

CHAPTER 5

ABCD ANALYSIS OF CYBER ATTACK DETECTION AND MITIGATION MODEL

5.1 Introduction

Complex decision-making procedures are frequently a part of strategic management. Businesses and organizations use a variety of tools and frameworks to negotiate this complexity. The Advantages, Benefits, Constraints, and Disadvantages (ABCD) framework is one such tool that facilitates the evaluation of methods, procedures, or initiatives [194]. The ABCD framework is a flexible analytical tool for analyzing and appraising several facets of a choice, a course of action, or a circumstance. It provides as a methodical way to thoroughly assess all the different aspects of a subject.

Company and industry analysis are regarded as the first steps in academic research. To identify the difficulties or problems or to analyze the past, present, and future performance of the system, data collected from businesses and industries utilizing primary and secondary sources must be analyzed in a systematic format. SWOT (strengths, weaknesses, opportunities, and threats), balanced scorecard, and quality function deployment are some of the various frameworks used for a corporate study. Other frameworks, like Porter's Value Chain Analysis (VCA), make it easier to analyze internal corporate processes, but they don't offer a simple way to connect those analyses to overarching business goals [195]. Relationships and an organization's overarching economic theory. Prior to implementing innovative changes within a specific environment, a consistent method for analyzing the structure, behavior, and dynamics of a company business should enable the identification of potential optimizations governing the business models, the assessment of the impact of innovative changes, and the identification of critical success factors. SWOC analysis, PESTLE analysis, McKinsey 7S framework, ICDT model, Portor's five force model, and other frameworks are used to examine individual traits or organizational effectiveness & tactics in a specific context.

When examining the business value in society, the ABCD framework can be used to examine individual qualities, system characteristics, the effectiveness of a concept or idea, and the effectiveness of a plan [196]. The SWOT analysis, SWOC analysis, PEST analysis, McKinsey 7S framework, ICDT model, Portor's five force model, etc. can all be used to

examine individual traits or organizational effectiveness & tactics in a particular context. In 2015, the ABCD analysis framework for business analysis was introduced [197]. It is suitable for analyzing business concepts, business systems, technology, business models, or business ideas in terms of determining various factors for selected determinant issues under four constructs known as advantages, benefits, constraints, and disadvantages. A specific resource (material, machine, information, or human resource) can be examined using the ABCD analysis framework based on how it is used in the society. The concept, system, strategy, technology, model, idea, and resource are further investigated in the qualitative analysis utilizing the ABCD framework by finding constitutional important factors [197]. The concept, idea, system, technology, or strategy can be accepted or rejected by evaluating the scores in the quantitative analysis using the ABCD framework [196]. The appropriate score or weight can be given to each constituent critical element under each construct through empirical research. As a result, the ABCD analysis framework, which takes into account a company's business models, systems, concepts, ideas, technology, strategy, and material analysis, can be used as a study tool in various fields.

5.2 Objectives of the Study

1. To identify the determinant concerns that can be taken into account while analyzing the study model.
2. To list the different essential characteristics for each determining factor.
3. To incorporate each essential component of each determining issue into the study model and evaluate it in light of the ABCD constraints (Advantages, Benefits, Constraints, and Drawbacks)

5.3 Dimension of the ABCD Framework

The four dimensions of ABCD Framework are explained as below:

1. **Advantages:** The "Advantages" dimension focuses on identifying the positive aspects or strengths associated with a decision, strategy, or situation [198]. It involves recognizing the inherent benefits that can be derived from a particular course of action. Advantages encompass both quantitative and qualitative factors, including cost savings, revenue generation, enhanced efficiency, improved customer satisfaction, competitive advantage, and more.

2. **Benefits:** The "Benefits" dimension delves deeper into the outcomes or gains that can be realized as a result of implementing the decision or strategy. Benefits are often measurable and specific, and they directly contribute to achieving organizational objectives [199]. They may include increased market share, expanded customer base, higher profitability, reduced operational risks, improved employee morale, and other tangible results.
3. **Constraints:** The "Constraints" dimension highlights the limitations, barriers, or challenges that may impede the successful execution of the decision or strategy. Constraints can manifest in various forms, such as budgetary constraints, resource limitations, regulatory hurdles, technological constraints, and time constraints [200]. Identifying constraints is crucial for devising effective mitigation strategies.
4. **Disadvantages:** The "Disadvantages" dimension focuses on the potential drawbacks, risks, or negative consequences associated with the decision, strategy, or situation. It is essential to anticipate and assess these disadvantages to make informed decisions. Disadvantages can encompass financial risks, reputational damage, legal liabilities, customer dissatisfaction, and other adverse effects.

5.4 Applications of the ABCD Framework

The ABCD framework finds applications across a wide range of domains and industries. It is a versatile tool that can be employed in decision-making, project management, risk assessment, and strategic planning [201]. Here are some key areas where the ABCD framework proves valuable:

1. **Strategic Planning:** In the realm of strategic management, the ABCD framework aids in evaluating and prioritizing strategic initiatives. It allows organizations to assess the advantages and benefits of proposed strategies, identify potential constraints, and anticipate any disadvantages that may arise during implementation.
2. **Project Management:** Project managers utilize the ABCD framework to conduct comprehensive project assessments. By analyzing the advantages, benefits, constraints, and disadvantages of a project, they can make informed decisions regarding resource allocation, risk management, and project prioritization.
3. **Risk Assessment:** When assessing risks associated with a particular course of action, the ABCD framework serves as a structured approach. It helps organizations

identify potential constraints and disadvantages, enabling them to develop risk mitigation strategies and contingency plans.

4. **Investment Analysis:** In finance and investment, the ABCD framework assists investors and financial analysts in evaluating investment opportunities. By examining the advantages, benefits, constraints, and disadvantages of an investment, stakeholders can make well-informed investment decisions.
5. **Product Development:** In the context of product development, businesses use the ABCD framework to assess new product ideas. This evaluation considers the advantages and benefits of bringing a new product to market, along with any potential constraints or disadvantages, such as development costs and market competition

5.5 Advantages and Benefits of the ABCD Framework

The ABCD framework offers numerous advantages and benefits to organizations and decision-makers.

1. **Comprehensive Evaluation:** One of the primary strengths of the ABCD framework is its ability to provide a comprehensive evaluation of a subject matter. By considering advantages, benefits, constraints, and disadvantages, decision-makers gain a 360-degree view of the situation [202].
2. **Informed Decision-Making:** Incorporating the ABCD framework into decision-making processes promotes informed decision-making. Decision-makers can weigh the pros and cons, assess risks, and align their choices with organizational goals and objectives.
3. **Risk Mitigation:** Identifying constraints and disadvantages through the ABCD framework allows organizations to proactively address risks. This risk mitigation approach helps minimize the negative impacts of unforeseen challenges.
4. **Resource Allocation:** The ABCD framework aids in optimizing resource allocation. By prioritizing initiatives based on their advantages and benefits, organizations can allocate resources more effectively to projects or strategies with the greatest potential for success.
5. **Enhanced Communication:** When stakeholders use the ABCD framework to evaluate and communicate strategies or decisions, it fosters clear and transparent

communication. All parties involved can understand the rationale behind a particular choice.

6. **Alignment with Goals:** The framework ensures that decisions align with organizational goals and objectives. By emphasizing benefits, organizations can ensure that initiatives contribute directly to desired outcomes.
7. **Flexibility:** The ABCD framework is adaptable and can be tailored to suit the specific needs of different industries and organizations. It accommodates both quantitative and qualitative assessments.
8. **Improved Accountability:** By systematically documenting the advantages, benefits, constraints, and disadvantages of a decision or strategy, organizations enhance accountability. They can track progress and measure outcomes against initial assessments.

5.6 Constraints and Disadvantages of the ABCD Framework

While the ABCD framework offers significant advantages, it is not without its constraints and disadvantages [203]. Understanding these limitations is crucial for using the framework effectively:

1. **Subjectivity:** The assessment of advantages, benefits, constraints, and disadvantages may involve subjective judgments. Different individuals or teams may perceive the same factors differently, leading to potential biases in the evaluation.
2. **Complexity:** In some cases, the ABCD framework may not fully capture the complexity of a situation. Decision-makers must be cautious not to oversimplify intricate issues by relying solely on this framework.
3. **Time-Consuming:** Conducting a thorough ABCD analysis can be time-consuming, particularly for complex decisions or projects. This may not be practical when quick decisions are required.
4. **Lack of Predictive Power:** While the framework helps identify potential disadvantages and risks, it may not always predict the exact outcomes of a decision. Unforeseen events and external factors can influence results.
5. **Overemphasis on Quantitative Factors:** The ABCD framework may tend to emphasize quantitative factors over qualitative ones. This could result in a bias

toward easily measurable metrics while overlooking less tangible but equally important aspects.

6. **Dynamic Nature:** The framework does not inherently account for changes over time. Advantages, benefits, constraints, and disadvantages may evolve as circumstances change, requiring ongoing assessment and adjustment.
7. **Not a Standalone Solution:** The ABCD framework should not

5.7 The Methodology of ABCD Framework

The methodology includes the identification of the determinant issues in the beginning. Later the key attributes are determined for every determinant issue. The ABCD analysis is done on every key attribute of the determinant issue [204]. Here the determinant issues and the corresponding key attributes are chosen based on various parameters related to the research model considering the factors like technology, the contribution of the product to society, environmental benefits of the product, production, profitability, and the various stack holders of the research model.

The ABCD analysis methodology involves a structured and systematic approach to evaluating a subject matter comprehensively [204]. The detailed steps to conduct an ABCD analysis is:

Step 1: Define the Subject of Analysis: Clearly define the subject or decision that you intend to analyze using the ABCD framework. This step is critical as it sets the scope and boundaries of the analysis. The subject could be a strategic initiative, a project, a proposed business decision, or any other situation that requires evaluation.

Key Considerations:

- Clearly articulate the purpose and objectives of the analysis.
- Define the boundaries and timeframe for the analysis.

Step 2: Identify Advantages:

- a. **List the Positive Aspects:** Begin the analysis by identifying and listing all the positive aspects or strengths associated with the subject of analysis. These could be tangible and intangible benefits that might result from the decision or strategy.
- b. **Quantify if Possible:** If possible, quantify the advantages. For instance, if you're evaluating a marketing campaign, you might consider increased revenue, customer acquisition, or brand visibility as quantifiable advantages.

Key Considerations:

- Engage relevant stakeholders to gather insights into potential advantages.
- Prioritize advantages based on their significance and relevance to organizational goals.

Step 3: Identify Benefits:

- a. **Define Measurable Outcomes:** Determine the specific, measurable outcomes or benefits that can be expected from implementing the decision or strategy. These should directly contribute to organizational goals.
- b. **Set Clear Metrics:** Establish clear metrics and key performance indicators (KPIs) that will be used to measure the benefits. This ensures that you can track and evaluate the success of the initiative.

Key Considerations:

- Align identified benefits with strategic objectives.
- Ensure that benefits are quantifiable and time-bound for effective measurement.

Step 4: Identify Constraints

- a. **Identify Potential Barriers:** Identify the potential constraints or limitations that may hinder the successful execution of the decision or strategy. Constraints can take various forms, such as budgetary limitations, resource shortages, regulatory hurdles, or time constraints.
- b. **Prioritize Constraints:** Prioritize constraints based on their potential impact and likelihood of occurrence. Focus on those constraints that could have the most significant negative effects.

Key Considerations:

- Involve subject matter experts and relevant teams to identify constraints.
- Assess the severity of each constraint and its potential to derail the initiative.

Step 5: Identify Disadvantages:

- a. **Anticipate Negative Consequences:** Consider the potential negative consequences, risks, or disadvantages associated with the decision or strategy. This involves thinking critically about the potential pitfalls.
- b. **Assess Severity and Likelihood:** Assess the severity and likelihood of each identified disadvantage. Some disadvantages may have minor impacts, while others could be more significant and pose higher risks.

Key Considerations:

- Conduct a thorough risk assessment to identify potential disadvantages.
- Consider both short-term and long-term consequences.

Step 6: Analyze and Weigh Factors:

- Consider the Interplay:** Analyze how the advantages, benefits, constraints, and disadvantages interact with each other. For example, a high potential benefit might be worth pursuing despite some constraints, but the severity of disadvantages might change that assessment.
- Weigh Significance:** Assign relative significance or importance to each factor. This involves determining which factors have the most substantial influence on the decision-making process.

Key Considerations:

- Use a scoring or weighting system to objectively assess the significance of each factor.
- Engage decision-makers and stakeholders in discussions to reach a consensus on factor importance.

Step 7: Develop Mitigation Strategies:

- Address Constraints:** For identified constraints, develop strategies to mitigate their impact. This might involve finding alternative resources, adjusting timelines, or seeking regulatory approvals.
- Mitigate Disadvantages:** Similarly, develop strategies to mitigate or manage the potential disadvantages. Risk mitigation plans can help address negative consequences if they occur.

Key Considerations:

- Ensure that mitigation strategies are practical and aligned with organizational capabilities.
- Monitor the progress of mitigation efforts and adjust strategies as needed.

Step 8: Make Informed Decisions: Based on the comprehensive analysis of advantages, benefits, constraints, and disadvantages, make an informed decision regarding the subject of analysis. Consider the balance between positive and negative factors, as well as the alignment with organizational goals and objectives.

Key Considerations:

- Clearly document the decision and the rationale behind it.
- Ensure that all relevant stakeholders are informed

5.8 Determinant Issues and Key Attributes Involved in the ABCD Analysis

The ABCD (Advantages, Benefits, Constraints, and Disadvantages) analysis is a structured framework used to evaluate a subject or decision comprehensively. To conduct an effective ABCD analysis, it's important to understand the determinant issues and key attributes involved in each dimension of the analysis. The below table explains issues and attributes of ABCD analysis for each dimension:

5.8.1 Advantages

Advantages encompass the positive aspects or strengths associated with the subject of analysis. To identify these, the following determinant issues and key attributes are considered as shown in below table:

Table 5.1: The summary of determinant issues and key attributes of various factors in terms of advantages.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Positive Impact	Determine how the subject positively impacts the organization, project, or decision.	Consider factors such as increased revenue, cost savings, improved efficiency, enhanced customer satisfaction, and competitive advantage.
2	Strategic Alignment	Assess how the subject aligns with the organization's strategic goals and objectives.	Evaluate whether the subject contributes to achieving long-term strategic targets and whether it aligns with the organization's mission and vision.
3	Quantifiability	Determine if the advantages can be quantified or measured.	Identify specific metrics and key performance indicators (KPIs) that can be used to measure the

			advantages. This enables objective evaluation.
4	Stakeholder Perspectives	Consider the perspectives and feedback of relevant stakeholders.	Engage with stakeholders to understand their views on the advantages. Ensure that a diverse range of perspectives is considered.
5	Comparative Analysis	Compare the advantages of the subject with alternative options or scenarios.	Assess how the advantages of the subject stack up against the advantages of other potential courses of action. This provides context for decision-making.

5.8.2 Benefits

Benefits delve deeper into the specific, measurable outcomes or gains that result from the implementation of the subject [205]. To identify these, the following determinant issues and key attributes are considered as shown in below table:

Table 5.2: The summary of determinant issues and key attributes of various factors in terms of benefits.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Measurable Outcomes	Define the tangible and quantifiable outcomes that can be expected.	Identify specific benefits such as increased market share, revenue growth, cost reduction, improved product quality, or enhanced brand reputation.
2	Time Frame	Determine the timeframe within which the benefits are expected to materialize.	Assess whether the benefits are short-term or long-term. This helps in setting realistic expectations and planning
3	Alignment with Goals	Evaluate how well the benefits align with organizational goals and objectives.	Ensure that the benefits directly contribute to achieving strategic objectives

			and are consistent with the organization's mission.
4	Attribution	Understand which aspects of the subject are responsible for generating specific benefits.	Attribute benefits to specific features or actions related to the subject. This helps in optimizing and replicating successful strategies.
5	Risk Mitigation	Consider how the benefits contribute to risk mitigation and resilience.	Analyze whether the benefits help in reducing risks, enhancing resilience to external factors, or improving the organization's ability to respond to challenges.

5.8.3 Constraints

Constraints encompass the limitations, barriers, or challenges that may impede the successful execution of the subject of analysis [206]. To identify these, the following determinant issues and key attributes are considered as shown in below table.

Table 5.3: The summary of determinant issues and key attributes of various factors in terms of constraints.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Resource Limitations	Assess the availability of resources, including budget, personnel, and technology.	Identify resource constraints that may affect the subject's implementation. Consider whether resource allocation is adequate.
2	Regulatory Compliance	Examine regulatory requirements and compliance issues.	Identify any legal or regulatory constraints that may impact the subject's implementation. Ensure that the subject complies with applicable laws and regulations.

3	Technological Challenges	Evaluate the technological feasibility and readiness for implementation.	Consider whether technological constraints, such as compatibility issues or infrastructure limitations, need to be addressed
4	Time Constraints	Assess the time frame available for implementation.	Determine whether time constraints, such as tight deadlines, could hinder the subject's successful execution. Develop strategies to manage time effectively.
5	Stakeholder Resistance	Anticipate potential resistance from stakeholders.	Identify stakeholders who may resist the subject's implementation and understand their concerns. Develop strategies for stakeholder engagement and communication.

5.8.4 Disadvantages

Disadvantages involve the potential drawbacks, risks, or negative consequences associated with the subject of analysis [207]. To identify these, the following determinant issues and key attributes are considered as shown in below table.

Table 5.4: The summary of determinant issues and key attributes of various factors in terms of advantages.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Risk Identification	Conduct a comprehensive risk assessment.	Identify potential risks and negative consequences associated with the subject. Consider both the likelihood and severity of these risks.

2	Reputational Impact	Evaluate how the subject may impact the organization's reputation.	Consider whether the subject poses reputational risks, such as negative public perception or damage to the brand image.
3	Financial Implications	Assess the financial implications of potential disadvantages.	Analyze the financial risks, including potential losses, increased costs, and budget overruns, that may arise from the subject's implementation.
4	Contingency Planning	Develop contingency plans for managing disadvantages.	Create strategies and action plans to mitigate or address potential disadvantages if they materialize. This ensures preparedness.
5	Monitoring and Evaluation	Plan for ongoing monitoring and evaluation.	Establish mechanisms for continuously assessing the subject's impact and identifying disadvantages as they emerge. This allows for timely interventions.

Effective ABCD analysis involves a holistic approach that integrates all four dimensions. Consider how the advantages align with the benefits, how constraints may impact disadvantages, and vice versa. A well-rounded analysis provides a comprehensive view of the subject, enabling more informed decision-making. The ABCD analysis is a valuable tool for systematically evaluating decisions, strategies, projects, or situations [208]. Understanding the determinant issues and key attributes within each dimension (Advantages, Benefits, Constraints, and Disadvantages) is essential for conducting a thorough and insightful analysis. By considering these factors, organizations can make informed choices that optimize positive outcomes, mitigate risks, and align with their strategic goals.

5.9 Framework of Systematic Review of its Usage

The ABCD analysis framework, which stands for Advantages, Benefits, Constraints, and Disadvantages, is a structured approach used to evaluate a subject or decision comprehensively. It provides a systematic method for considering both positive and negative aspects to make well-informed decisions. In this systematic review, we will explore the usage of the ABCD analysis framework in various contexts and industries [209].

Table 5.5: The summary of Systematic Review of ABCD Analysis Usage.

Sl. No.	Factor	Application	Benefits	Constraints
1	Strategic Planning	The ABCD framework is widely used in strategic planning. Organizations evaluate proposed strategies by considering their advantages and benefits against constraints and disadvantages. This aids in selecting strategies aligned with long-term objectives.	Improved alignment with organizational goals, better resource allocation, and reduced risks associated with strategic decisions.	Subjectivity in assessing advantages and disadvantages, and the need for thorough data collection.
2	Project Management	Project managers employ the ABCD analysis to assess project feasibility, resource allocation, and risk mitigation. It helps in understanding the	Enhanced project planning, effective resource allocation, and better risk management.	Time-consuming process, and the need for detailed analysis for complex projects.

		potential benefits and constraints involved.		
3	Risk Assessment	In risk assessment, the ABCD framework helps in identifying potential disadvantages and constraints that could lead to adverse events. It assists in devising mitigation strategies.	Enhanced risk management, proactive identification of potential issues, and improved decision-making.	Subjectivity in risk assessment and the challenge of predicting all possible risks.
4	Investment Analysis	Investors and financial analysts use ABCD analysis to evaluate investment opportunities. They assess potential advantages and benefits against constraints and disadvantages to make investment decisions.	Informed investment decisions, reduced financial risks, and improved portfolio management.	The complexity of financial markets and the need for robust data analysis.
5	Product Development	Businesses apply the ABCD framework to assess new product ideas. It helps in evaluating potential benefits and advantages against constraints and disadvantages.	Enhanced product development decisions, improved product quality, and increased market competitiveness.	Subjectivity in product assessment and the need for comprehensive market research.
6	Supply Chain Management	In supply chain and inventory	Reduced carrying costs, improved	Continuous monitoring and

		management, ABCD analysis helps optimize stock levels. It categorizes items based on their importance and value, enabling organizations to allocate resources effectively.	inventory turnover, and better supply chain efficiency.	updating of item categorization.
7	Strategic Resource Allocation	Organizations employ the ABCD framework to allocate resources such as budgets, personnel, and technology. It helps prioritize resource allocation based on potential advantages and benefits.	Efficient resource allocation, cost optimization, and improved strategic decision-making.	Resource constraints may limit the implementation of strategies with high potential benefits.
8	Operational Efficiency Improvement	Companies use ABCD analysis to identify areas for operational improvement. By assessing advantages and benefits against constraints and disadvantages, they prioritize process enhancements.	Enhanced efficiency, cost savings, and streamlined operations.	Resistance to change and the need for continuous process monitoring.
9	Marketing Campaign Evaluation	In marketing, the ABCD framework is employed to evaluate	Improved marketing ROI, better targeting,	The complexity of tracking campaign metrics and the

		the effectiveness of advertising campaigns. It helps assess advantages and benefits against constraints and disadvantages.	and data-driven campaign optimization.	need for real-time data analysis.
--	--	--	--	-----------------------------------

5.10 Review of Factors and Elemental ABCD Analysis with Determinant Issues

Factors and Elemental ABCD Analysis:

1. Factors in ABCD analysis typically refer to the criteria used for categorizing items. These criteria often include factors like demand volume, cost, or criticality.
2. Elemental ABCD analysis might involve breaking down these factors into more specific elements or sub-criteria. For example, if "cost" is a factor, elemental analysis could involve considering purchase cost, holding cost, or transportation cost separately.

Determinant Issues:

1. Determinant issues are the key concerns or challenges associated with ABCD analysis. These could include issues related to data accuracy, choosing appropriate criteria, or implementing the results effectively.

5.10.1 A review of Factors and Elemental ABCD Analysis and Determinant Issues:

1. **Factors in ABCD Analysis:** Analyzing the different factors commonly used in ABCD analysis and their relative importance in various industries or contexts.
2. **Elemental Analysis:** Exploring how breaking down factors into smaller elements can provide more nuanced insights into item categorization and inventory management.
3. **Determinant Issues in ABCD Analysis:** Reviewing challenges and critical issues that organizations may encounter when implementing ABCD analysis, such as data quality issues or resistance from stakeholders.

4. **Case Studies:** Providing real-world examples and case studies of organizations that have successfully applied ABCD analysis, highlighting the factors, elemental analysis, and how they addressed determinant issues.

5.11. Key Attributes under Cyber Security in ABCD Analysis

In ABCD analysis applied to cybersecurity, there are four key attributes that are typically used to categorize assets or components based on their importance or risk level. These key attributes are:

1. **Asset Value (A):** Asset value refers to the importance or value of a particular component or asset within the organization's cybersecurity infrastructure. This attribute assesses how critical the asset is to the organization's operations. High-value assets (e.g., customer databases, critical systems) fall into the "A" category, signifying their utmost importance.
2. **Business Impact (B):** Business impact measures the potential consequences of a cybersecurity breach or compromise on the organization's operations. It considers factors such as financial losses, reputational damage, legal implications, and operational disruptions. Assets with a significant potential impact on the business are categorized as "B."
3. **Criticality (C):** Criticality assesses the level of criticality or essentiality of an asset in supporting the organization's core functions. It considers how integral an asset is to business processes and continuity. High-criticality assets are categorized as "C."
4. **Defense Difficulty (D):** Defense difficulty evaluates the challenges and complexities associated with protecting an asset from cybersecurity threats. This attribute takes into account factors like the asset's susceptibility to attacks, the effectiveness of existing security measures, and the difficulty of implementing additional safeguards. Assets that are challenging to defend effectively are categorized as "D."

These four key attributes provide a structured framework for organizations to assess and categorize their cybersecurity assets, helping them prioritize their cybersecurity efforts and allocate resources according to the level of risk or importance associated with each asset. This approach is valuable for effective risk management and resource optimization in cybersecurity.

Cybersecurity is a critical concern for organizations in today's digital age. To effectively manage cybersecurity risks, many organizations employ the ABCD analysis framework, which categorizes assets based on their importance or risk level. The key attributes in cybersecurity ABCD analysis are Asset Value (A), Business Impact (B), Criticality (C), and Defense Difficulty (D) [210]. These attributes help organizations prioritize their cybersecurity efforts and allocate resources appropriately.

Table 5.6: Advantages of key attributes under cyber security in ABCD analysis

Sl. No.	Factor	Definition	Advantages
1	Asset Value	Asset Value (A) refers to the importance or value of a particular asset within an organization's cybersecurity infrastructure. This attribute assesses how critical the asset is to the organization's operations, reputation, and overall success.	<ul style="list-style-type: none"> • Resource Prioritization: By categorizing assets based on their value, organizations can prioritize resource allocation for the protection of high-value assets. • Risk Mitigation: Identifying and protecting high-value assets helps reduce the risk of financial losses and reputational damage in case of a cybersecurity breach. • Strategic Focus: Focusing on asset value aligns cybersecurity efforts with the organization's strategic goals and objectives.
2	Business Impact	Business Impact (B) measures the potential consequences of a cybersecurity breach or compromise on an organization's operations. It takes into account various factors, including financial	<ul style="list-style-type: none"> • Informed Decision-Making: Assessing business impact helps organizations make informed decisions regarding cybersecurity investments and risk management strategies. • Risk Assessment: It enables a comprehensive risk assessment

		losses, reputational damage, legal implications, and operational disruptions.	that considers real-world business implications.
3	Criticality	Criticality (C) assesses the level of criticality or essentiality of an asset in supporting an organization's core functions and business continuity. It considers how integral an asset is to business processes.	<ul style="list-style-type: none"> • Business Continuity: Identifying asset criticality helps organizations ensure business continuity by focusing on protecting assets essential for core operations. • Risk Reduction: It enhances overall resilience against cyber threats by prioritizing the protection of critical assets.
4	Defense Difficulty	Defense Difficulty (D) evaluates the challenges and complexities associated with protecting an asset from cybersecurity threats. This attribute takes into account factors such as the asset's susceptibility to attacks, the effectiveness of existing security measures, and the difficulty of implementing additional safeguards.	<ul style="list-style-type: none"> • Proactive Risk Mitigation: Highlighting assets that are challenging to defend effectively promotes a proactive approach to addressing cybersecurity weaknesses. • Continuous Improvement: Encourages continuous improvement in cybersecurity practices and capabilities.

Table 5.7: Benefits of key attributes under cyber security in ABCD analysis

Sl. No.	Factor	Definition	Benefits
1	Asset Value	Asset Value (A) refers to the importance or value of a particular asset within an organization's cybersecurity	<ul style="list-style-type: none"> • Protection of Critical Assets: High-value assets are safeguarded effectively, reducing the likelihood of data

		<p>infrastructure. This attribute assesses how critical the asset is to the organization's operations, reputation, and overall success.</p>	<p>breaches or system compromises.</p> <ul style="list-style-type: none"> • Cost Reduction: Resource allocation is optimized, minimizing unnecessary cybersecurity spending on low-value assets. • Compliance: Asset value considerations are often aligned with regulatory requirements, facilitating compliance efforts.
2	Business Impact	<p>Business Impact (B) measures the potential consequences of a cybersecurity breach or compromise on an organization's operations. It takes into account various factors, including financial losses, reputational damage, legal implications, and operational disruptions.</p>	<ul style="list-style-type: none"> • Incident Response Planning: Understanding business impact supports the development of effective incident response and recovery plans. • Prioritization of Mitigation Efforts: Organizations can prioritize efforts to protect assets that, if compromised, would have the most significant business impact
3	Criticality	<p>Criticality (C) assesses the level of criticality or essentiality of an asset in supporting an organization's core functions and business continuity. It considers</p>	<ul style="list-style-type: none"> • Disaster Recovery Planning: Asset criticality supports disaster recovery planning, ensuring that vital assets are quickly restored in case of an incident.

		how integral an asset is to business processes.	<ul style="list-style-type: none"> Resource Allocation Efficiency: Resources are allocated efficiently, as high-criticality assets receive the attention they require.
4	Defense Difficulty	Defense Difficulty (D) evaluates the challenges and complexities associated with protecting an asset from cybersecurity threats. This attribute takes into account factors such as the asset's susceptibility to attacks, the effectiveness of existing security measures, and the difficulty of implementing additional safeguards.	<ul style="list-style-type: none"> Resource Optimization: Identifying assets with higher defense difficulty allows organizations to allocate additional resources or expertise where needed most. Vulnerability Mitigation: Assets that are challenging to defend can be prioritized for vulnerability management and mitigation efforts.

Table 5.8: Constraints of key attributes under cyber security in ABCD analysis

Sl. No.	Factor	Definition	Constraints
1	Asset Value	Asset Value (A) refers to the importance or value of a particular asset within an organization's cybersecurity infrastructure. This attribute assesses how critical the asset is to the organization's operations, reputation, and overall success.	<ul style="list-style-type: none"> Resource Allocation Challenge: Protecting high-value assets may require significant investments in security measures, which can strain an organization's resources. Neglect of Less Valuable Assets: Overemphasis on asset value alone may neglect less valuable but

			still important assets, creating vulnerabilities.
2	Business Impact	Business Impact (B) measures the potential consequences of a cybersecurity breach or compromise on an organization's operations. It takes into account various factors, including financial losses, reputational damage, legal implications, and operational disruptions.	<ul style="list-style-type: none"> • Complex Assessment: Assessing the full extent of business impact can be complex and time-consuming, requiring access to comprehensive data on business operations. • Subjectivity: Determining the business impact may involve subjective judgments, potentially leading to varying assessments.
3	Criticality	Criticality (C) assesses the level of criticality or essentiality of an asset in supporting an organization's core functions and business continuity. It considers how integral an asset is to business processes.	<ul style="list-style-type: none"> • Subjective Assessment: Determining asset criticality may involve subjective judgments, and different stakeholders may have varying views. • Risk of Neglect: Focusing on critical assets alone may lead to neglect of less critical but still valuable assets, potentially creating vulnerabilities
4	Defense Difficulty	Defense Difficulty (D) evaluates the challenges and complexities associated with protecting an asset from cybersecurity threats. This attribute takes into account	<ul style="list-style-type: none"> • Technical Expertise Required: Assessing defense difficulty may require technical expertise

		factors such as the asset's susceptibility to attacks, the effectiveness of existing security measures, and the difficulty of implementing additional safeguards.	and risk assessments, which can be resource-intensive. <ul style="list-style-type: none"> • Resource Intensive: It may uncover vulnerabilities that demand immediate attention and resource allocation.
--	--	---	--

Table 5.9: Drawbacks of key attributes under cyber security in ABCD analysis

Sl. No	Factor	Definition	Drawbacks
1	Asset Value	Asset Value (A) refers to the importance or value of a particular asset within an organization's cybersecurity infrastructure. This attribute assesses how critical the asset is to the organization's operations, reputation, and overall success.	Limited Scope: Focusing solely on asset value may not consider other critical factors like business impact or criticality, leading to an incomplete risk assessment.
2	Business Impact	Business Impact (B) measures the potential consequences of a cybersecurity breach or compromise on an organization's operations. It takes into account various factors, including financial losses, reputational damage, legal implications, and operational disruptions.	Overly Cautious Approaches: Organizations may adopt overly cautious cybersecurity approaches if they focus solely on high business impact without considering other attributes.

3	Criticality	Criticality (C) assesses the level of criticality or essentiality of an asset in supporting an organization's core functions and business continuity. It considers how integral an asset is to business processes.	Potential for Overemphasis: Organizations may overly prioritize high-criticality assets, neglecting other factors like asset value or defense difficulty.
4	Defense Difficulty	Defense Difficulty (D) evaluates the challenges and complexities associated with protecting an asset from cybersecurity threats. This attribute takes into account factors such as the asset's susceptibility to attacks, the effectiveness of existing security measures, and the difficulty of implementing additional safeguards.	Resource Allocation Challenges: Organizations may need to invest more resources in securing assets with high defense difficulty, potentially straining their budgets.

The key attributes under cybersecurity in ABCD analysis - Asset Value (A), Business Impact (B), Criticality (C), and Defense Difficulty (D) - provide organizations with a structured framework to assess and categorize their assets based on their importance and risk [211]. Each attribute offers advantages, benefits, constraints, and potential drawbacks that organizations must carefully consider in their cybersecurity risk management strategies. By balancing these attributes and applying them effectively, organizations can optimize their cybersecurity efforts, reduce risks, and better protect their digital assets in an increasingly interconnected world.

5.12 ABCD Analysis of Cyber Security in Terms of Performance Metrics

In the context of cybersecurity, ABCD analysis can be applied to evaluate the performance of various security measures, components, or aspects of an organization's security posture. By applying ABCD analysis to cybersecurity performance metrics, organizations can better allocate their resources, prioritize security efforts, and improve their overall security posture.

5.12.1 ABCD Analysis of Cyber Security in Terms of Performance Metrics Sensitivity

Cyber attack detection and mitigation play a crucial role in ensuring the security of digital systems. When evaluating these processes in terms of the performance metric "sensitivity," which measures the ability to correctly identify all relevant instances of cyber attacks, here are some advantages, benefits, constraints, and drawbacks:

Table 5.10: Advantages and Benefits of performance metrics sensitivity under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Improved Security	Cyber attack detection and mitigation enhance overall security by identifying and responding to threats in real-time, reducing the risk of data breaches and system compromise.
2	Early Threat Detection	High sensitivity in detection systems allows for the early identification of potential threats, minimizing the time attackers have to exploit vulnerabilities.
3	Reduced False Positives	Advanced detection systems with high sensitivity often result in fewer false alarms, reducing the operational burden on security teams.
4	Compliance	Meeting regulatory and compliance requirements becomes easier when you can demonstrate effective detection and mitigation capabilities.
5	Business Continuity	Effective cyber attack detection and mitigation help maintain business continuity by preventing or minimizing disruptions caused by attacks

Table 5.11: Constraints and Drawbacks of performance metrics sensitivity under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Resource Intensive	High-sensitivity detection systems may require significant computational resources, which can lead to performance bottlenecks or increased costs.

2	Complexity	Implementing and managing sensitive detection systems can be complex, requiring skilled personnel and specialized tools.
3	Tuning Challenges	Balancing sensitivity to detect real threats with minimizing false positives can be challenging and requires ongoing tuning and refinement.
4	Privacy Concerns	Sensitive detection methods may inadvertently intrude on user privacy, raising ethical and legal concerns.
5	Cost	Advanced detection and mitigation solutions can be expensive to deploy and maintain, making them less accessible to smaller organizations.
6	Overhead	Some sensitive detection methods may introduce network or system overhead, affecting overall performance.

5.12.2 ABCD Analysis of Cyber Security in Terms of Performance Metrics Specificity

Cyber attack detection and mitigation play a crucial role in ensuring the security of digital systems. When evaluating these processes in terms of the performance metric "specificity," which measures the ability to correctly identify all relevant instances of cyber attacks, here are some advantages, benefits, constraints, and drawbacks:

Table 5.12: Advantages and Benefits of performance metrics specificity under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Improved Security	Cyber attack detection and mitigation enhance overall security by identifying and countering threats promptly.
2	Early Warning	Early detection allows organizations to respond quickly, minimizing potential damage.
3	Reduced Downtime	Mitigation helps reduce system downtime, ensuring business continuity.
4	Data Protection	It safeguards sensitive data from unauthorized access or theft.
5	Legal Compliance	Complying with regulations is easier when cyber threats are actively addressed.
6	Reputation Preservation	Protecting against cyber attacks helps maintain a positive reputation.

Table 5.13: Constraints and Drawbacks of performance metrics specificity under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	False Positives	High specificity may lead to false positives, wasting resources investigating non-threats.
2	Resource Intensive	Effective detection and mitigation require significant computing power and personnel.
3	Complexity	Implementation and maintenance can be complex and costly.
4	Privacy Concerns	Overly aggressive measures may infringe on user privacy.
5	Adaptability	Attackers evolve, and detection methods may struggle to keep up.
6	Cost	Comprehensive solutions can be expensive to deploy and maintain.

5.12.3 ABCD Analysis of Cyber Security in Terms of Performance Metrics Precision

The advantages, benefits, constraints, and drawbacks of cyber attack detection and mitigation in terms of performance metrics, specifically focusing on precision:

Table 5.14: Advantages and Benefits of performance metrics precision under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	High Precision	Cyber attack detection and mitigation systems aim to minimize false positives, making them highly precise in identifying actual threats. High precision means that when an alert is triggered, it is more likely to be a genuine threat, reducing the chances of unnecessary actions.
2	Reduced False Alarms	The high precision of these systems leads to fewer false alarms, allowing security teams to focus their efforts on legitimate threats, which saves time and resources.

3	Enhanced Security	Improved precision means a better chance of identifying sophisticated, targeted attacks that could have severe consequences if left undetected.
4	Compliance	Many industries and organizations must adhere to regulatory requirements regarding cybersecurity. Precise detection and mitigation help meet these compliance obligations.

Table 5.15: Constraints and Drawbacks of performance metrics precision under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Overlooked Threats	Overemphasis on precision can lead to the system missing certain threats, especially those that are evolving and using novel techniques. This can create a false sense of security.
2	Resource Intensive	Achieving high precision often requires sophisticated algorithms and extensive computational resources. This can be costly to implement and maintain.
3	Complexity	Precision-focused systems can be complex to configure and fine-tune. They may require a skilled cybersecurity team to manage effectively.
4	Potential for Slow Response	Excessive emphasis on precision can lead to slower response times when a real threat is detected, as the system may spend more time analyzing data to reduce false positives.
5	Limited Scalability	Maintaining high precision at scale can be challenging. As the volume of data and network traffic increases, maintaining the same level of precision can become difficult.

While precision is a critical performance metric in cyber attack detection and mitigation, it's essential to strike a balance between precision and other metrics like recall (the ability to detect all actual threats). Overemphasizing precision can lead to certain threats being overlooked and may pose resource and complexity challenges.

5.12.4 ABCD Analysis of Cyber Security in Terms of Performance Metrics Recall

Cyber attack detection and mitigation play a crucial role in ensuring the security of digital systems. When evaluating these processes in terms of the performance metric "recall," which measures the ability to correctly identify all relevant instances of cyber attacks, here are some advantages, benefits, constraints, and drawbacks:

Table 5.16: Advantages and Benefits of performance metrics recall under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	High Sensitivity	A high recall rate indicates that the system effectively identifies most cyber attacks, reducing the risk of undetected threats.
2	Early Threat Detection	Improved recall means that threats can be detected at an early stage, allowing for prompt mitigation and minimizing potential damage.
3	Enhanced Security	A system with high recall is more likely to catch sophisticated and evasive attacks, enhancing overall security.
4	Reduced False Negatives	Improved recall reduces the number of false negatives, ensuring that genuine threats are not overlooked.

Table 5.17: Constraints and Drawbacks of performance metrics recall under cyber security

Sl. No.	Factor	Constraints and Drawbacks
1	Increased False Positives	In pursuit of higher recall, there may be an increase in false positives, leading to unnecessary alerts and potentially overwhelming security personnel.
2	Resource Intensive	Implementing systems with high recall often requires significant computational resources, which can be costly.
3	Complexity	Highly sensitive detection systems can be complex to configure and maintain, requiring skilled personnel.

4	Trade-off with Precision	Recall is often in a trade-off relationship with precision. Increasing recall may decrease precision, meaning more false alarms.
5	Limited Scope	Achieving extremely high recall may not be feasible for all types of cyber attacks, and certain attacks may still go undetected.
6	Contextual Challenges	Recognizing novel or zero-day attacks, for which there is no prior data, can be challenging for recall-focused systems.

While high recall is essential for comprehensive cyber attack detection and mitigation, it must be balanced with precision and consider resource constraints. The choice of recall as a performance metric should align with the specific security goals and operational requirements of the organization or system in question.

5.12.5 ABCD Analysis of Cyber Security in Terms of Performance Metrics F-measure

When it comes to cyber attack detection and mitigation, performance metrics like the F-measure can help assess the effectiveness of these systems.

Table 5.18: Advantages and Benefits of performance metrics F-measure under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Precision and Recall Balance	The F-measure combines precision and recall, providing a single metric that balances the trade-off between false positives and false negatives. This helps in understanding how well the system detects and mitigates attacks without overwhelming security teams with false alarms.
2	Comprehensive Assessment	It provides a holistic view of system performance, considering both successful detections and missed attacks, making it a useful metric for assessing the overall effectiveness of a cyber attack detection and mitigation system.
3	Quantitative Comparison	F-measure allows for quantitative comparisons between different detection and mitigation approaches, making it easier to evaluate and choose the most suitable solution for a specific context.

Table 5.19: Constraints and Drawbacks of performance metrics F-measure under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Threshold Dependency	F-measure is sensitive to the choice of a threshold for classification. Adjusting the threshold can significantly impact the F-measure, making it challenging to determine an optimal setting that balances precision and recall for all scenarios.
2	Class Imbalance	In real-world scenarios, the number of legitimate network activities often greatly outweighs the number of cyber attacks. This class imbalance can affect the F-measure, as the system may have high precision but lower recall due to a focus on minimizing false positives.
3	Limited to Binary Classification	F-measure is typically used for binary classification (attack vs. non-attack), which may not fully capture the complexity of modern cyber threats that involve multiple attack vectors and stages.
4	Difficulty in Interpretation	While the F-measure provides a single metric, it may not offer detailed insights into the specific strengths and weaknesses of a system. Security analysts may need additional metrics and visualizations to understand the system's behavior better.
5	Doesn't Account for Attack Severity	The F-measure treats all attacks and missed detections equally, without considering the potential impact or severity of different types of attacks.

5.12.6 ABCD Analysis of Cyber Security in Terms of Performance Metrics Accuracy

An analysis of cybersecurity in terms of performance metrics accuracy, considering the advantages, benefits, constraints, and disadvantages are listed in below tables.

Table 5.20: Advantages and Benefits of performance metrics accuracy under cyber security.

Sl. No.	Factor	Advantages and Benefits
---------	--------	-------------------------

1	effective Decision-Making	Accurate performance metrics provide reliable data, enabling organizations to make informed decisions about their cybersecurity strategies.
2	Early Threat Detection	Accurate metrics help in the early detection of security threats and vulnerabilities, allowing for timely mitigation.
3	Improved Resource Allocation	Organizations can allocate resources more efficiently when they have accurate data on where security improvements are needed most.
4	Compliance Assurance	Accurate metrics assist in demonstrating compliance with industry regulations and standards, reducing legal and financial risks.
5	Benchmarking	Accurate metrics allow organizations to benchmark their security performance against industry standards and best practices.

Table 5.21: Constraints and Drawbacks of performance metrics accuracy under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Data Collection Challenges	Gathering accurate data can be challenging, especially in complex IT environments with diverse systems and tools.
2	False Positives/Negatives	Accuracy issues can lead to false positives (indicating a threat when there isn't one) or false negatives (failing to detect an actual threat), which can undermine trust in the metrics.
3	Measurement Complexity	Some aspects of cybersecurity, like quantifying the effectiveness of security awareness training, are inherently challenging to measure accurately.
4	Resource Intensiveness	Achieving high accuracy may require significant resources, including advanced tools and skilled personnel.
5	Dynamic Threat Landscape	The cybersecurity landscape evolves rapidly, and accurate metrics can quickly become outdated if not continuously monitored and adjusted.

6	Limited Visibility	Some cybersecurity threats may occur outside an organization's network, making it challenging to gather accurate data on them.
7	Human Error	Inaccuracies can occur due to human error in data collection, analysis, or reporting.
8	Overemphasis on Metrics	Relying solely on metrics for decision-making can lead to overlooking qualitative aspects of cybersecurity, such as social engineering attacks.

Balancing the advantages and disadvantages of accuracy in performance metrics is crucial [212]. Organizations should invest in accurate data collection methods, regularly update their metrics, and supplement quantitative data with qualitative assessments to achieve a more comprehensive understanding of their cybersecurity posture.

5.12.7 ABCD Analysis of Cyber Security in Terms of Performance Metrics False Positive Rate

Cyber attack detection and mitigation come with various advantages, benefits, constraints, and drawbacks in terms of performance metrics like the False Positive Rate (FPR).

Table 5.22: Advantages and Benefits of performance metrics False Positive Rate under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Enhanced Security	Effective detection and mitigation help protect sensitive data and systems from cyber threats, reducing the risk of breaches.
2	Early Threat Detection	Cybersecurity tools can identify attacks in their early stages, allowing organizations to respond before significant damage occurs.
3	Cost Savings	By preventing successful attacks, organizations can avoid the financial losses associated with data breaches and system downtime.
4	Regulatory Compliance	Many industries and regions have stringent data protection regulations. Proper detection and mitigation measures help organizations stay compliant.

5	Reputation Management	Successfully preventing cyberattacks helps maintain the trust of customers and partners, safeguarding an organization's reputation.
6	Incident Response Improvement	Continuous monitoring and analysis can lead to improved incident response capabilities over time.

Table 5.23: Constraints and Drawbacks of performance metrics False Positive Rate under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	False Positives	The main constraint is the False Positive Rate (FPR), where legitimate activities are incorrectly flagged as threats. High FPR can lead to unnecessary alerts and operational disruptions.
2	Resource Intensive	Implementing robust detection and mitigation systems can be resource-intensive, requiring significant hardware, software, and personnel investments.
3	Complexity	Cybersecurity solutions can be complex, requiring specialized knowledge to configure and maintain effectively
4	Evolving Threats	Cyber threats are constantly evolving, and attackers frequently adapt their tactics. Detection and mitigation methods may lag behind emerging threats
5	Privacy Concerns	Some detection methods can intrude on user privacy, raising ethical and legal concerns.
6	User Experience	Excessive false positives can negatively impact user experience, leading to frustration and reduced productivity.

While cyber attack detection and mitigation offer substantial advantages in terms of security and compliance, they also come with the constraint of managing the False Positive Rate, which, if not properly addressed, can lead to operational challenges and reduced user satisfaction. Balancing these factors is crucial for effective cybersecurity measures.

5.12.8 ABCD Analysis of Cyber Security in Terms of Performance Metrics False Negative Rate

Cyber attack detection and mitigation are crucial aspects of cybersecurity, and performance metrics like false negative rates play a significant role in evaluating their effectiveness [213]. Here are some advantages, benefits, constraints, and drawbacks in terms of this specific performance metric:

Table 5.24: Advantages and Benefits of performance metrics False Negative Rate under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Improved Security	Low false negative rates indicate that the system is effective at detecting genuine threats. This directly contributes to improved overall cybersecurity.
2	Early Threat Detection	A low false negative rate means that cyber threats are identified early in their lifecycle, allowing organizations to respond proactively and reduce potential damage.
3	Reduced Risk	By minimizing missed threats, organizations can reduce the risk of data breaches, financial losses, and reputational damage.
4	Enhanced Trust	Effective detection and low false negative rates can enhance customer and stakeholder trust in an organization's ability to protect sensitive data.

Table 5.25: Constraints and Drawbacks of performance metrics False Negative Rate under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Resource Intensive	Achieving a low false negative rate often requires advanced technologies and significant computational resources, which can be expensive to implement and maintain.
2	False Positives	While focusing on reducing false negatives, there's a risk of increasing false positives, which can lead to unnecessary alerts and operational disruptions.

3	Complexity	Highly accurate detection systems tend to be complex and may require skilled personnel to operate and fine-tune, adding to operational complexity and costs.
4	Adaptation Challenges	Cyber threats constantly evolve, and achieving a consistently low false negative rate may be challenging as attackers develop new techniques and tactics.
5	Privacy Concerns	Some advanced detection methods may involve the monitoring of user activities, which can raise privacy concerns and legal issues.
6	Overfitting	Over-optimization to reduce false negatives may lead to overfitting, where the system becomes less effective at handling new, previously unseen threats.

Achieving a low false negative rate in cyber attack detection and mitigation is a critical goal, but it comes with its own set of advantages, constraints, and potential drawbacks. Organizations must carefully balance these factors to develop a robust cybersecurity strategy.

5.12.9 ABCD Analysis of Cyber Security in Terms of Performance Metrics Matthews Correlation Coefficient

Cyber-attack detection and mitigation involve complex processes that can be evaluated using performance metrics like the Matthews Correlation Coefficient (MCC) [214]. Here's an overview of the advantages, benefits, constraints, and drawbacks associated with using MCC to assess these processes:

Table 5.26: Advantages and Benefits of performance metrics Matthews Correlation Coefficient under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Robustness	MCC provides a balanced measure that considers both true positives and true negatives, making it suitable for imbalanced datasets common in cyber attack detection.
2	Sensitivity and Specificity	MCC considers both sensitivity (true positive rate) and specificity (true negative rate), allowing for a holistic evaluation of a system's performance.

3	Easy Interpretation	MCC values range from -1 to +1, with higher values indicating better performance. This simplicity makes it easy to interpret and compare results.
4	Suitable for Binary Classification	MCC is well-suited for binary classification problems, which are common in cyber attack detection (attack or non-attack).

Table 5.27: Constraints and Drawbacks of performance metrics Matthews Correlation Coefficient under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Limited to Binary Classification	MCC is not designed for multi-class classification, which can be a limitation when dealing with more complex cyber-attack scenarios involving multiple attack types.
2	Sensitivity to Imbalanced Datasets	While MCC is robust to imbalanced datasets to some extent, extreme class imbalances can still lead to skewed results.
3	Focus on two Classes	MCC is primarily concerned with the performance of two classes (positive and negative), which may not fully capture the nuances of multi-stage or multi-layer cyber-attack detection systems.
4	Lack of Explanation	MCC provides a numerical score but does not explain the underlying reasons for a system's performance, making it less useful for diagnosing specific weaknesses.

Using the Matthews Correlation Coefficient (MCC) to evaluate cyber-attack detection and mitigation has advantages in terms of robustness and simplicity, especially for binary classification tasks. However, it may have limitations when dealing with multi-class problems or highly imbalanced datasets, and it doesn't provide detailed insights into the causes of performance. It's important to consider these factors when choosing performance.

5.12.10 ABCD Analysis of Cyber Security in Terms of Performance Metrics Encryption and Decryption Time

Here are some advantages, benefits, constraints, and drawbacks of cyber-attack detection and mitigation in terms of encryption and decryption time:

Table 5.28: Advantages and Benefits of performance metrics encryption and decryption time under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Security Enhancement	Encryption and decryption processes are crucial for securing data in transit and at rest. Implementing these can significantly enhance overall cybersecurity.
2	Data Privacy	Encryption ensures that sensitive information remains confidential, protecting user data, financial transactions, and communications from unauthorized access.
3	Compliance	Encryption is often required to comply with data protection regulations like GDPR or HIPAA, helping organizations avoid legal issues and fines.
4	Reduced Data Breach Risk	By encrypting data, the risk of data breaches is lowered, as even if attackers gain access to encrypted data, it's unreadable without the decryption key.
5	Secure Communication	Encryption safeguards sensitive information during communication, ensuring secure email, messaging, and online transactions.
6	Trust Building	Using encryption can build trust with customers, partners, and clients, as they know their data is being handled securely.

Table 5.29: Constraints and Drawbacks of performance metrics encryption and decryption time under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Performance Impact	Encryption and decryption processes can introduce latency, affecting the speed and responsiveness of systems and applications.

2	Resource Intensive	Strong encryption requires significant computational resources, which can be a constraint on resource-limited devices or systems
3	Key Management	Proper key management is crucial for encryption. Losing encryption keys can result in data loss, and managing keys can be complex and costly.
4	Compatibility Issues	Not all systems and software support the same encryption algorithms or standards, leading to compatibility challenges when data needs to be shared or transferred.
5	Vulnerabilities	Encryption isn't immune to vulnerabilities. Weak encryption algorithms or implementation flaws can be exploited by attackers.
6	Operational Complexity	Implementing encryption and decryption processes can be operationally complex, requiring skilled personnel and ongoing maintenance.

While encryption and decryption are essential for cybersecurity, they come with trade-offs in terms of performance, resource usage, and operational complexity. Organizations need to carefully weigh the advantages and drawbacks when implementing these measures to protect their data and systems effectively.

5.12.11 ABCD Analysis of Cyber Security in Terms of Performance Metrics Security Level

Here are some advantages, benefits, constraints, and drawbacks of cyber-attack detection and mitigation in terms of security level:

Table 5.30: Advantages and Benefits of performance metrics Security Level under cyber security.

Sl. No.	Factor	Advantages and Benefits
1	Improved Security	Performance metrics help organizations identify vulnerabilities and weaknesses, allowing them to strengthen their security measures.

2	Risk Reduction	By measuring security levels, businesses can proactively identify and mitigate risks, reducing the likelihood of cyberattacks.
3	Resource Allocation	Metrics enable efficient allocation of resources by prioritizing security efforts based on the importance of assets.
4	Compliance	Performance metrics help organizations meet regulatory and compliance requirements by demonstrating their commitment to security.
5	Incident Response	Metrics aid in detecting and responding to security incidents faster, minimizing damage and downtime.

Table 5.31: Constraints and Drawbacks of performance metrics Security Level under cyber security.

Sl. No.	Factor	Constraints and Drawbacks
1	Complexity	Implementing performance metrics can be complex and resource-intensive, especially for large organizations with diverse assets.
2	False Positives/Negatives	Metrics may generate false positives or negatives, leading to wasted resources or missed threats.
3	Measurement Challenges	It can be difficult to measure security comprehensively, as some threats may go undetected or unmeasured.
4	Privacy Concerns	Collecting and analyzing security metrics may raise privacy concerns if it involves monitoring employees' activities.
5	Cost	Implementing and maintaining the infrastructure needed for robust performance metrics can be costly.
6	Data Management	Storing and managing large volumes of security-related data can be a challenge.
7	Resistance to Change	Employees may resist performance metric implementations if they perceive them as invasive or disruptive.
8	Overemphasis on Metrics	Over-reliance on metrics can lead to a false sense of security, neglecting qualitative aspects of cybersecurity.

It's essential for organizations to strike a balance between the advantages and disadvantages while implementing performance metrics for security levels [215]. Effective cybersecurity strategies should combine quantitative metrics with qualitative assessments to provide a holistic view of an organization's security posture.

5.12. Conclusion

The ABCD analysis framework is a systematic approach that helps individuals and organizations make informed decisions and solve complex problems. It encourages a structured process of assessment, creative idea generation, careful evaluation, and effective execution. This framework can be applied to a wide range of scenarios, from business strategy development to personal decision-making, to ensure that decisions are well-informed and actions are purposeful. A cyber-attack detection and mitigation framework offer several benefits, including improved security, proactive defense, risk reduction, regulatory compliance, and efficient resource allocation. However, these advantages must be weighed against the potential constraints and drawbacks, such as complexity, false positives, resource demands, and adaptability challenges. To maximize the benefits and mitigate the drawbacks, organizations should carefully choose and tailor a framework to their specific needs while staying agile in responding to evolving cyber threats.

The ABCD analysis framework is a systematic approach that helps individuals and organizations make informed decisions and solve complex problems. It encourages a structured process of assessment, creative idea generation, careful evaluation, and effective execution. This framework can be applied to a wide range of scenarios, from business strategy development to personal decision-making, to ensure that decisions are well-informed and actions are purposeful. Cyber-attack detection and mitigation offer significant advantages in protecting organizations from cyber threats and financial losses while preserving their reputation. However, these benefits come with constraints and drawbacks, such as resource requirements, false alarms, and the evolving nature of cyber threats. To effectively manage these challenges, organizations must develop a comprehensive cybersecurity strategy that balances risk and resources while continually adapting to the changing threat landscape.

CHAPTER 6

CONCLUSION

In modern society, major changes are brought about due to the technology development. However, for perpetrating human criminal activities, each technological alteration causes a few unforeseen issues by taking merits of which the lawbreakers explore novel methodologies. Not just individuals or a nation are affected by technology-generated crimes but have huge ramifications globally. The Internet, which paves the way for the menace of cybercrimes, is a gray area. A general space termed 'cyberspace' emerged through the convergence of computer networks along with telecommunications facilitated by digital technologies. For a galaxy of human activities that converge on the internet, cyberspace has emerged to be a platform; in addition, it has also become the most happening place today. For communication, commerce, advertising, banking, education, research, and entertainment, the Internet is wielded hugely. Some rare humans don't use the internet. Hence, the internet provides something to all that it just maximizes. In upcoming technologies like (a) social media, (b) cloud computing, (c) smartphone technology; (d) critical infrastructure, emerging threats were detected; always taking advantage of their unique characteristics. Nevertheless, since it requires domain knowledge about the attacks along with the ability to evaluate the threats' possibility, guaranteeing CS is a complex task. The emerging nature of attacks is the key issue of CS. Detection along with evaluation is valuable; however, deployed techniques' certain disadvantages are encompassed. Regarding detection along with the evaluation of real attacks, the information is extremely constrained. The concern for CS of ICSs is increased by the developing attacks against CPSs recently. The present efforts of ICS CS are significantly grounded on firewalls, and data diodes, together with other techniques of intrusion prevention that might not be adequate for enhancing cyber threats as motivated attackers. By employing (1) network traffic data, (2) host system data; (3) gauged process parameters, a CAD engendered on the defense-in-depth concept is presented for augmenting the ICS's CS. Thus, for physical and cyber-attacks, those systems have emerged to be a key aim. Grounded on DL-like hybrid systems, which fuse various methodologies, AI approaches have been proposed along with implemented. To present various AI techniques of DL with enhanced performance, enhancing the prevailing methods could assist. Determining malicious activity in cyberspace by employing BReLU-ResNet is the goal along with mitigating it by deploying a Bait-centric system.

For mitigation, a new technique of BReLU-ResNet-centric CAD System with a Bait-centric approach is proposed. For monitoring cyber-attacks rapidly, various operations are designed. In CAD, various operations were concerned about the methodology's efficacy. For finding intrusions, Pre-processing, characteristic extraction, FS, along with classification is wielded. Whether the data are normal or else malicious are found by the typing phase. If the records are normal or attacked are detected by the classification phase. The data transmission process starts if the data is normal. By employing SHP-ECC, the encryption and decryption process is conducted for ensuring security. For evaluating the rule's efficacy, the experiment is completed with performance and comparative evaluation of the provided techniques regarding a few performance indicators.

The experimental evaluation is done where the proven technique's performance along with comparison appraisal is encompassed regarding several performance metrics for validating the proffered technique's efficiency. By employing TN, TP, FN, and FP, the system was analyzed for offering more insight into the performance; in addition, other metrics like the classification precision, the classification recall, the F1-score of classification, FNR, together with MCC are also estimated.

Several uncertainties might be tackled by the presented system; in addition, propitious outcomes could be achieved. For the evaluation, the openly accessible UNSW-NB 15 is wielded. For sensitivity, specificity, accuracy, Precision, recall, FM, FPR, FNR, Matthew's correlation coefficient, and excessive SL, the proffered system acquired 98.34%, 77.54%, 96.6%, 97.96 %, 98.34%, 98.15 %, 22.46%, 1.66 %, 77.38 % 93.75 % respectively. When weighed against the prevailing techniques, the developed system depicted enhanced performance along with sustains to be dependable and robust. The research will be elaborated for including more superior neural networks along with various kinds of realistic attacks in the future.

CHAPTER 7

FUTURE SCOPE OF THE WORK

The research work is concluded in this chapter by suggesting future research directions.

7.1 Future Work

Some more moving target defense mechanisms can be analyzed and can be enhanced in handling unknown cyber-attacks in the future. By integrating them into hardware components, the proposed methods can be evaluated in real-time. Another extension of collaborative attacks is where the malicious nodes cooperate to attack the network. For securing the network from all other attacks, the cryptographic techniques can be integrated with the mitigating techniques. For extracting attack data, setting up honey-pots might be one of the dimensions of this extension. For detecting attack patterns, those attack data might be evaluated by employing suitable tools. For training IDS and IPS systems, the resulting patterning might be wielded for automating the future process. For the enhanced determination of cyber-attacks, those attacks might be wielded for implementing cyber threat-hunting methodologies. By utilizing honey-pot data and attack modeling methodologies, this research's other dimension might enhance the evaluation of APTs.

REFERENCES

- [1].Hu, J. (2010). Host-based anomaly intrusion detection. *Handbook of information and communication security*, 1(1), 235-255.
- [2].Kumar, D. A., & Venugopalan, S. R. (2017). Intrusion detection systems: A review. *International Journal of Advanced Research in Computer Science*, 8(8), 356-370.
- [3].Kumar, V., & Sangwan, O. P. (2012). Signature based intrusion detection system using SNORT. *International Journal of Computer Applications & Information Technology*, 1(3), 35-41.
- [4].Tucker, J., Coughlan, M. K., Nelson, T., & Klimkowski, B. (2016). Implementing an Anomaly-Based Intrusion Detection System: Focus on Internal Threat–Masquerade Attacks. *American International Journal of Contemporary Research*, 6(4), 1-11.
- [5].Raj, S., & Thomas, A. (2017). A study on various secret data embedding techniques in digital images for secure communication. *International Journal of Scientific Engineering and Science*, 1(2), 48-52.
- [6].Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *Journal of Information Security and Applications*, 58(1), 1-9.
- [7].Jiankun Hu. (2010). Host-based anomaly intrusion detection. *Handbook of Information and Communication Security*, (PP. 1-22). Springer Berlin, Heidelberg.
- [8].Ilker KARA and Murat AYDOS. (2020). Cyber fraud: Detection and analysis of the crypto-ransomware. In *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2020, pp. 28-31, 2020.
- [9].Panagiotis Kantartopoulos, Nikolaos Pitropakis, Alexios Mylonas and Nicolas Kylilis. (2020). Exploring adversarial attacks and defenses for fake Twitter account detection. *Technologies*, 8(1), 1-19.
- [10]. Palash Sandip Dusane and Yallamandhala Pavithra. (2020). Logic Bomb: An insider attack. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(3), 3662-3665.
- [11]. Tariq Banday M, Jameel A Qadri and Nisar A Shah. (2009). Study of botnets and their threats to internet security. *Sprouts: Working Papers on Information Systems*, 9(24), 1-12.

- [12]. Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3(1), 1-23.
- [13]. Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah and Farhan Ahmad. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Emerging Telecommunications Technologies*, 32(1), 1-29.
- [14]. Sandeep Singh. (2013). Intrusion detection systems (IDS) and intrusion prevention systems (IPS) for network security: A critical analysis. *International Journal of Research in Engineering & Applied Sciences*, 3(3), 1-9.
- [15]. Eric Gyamfi and Anca Jurcut. (2022). Intrusion detection in the internet of things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets. *Sensors*, 22(1), 1-33.
- [16]. Mutep Y AlYousef and Nabih T Abdelmajeed. (2019). Dynamically detecting security threats and updating a signature-based intrusion detection system's database. *Procedia Computer Science*, 159(1), 1507-1516.
- [17]. Nilotpal Chakraborty. (2013). Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research (IJCBR)*, 4(2), 1-8.
- [18]. Mohammed Misbahuddin, Sachin Narayanan, and Bishwa Ranjan Ghoshm. (2009). Dynamic IDP signature processing by fast elimination using DFA. *International Journal of Network Security & Its Applications (IJNSA)*, 1(2), 29-38.
- [19]. Ibrahim Al-Shourbaji and Samaher Al-Janabi. (2017). Intrusion detection and prevention systems in wireless networks. *Kurdistan Journal for Applied Research*, 2(3), 29-38.
- [20]. Lizhen Tang and Qusay H Mahmoud. (2021). A survey of machine learning-based solutions for phishing website detection. *Machine Learning and Knowledge Extraction*, 3(2), 672-694.
- [21]. Iqbal H Sarker. (2021). CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks. *Internet of Things*. 14(4), 1-43.
- [22]. Manhas, J., & Kotwal, S. (2021). Implementation of intrusion detection system for internet of things using machine learning techniques. *Multimedia Security: Algorithm Development, Analysis and Applications*, 20(1), 217-237.

- [23]. Muhammad Shakil Pervez and DewanMdFarid. (2014). Feature Selection and Intrusion classification in NSL-KDD Cup 99 Dataset Employing SVMs. In *8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014)*, 2014, (pp. 1-7), Dhaka, Bangladesh.
- [24]. Preeti Mishra. (2019). A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 21(1), 686-728.
- [25]. Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection Systems on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, 7(3), 366-370.
- [26]. Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering—a systematic literature review. *Information and software technology*, 51(1), 7-15.
- [27]. Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In *SoutheastCon 2017, 2017*, (pp. 1-6). IEEE.
- [28]. Chowdhury, S., (2017). Botnet detection using graph-based feature clustering. *Journal of bigdata*, 4(1), 25-36
- [29]. Neethu, B. (2013). Adaptive intrusion detection using machine learning. *International Journal of Computer Science and Network Security (IJCSNS)*, 13(3), 118-124.
- [30]. Kozik, R., Choraś, M., Renk, R., & Hołubowicz, W. (2015, September). A proposal of an algorithm for web applications cyber attack detection. In *IFIP International Conference on Computer Information Systems and Industrial Management, 2015*, (pp. 680-687). Springer, Berlin, Heidelberg.
- [31]. Nguyen, H. T., & Franke, K. (2012, December). Adaptive Intrusion Detection System via online machine learning. In *2012 12th international conference on hybrid intelligent systems (HIS), 2012*, (pp. 271-277). IEEE.
- [32]. Xie, M., Hu, J., & Slay, J. (2014, August). Evaluating host-based anomaly detection systems: Application of the one-class SVM algorithm to ADFA-LD. In *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2014*, (pp. 978-982). IEEE.
- [33]. Zamani, M., & Movahedi, M. (2013). Machine learning techniques for intrusion detection. *arXiv preprint arXiv:1312.2177*.

- [34]. Hoque, M. S., Mukit, M., Bikas, M., & Naser, A. (2012). An implementation of an intrusion detection system using a genetic algorithm. *arXiv preprint arXiv:1204.1336*.
- [35]. Wang, J., & Paschalidis, I. C. (2016). Botnet detection is based on anomaly and community detection. *IEEE Transactions on Control of Network Systems*, 4(2), 392-404.
- [36]. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Towards Generating Real-life Datasets for Network Intrusion Detection. *Int. J. Netw. Secure.*, 17(6), 683-701.
- [37]. Wijesinghe, U., Tupakula, U., & Varadharajan, V. (2015, January). An enhanced model for network flow-based botnet detection. In *Proceedings of the 38th Australasian computer science conference (ACSC 2015)*, 2015,(pp. 101-110). Sydney, Australia.
- [38]. Haddadi, F., Cong, D. L., Porter, L., & Zincir-Heywood, A. N. (2015, May). On the effectiveness of different botnet detection approaches. In *International conference on information security practice and experience, 2015*, (pp. 121-135). Springer, Cham.
- [39]. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, 51(2), 1-7.
- [40]. Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2016, January). A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. In *2016 8th International Conference on Communication Systems and Networks (COMSNETS, 2016)*, (pp. 1-2). IEEE.
- [41]. Kato, K., & Klyuev, V. (2014). An intelligent DDoS attack detection system using packet analysis and support vector machine. *IJICR*, 14(5), 35-47.
- [42]. Gallagher, B., Eliassirad, T.(2009) "Classification of http attacks: a study on the ECML/PKDD 2007 discovery challenge", *Lawrence Livermore National Laboratory (LLNL)*,2009, (1-10). Livermore, CA.
- [43].Torrano-Gimenez, C., Perez-Villegas, A., Alvarez, G., "An Anomaly- based Web Application Firewall", In *Proc. of International Conference on Security and Cryptography (SECRYPT 2009)*, (pp. 23-28). INSTICC Press.
- [44]. Grill, G., Dallaire, C. O., Chouinard, E. F., Sindorf, N., & Lehner, B. (2014). Development of new indicators to evaluate river fragmentation and flow regulation at large scales: A case study for the Mekong River Basin. *Ecological Indicators*, 45(1), 148-159.

- [45]. Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., & Hakimian, P. (2011, July). Detecting P2P botnets through network behavior analysis and machine learning. In *2011 Ninth annual international conference on privacy, security and trust*, (pp. 174-180). IEEE.
- [46]. Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December). Feasibility of supervised machine learning for cloud security. In *2016 International Conference on Information Science and Security (ICISS)*, 2016, (pp. 1-5). IEEE.
- [47]. Gallagher, B., & Eliassi-Rad, T. (2009). *Classification of http attacks: a study on the ECML/PKDD 2007 discovery challenge* (No. LLNL-TR-414570). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).
- [48]. Yusof, A. R. A., Udzir, N. I., & Selamat, A. (2016, August). An evaluation of the KNN-SVM algorithm for detection and prediction of DDoS attacks. In *International conference on industrial, engineering and other applications of applied intelligent systems*, 2016, (pp. 95-102). Springer, Cham.
- [49]. Kumar, P. A. R., & Selvakumar, S. (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. *Computer Communications*, 36(3), 303-319.
- [50]. Yavanoglu, O., & Aydos, M. (2017, December). A review on cyber security datasets for machine learning algorithms. In *2017 IEEE international conference on big data (big data), 2017*, (pp. 2186-2193). IEEE.
- [51]. Canongia, C., & Mandarino, R. (2012). Cybersecurity: The new challenge of the information society. In *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions*, 2012, (pp. 165-184). IGI Global.
- [52]. Twomey, P. (2010). Cyber Security Threats. *The Lowy Institute for International Policy, Sydney*.
- [53]. Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. *Computer networks*, 34(4), 579-595.
- [54]. McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. *ACM Transactions on Information and System Security (TISSEC)*, 3(4), 262-294.
- [55]. Perez-Villegas, A., Torrano-Gimenez, C., & Alvarez, G. (2010). Applying Markov chains to web intrusion detection. In *Proceedings of XVII Spanish meeting on*

- cryptology and information security. RECSI*, 2010, (pp. 361-366), Ed. University of Cantabria.
- [56]. TorranoGimenez C., PerezVillegas,A., Alvarez, G.,(2010). An anomaly-based approach for intrusion detection in web traffic. *Journal of Information Assurance and Security*, 5(4), 446-454.
- [57]. TorranoGimenez, C., Perez-Villegas, A., Alvarez, G.,(2010). A Self-Learning Anomaly-Based Web Application Firewall. *Advances in Intelligent and Soft Computing*, 63(1), 85-92.
- [58]. Torrano-Gimenez, C., Perez-Villegas, A., Alvarez, G. (2009). An Anomaly- based Web Application Firewall”, In Proc. of International Conference on Security and Cryptography (SECRYPT 2009), 2009, (pp. 23-28). INSTICC Press.
- [59]. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, 34(8), 5766-5781.
- [60]. Yuchong Li and Qinghui Liu. (2021). A comprehensive review study of cyber-attacks and cyber security Emerging trends and recent developments. *Energy Reports*. 7(1), 8176–8186.
- [61]. Thierry Mbah Mbelli and Barry Dwolatzky. (2016). Cyber security, a threat to cyberbanking in South Africa. In *3rd International Conference on Cyber Security and Cloud Computing*, 2016, (pp. 1-6), IEEE.
- [62]. Saravanan A and Sathya Bama S. (2019). A review on cyber security and the fifth generation cyberattacks. *Journal of Computer Science and Technology*, 12(2), 50-56.
- [63]. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62(1), 10-15.
- [64]. Shaikha Hasan, Mazen Ali, Sherah Kurnia and Ramayah Thurasamy. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58(1), 1-16.
- [65]. Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842*.
- [66]. Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. In *IOP Conference Series: Materials Science and Engineering*, 981(1), 1-8.

- [67]. Mentsiev, A. U., Magomadov, V. S., Ashakhanova, M. Z., & Alams, M. T. (2019). How the development of Blockchain affected cybersecurity. *Journal of Physics: Conference Series*, 1399(3), 1-5.
- [68]. Alex R Mathew. (2019). Cyber security through blockchain technology. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(10), 3821-3824.
- [69]. In Lee. (2020). Internet of things (IoT) cybersecurity literature review and IoT cyber risk management. *Future Internet*, 12(9), 1-21.
- [70]. Nadeem M, Marshall O, Singh S, Fang X, Yuan X (2016). Semi-supervised deep neural network for network intrusion detection. In: Proceedings of the KSU conference on cybersecurity, education, research, and practice, 2016, (pp 1–13).
- [71]. Zhao, G., Zhang, C., & Zheng, L. (2017, July). Intrusion detection using deep belief network and probabilistic neural network. In *2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC), 2017*, (pp. 639-642). IEEE.
- [72]. Alrawashdeh, K., & Purdy, C. (2016, December). Toward an online anomaly intrusion detection system based on deep learning. In *2016 15th IEEE international conference on machine learning and applications (ICMLA), 2016*, (pp. 195-200). IEEE.
- [73]. Vishwakarma, S., Sharma, V., & Tiwari, A. (2017). An intrusion detection system using KNN-ACO algorithm. *Int J Comput Appl*, 171(10), 18-23.
- [74]. Hajisalem, V., & Babaie, S. (2018). A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. *Computer Networks*, 136(1), 37-50.
- [75]. KarimipourH, Dehghantanha A, Parizi R M, Choo K R and Leung H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 7(1), 80778 - 80788.
- [76]. Kanimozhi, V., & Jacob, T. P. (2019). Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *International Journal of Engineering Applied Sciences and Technology*, 4(6), 2455-2143.
- [77]. Defu Wang, Xiaojuan Wang, Yong Zhang and Lei Jin. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of Information Security and Applications*. 46(27), 45-52.

- [78]. Wei, F., Wen, Z., & He, H. (2019). Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. *IEEE Transactions on Smart Grid*, 11(3), 2476-2486.
- [79]. Perez-Diaz, Jesus Arturo, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu (2020). Flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8(2), 155859-155872.
- [80]. Ban Mohammed Khammas. (2020). Ransomware Detection using Random Forest Technique. *ICT Express*, 6(4), 325–331.
- [81]. Farrukh, Y. A., Ahmad, Z., Khan, I., & Elavarasan, R. M. (2021, November). A sequential supervised machine learning approach for cyber attack detection in a smart grid system. In *2021 North American Power Symposium (NAPS), 2021*, (pp. 1-6). IEEE.
- [82]. Sumathy S, Revathy M and Manikandan R. (2021). Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning. *Materials Today: Proceedings(In Press)*, 5(1), 1-8.
- [83]. Iqbal H Sarker. (2021). CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks. *Internet of Things*. 14(1), 1-43.
- [84]. Manhas, J., & Kotwal, S. (2021). Implementation of intrusion detection system for internet of things using machine learning techniques. *Multimedia Security: Algorithm Development, Analysis and Applications*, 7(1), 217-237.
- [85]. Pervez, M. S., & Farid, D. M. (2014, December). Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In *The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014), 2014*, (pp. 1-6). IEEE.
- [86]. Preeti Mishra. (2019). A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 21(1), 686-728.
- [87]. Donghwoon Kwon, Hyunjoo Kim, Jino Kim, Sang C Suh, Ikkyun Kim and Kuinam J Kim. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing*. 22(2), 949–961.

- [88]. Ayyaz-Ul-Haq Qureshi, HadiLarijani, NhamoinesuMtetwa, Abbas Javedand Jawad Ahmad. (2019). RNN-ABC A New Swarm Optimization Based Technique for Anomaly Detection. *Computers*, 8(3), 1-16.
- [89]. Ying Gao, Hongrui Wu, Binjie Song, YaqiaJin, Xiongwen Luo, and Xing Zeng. (2019). A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network. *IEEE Access*, 7(2), 154560 - 154571.
- [90]. Mrutyunjaya Panda and ManasRanjanPatra. (2007). Network intrusion detection using naïve bayes. *IJCSNS International Journal of Computer Science and Network Security*. 7(12), 258-263.
- [91]. Awad W A and ELseuofi S M. (2011). Machine learning methods for spam e-mail classification. *International Journal of Computer Science & Information Technology (IJCSIT)*, 13(1), 173-184.
- [92]. RamaniSagar, RutvijJhaveri and Carlos Borrego. (2020). applications in security and evasions in machine learning a survey. *Electronics*, 1(1), 1-42.
- [93]. Renuka, D. K., Visalakshi, P., & Sankar, T. J. I. J. C. A. (2015). Improving E-mail spam classification using ant colony optimization algorithm. *Int. J. Comput. Appl*, 22(2), 22-26.
- [94]. Vivek Nandan Tiwari, SatyendraRathore and Kailash Patidar. (2016). Enhanced method for intrusion detection over KDD cup 99 datasets. *International Journal of Current Trends in Engineering & Technology*. 2(2), 218-224.
- [95]. Vinayakumar R, MamounAlazab, Soman K P, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, 7(2), 41525 - 41550.
- [96]. Anna L. Buczak and ErhanGüven. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176.
- [97]. Gary Stein, Bing Chen, Annie S Wu and KienAHua. (2005). Decision tree classifier for network intrusion detection with ga-based feature selection. In *Proceedings of the 43rd Annual Southeast Regional Conference*. March 18-20, (pp. 136-141). Kennesaw, Georgia, Alabama, USA.
- [98]. Yara Rizk, Nadine Hajj, NicholasMitri, and Mariette Awad. (2019). Deep belief networks and cortical algorithms are a comparative study for supervised classification. *Applied Computing and Informatics*. 15(2), 81-93.

- [99]. Sang Min Lee, Dong Seong Kim, Ji Ho Kim and Jong Sou Park. (2010). Spam detection using feature selection and parameters optimization. In *International Conference on Complex, Intelligent and Software Intensive Systems*. (pp. 883-888), Krakow, Poland.
- [100]. Megha Rathi and Vikas Pareek. (2013). spam mail detection through data mining – a comparative performance analysis. *International Journal of Modern Education and Computer Science*. 12(2), 31-39.
- [101]. Wang, Z. (2015). The applications of deep learning on traffic identification. *BlackHat USA*, 24(11), 1-10.
- [102]. Cox, J. A., James, C. D., & Aimone, J. B. (2015). A signal processing approach for cyber data classification with deep neural networks. *Procedia Computer Science*, 61(5), 349-354.
- [103]. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26). ACM.
- [104]. Ma, T., Wang, F., Cheng, J., Yu, Y., & Chen, X. (2016). A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. *Sensors*, 16(10), 1701-1713.
- [105]. Tang, T. A., L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho (2018). Deep recurrent neural network for intrusion detection in SDN-based networks. In *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, (pp. 202–206). IEEE.
- [106]. Chawla, S. (2017). *Deep learning-based intrusion detection system for the Internet of Things*. The University of Washington.
- [107]. Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*, 56(2), 169-175.
- [108]. Lotfollahi, M., Jafari Siavoshani, M., Shirali Hossein Zade, R., & Saberian, M. (2020). Deep packet: A novel approach for encrypted traffic classification using deep learning. *Soft Computing*, 24(3), 1999-2012.
- [109]. Zhou, L., X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang (2018). Cyber-attack classification in the smart grid via deep neural network. In *Proceedings of the*

- 2nd International Conference on Computer Science and Application Engineering, (pp. 90-103). ACM.
- [110]. Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou, F., ... & Tian, Z. (2018). Deep learning based multi-channel intelligent attack detection for data security. *IEEE transactions on Sustainable Computing*, 5(2), 204-212.
- [111]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82(2), 761-768.
- [112]. Diro, A., & Chilamkurti, N. (2018). Leveraging LSTM networks for attack detection in fog-to-things communications. *IEEE Communications Magazine*, 56(9), 124-130.
- [113]. Wang H, Ruan J, Cao G, Ma Z, Zhou B, Fu X. (2018). Deep learning aided interval state prediction for improving cyber security in energy internet. *Energy*. 174(4), 1-24.
- [114]. Fan Zhang, Hansaka Angel Dias EdirisingheKodituwakku, J. Wesley Hines, and Jamie Coble. (2019). Multi-layer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7), 4362-4369.
- [115]. Basumallik, S., R. Ma, and S. Eftekharijad (2019). Packet-data anomaly detection in pmu-based state estimator using convolutional neural network. *International Journal of Electrical Power & Energy Systems* 107(2), 690–702.
- [116]. NevrusKaja, Adnan Shaout and Di Ma. (2019). An intelligent intrusion detection system. *Applied Intelligence*. 49(6), 3235–3247.
- [117]. Kaiyuan Jiang, Wenya Wang, Aili Wang and Haibin Wu. (2020). Network intrusion detection combined hybrid sampling with a deep hierarchical network. *IEEE Access*. 8(2), 32464 - 32476.
- [118]. Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha and Reza M. Parizi. (2020). An ensemble deep learning-based cyberattack detection in an industrial control system. *IEEE Access*, 8(5), 83965-83973.
- [119]. Ismail, M., Shaaban, M. F., Naidu, M., & Serpedin, E. (2020). Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, 11(4), 3428-3437.
- [120]. Moshe Kravchik and Asaf Shabtai. (2022). Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA. *IEEE Transactions on Dependable and Secure Computing*, 19(4), 2179 - 2197.

- [121]. Zhe Wu, Scarlett Chen, David Rincon and Panagiotis D Christofides. (2020). Post-cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*. 159(6), 248-261.
- [122]. Georgios Tertytchny, Nicolas Nicolaou and Maria K Michael. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber-physical systems using machine learning. *Microprocessors and Microsystems*. 77(1), 1-23.
- [123]. Huaizhi Wang, JiaqiRuan, Guibin Wang, Bin Zhou, Yitao Liu, Xueqian Fu, Jianchun Peng. (2018). Deep learning-based interval state estimation of ac smart grids against sparse cyberattacks. *IEEE Transactions on Industrial Informatics*. 14 (11), 4766-4778.
- [124]. Defu Wang, Xiaojuan Wang, Yong Zhang and Lei Jin. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of Information Security and Applications*. 46(27), 45-52.
- [125]. Perez-Diaz, Jesus Arturo, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu (2020). Flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8(2), 155859-155872.
- [126]. KarimipourH, Dehghantanha A, Parizi R M, Choo K R and Leung H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 7(3), 80778 - 80788.
- [127]. Fanrong Wei, ZhiqiangWanHaibo He. (2019). Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning. *IEEE Transactions on Smart Grid*, 11(3), 2476-2486.
- [128]. Ismail, M., Shaaban, M. F., Naidu, M., & Serpedin, E. (2020). Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, 11(4), 3428-3437.
- [129]. Elnour M, Meskin N, Khan K, and Jain R. (2020). A dual-isolation-forests-based attack detection framework for industrial control systems. *IEEE Access*, 8(1), 36639-36651.
- [130]. Paridari K, O'Mahony N, Mady A. E. D, Chabukswar R, Boubekeur M and Sandberg H. (2017). A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. *Proceedings of the IEEE*, 106(1), 113-128.

- [131]. Barrere M, Hankin C, Nicolaou N, Eliadses D. G and Parisini T. (2020). Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *Journal of information security and applications*, 52(1), 1-17.
- [132]. Yang J, Zhou C, Yang S, Xu H and Hu B. (2017). Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(5), 4257-4267.
- [133]. Adepu S and Mathur A. (2018). Assessing the effectiveness of attack detection at a hack fest on industrial control systems. *IEEE Transactions on Sustainable Computing*, 6(2), 231-244.
- [134]. Abana M. A, Peng M, Zhao Z and Olawoyin L. A. (2016). Coverage and rate analysis in heterogeneous cloud radio access networks with device-to-device communication. *IEEE Access*, 4(2), 2357-2370.
- [135]. Sargolzaei A, Yazdani K, Abbaspour A, Crane III C. D and Dixon W. E (2019). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics*, 16(6), 4281-4292.
- [136]. Ponomarev, S., & Atkison, T. (2015). Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 252-260.
- [137]. Guo H, Pang Z. H, Sun J and Li J. (2021). An output-coding-based detection scheme against replay attacks in cyber-physical systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(10), 3306-3310.
- [138]. Han S, Xie M, Chen H. H and Ling Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE systems journal*, 8(4), 1052-1062.
- [139]. Lu K. D, Zeng G. Q, Luo X, Weng J, Luo W and Wu Y. (2021). Evolutionary deep belief network for cyber-attack detection in industrial automation and control system. *IEEE Transactions on Industrial Informatics*, 17(11), 7618-7627.
- [140]. Genge B, Siaterlis C, Fovino I. N and Masera M (2012). A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers & Electrical Engineering*, 38(5), 1146-1161.
- [141]. Baldoni S, Battisti F, Carli M and Pascucci F. (2021). On the use of Fibonacci sequences for detecting injection attacks in cyber-physical systems. *IEEE Access*, 9(1), 41787-41798.

- [142]. Sui T, Mo Y, Marelli D, Sun X and Fu, M (2020). The vulnerability of cyber-physical systems under stealthy attacks. *IEEE Transactions on Automatic Control*, 66(2), 637-650.
- [143]. Jahromi A. N, Karimipour H, Dehghantanha A and Choo K. K. R. (2021). Toward detection and attribution of cyber-attacks in IoT-enabled cyber-physical systems. *IEEE Internet of Things Journal*, 8(17), 13712-13722.
- [144]. Lv Z, Han Y, Singh A. K, Manogaran G and Lv H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics*, 17(2), 1496-1504.
- [145]. Haller P and Genge B. S (2017). Using sensitivity analysis and cross-association for the design of intrusion detection systems in industrial cyber-physical systems. *IEEE Access*, 5(1), 9336-9347.
- [146]. Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with Bait Based Approach for Mitigation. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 243-258.
- [147]. Selent, D. (2010). Advanced encryption standard. *Rivier Academic Journal*, 6(2), 1-14.
- [148]. Zhang, X., & Parhi, K. K. (2002). Implementation approaches for the advanced encryption standard algorithm. *IEEE Circuits and systems Magazine*, 2(4), 24-46.
- [149]. Heron, S. (2009). Advanced encryption standard (AES). *Network Security*, 2009(12), 8-12.
- [150]. Farooq, U., & Aslam, M. F. (2017). Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. *Journal of King Saud University-Computer and Information Sciences*, 29(3), 295-302.
- [151]. Kumar, K., Ramkumar, K. R., & Kaur, A. (2020, June). A design implementation and comparative analysis of advanced encryption standard (AES) algorithm on FPGA. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, (pp. 182-185). IEEE.
- [152]. İzdemir, F., & İdemiş İzger, Z. (2021). Rivest-Shamir-Adleman Algorithm. In *Partially Homomorphic Encryption*, (pp. 37-41). Springer, Cham.

- [153]. Bafandehkar, M., Yasin, S. M., Mahmood, R., & Hanapi, Z. M. (2013, December). Comparison of ECC and RSA algorithm in resource constrained devices. In *2013 international conference on IT convergence and security (ICITCS)* (pp. 1-3). IEEE.
- [154]. Mahto, D., Khan, D. A., & Yadav, D. K. (2016, June). Security analysis of elliptic curve cryptography and RSA. In *Proceedings of the world congress on engineering*, (pp. 419-422), 2016.
- [155]. Scripcariu, L. (2015, July). A study of methods used to improve encryption algorithms robustness. In *2015 International Symposium on Signals, Circuits and Systems (ISSCS)* (pp. 1-4). IEEE.
- [156]. Abualigah, L., Abd Elaziz, M., Sumari, P., Geem, Z. W., & Gandomi, A. H. (2022). Reptile Search Algorithm (RSA): A nature-inspired meta-heuristic optimizer. *Expert Systems with Applications*, *191*(2), 116158.
- [157]. Hazay, C., Mikkelsen, G. L., Rabin, T., Toft, T., & Nicolosi, A. A. (2019). Efficient RSA key generation and threshold paillier in the two-party setting. *Journal of Cryptology*, *32*(2), 265-323.
- [158]. Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. *Ubiquity*, *9*(20), 1-8.
- [159]. Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.
- [160]. McGrew, D., Igoe, K., & Salter, M. (2011). Fundamental elliptic curve cryptography algorithms. Retrieved from [RFC 6090: Fundamental Elliptic Curve Cryptography Algorithms \(rfc-editor.org\)](https://www.rfc-editor.org/rfc/rfc6090) on 07/05/2022.
- [161]. Setiadi, I., Kistijantoro, A. I., & Miyaji, A. (2015, August). Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems. In *2015 2nd International Conference on Advanced Informatics: Concepts, Theory and Applications (ICAICTA)* (pp. 1-6). IEEE.
- [162]. Li, V. C. (2012). Tailoring ECC for special attributes: A review. *International Journal of Concrete Structures and Materials*, *6*(3), 135-144.
- [163]. Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEE Access*, *8*(1), 52018-52027.
- [164]. Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2017). A robust ECC-based provable secure authentication protocol with privacy preserving for

- industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8), 3599-3609.
- [165]. Standard, D. E. (1999). Data encryption standard. *Federal Information Processing Standards Publication*, 5(5), 112-122.
- [166]. Biryukov, A., & De Cannière, C. (2011). Data encryption standard (DES). *Encyclopedia of Cryptography and Security*, 5(5), 295-301.
- [167]. Smid, M. E., & Branstad, D. K. (1988). Data encryption standard: past and future. *Proceedings of the IEEE*, 76(5), 550-559.
- [168]. Paar, C., & Pelzl, J. (2010). The data encryption standard (DES) and alternatives. In *Understanding Cryptography* (pp. 55-86). Springer, Berlin, Heidelberg.
- [169]. Mehrotra, K., Mohan, C. K., & Ranka, S. (1997). *Elements of artificial neural networks*. MIT press.
- [170]. Wu, Y. C., & Feng, J. W. (2018). Development and application of artificial neural network. *Wireless Personal Communications*, 102(2), 1645-1656.
- [171]. Lek, S., & Guégan, J. F. (1999). Artificial neural networks as a tool in ecological modelling, an introduction. *Ecological modelling*, 120(2), 65-73.
- [172]. Ding, S., Li, H., Su, C., Yu, J., & Jin, F. (2013). Evolutionary artificial neural networks: a review. *Artificial Intelligence Review*, 39(3), 251-260.
- [173]. Islam, M. M., & Murase, K. (2001). A new algorithm to design compact two-hidden-layer artificial neural networks. *Neural Networks*, 14(9), 1265-1278.
- [174]. Lavin, A., & Gray, S. (2016). Fast algorithms for convolutional neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 4013-4021). IEEE.
- [175]. Zhang, Q., Zhang, M., Chen, T., Sun, Z., Ma, Y., & Yu, B. (2019). Recent advances in convolutional neural network acceleration. *Neuro computing*, 323(1), 37-51.
- [176]. Liu, T., Fang, S., Zhao, Y., Wang, P., & Zhang, J. (2015). Implementation of training convolutional neural networks. *arXiv preprint arXiv:1506.01195*.
- [177]. Xiao, Q., Liang, Y., Lu, L., Yan, S., & Tai, Y. W. (2017, June). Exploring heterogeneous algorithms for accelerating deep convolutional neural networks on FPGAs. In *Proceedings of the 54th Annual Design Automation Conference 2017* (pp. 1-6). ACM publishers.
- [178]. Liu, Y. (2020). DDoS attack detection via multi-scale convolutional neural network. *Computers, Materials & Continua*, 62(3), 1317-1333.

- [179]. Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with Bait Based Approach for Mitigation. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 243-258.
- [180]. Hameed, S. S., Hassan, W. H., & Latiff, L. A. (2021). An efficient fog-based attack detection using ensemble of MOA-WMA for Internet of Medical Things. In *International Conference of Reliable Information and Communication Technology* (pp. 774-785). Springer, Cham.
- [181]. Al-Wesabi, F. N. (2020). Proposing high-smart approach for content authentication and tampering detection of Arabic text transmitted via Internet. *IEICE Transactions on Information and Systems*, 103(10), 2104-2112.
- [182]. Li, C., & Gaudiot, J. L. (2019, July). Detecting malicious attacks exploiting hardware vulnerabilities using performance counters. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, (pp. 588-597). IEEE.
- [183]. Yousefnezhad, M., Hamidzadeh, J., & Aliannejadi, M. (2021). Ensemble classification for intrusion detection via feature extraction based on deep Learning. *Soft Computing*, 25(20), 12667-12683.
- [184]. Sangeetha Prabhu, & Nethravathi, P. S., (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 176-183.
- [185]. Albawi, S., Mohammed, T. A., & Al-Zawi, S. (2017, August). Understanding of a convolutional neural network. In *2017 international conference on engineering and technology (ICET)*, (pp. 1-6). IEEE.
- [186]. Targ, S., Almeida, D., & Lyman, K. (2016). Resnet in resnet: Generalizing residual architectures. *arXiv preprint arXiv:1603.08029*.
- [187]. He, F., Liu, T., & Tao, D. (2020). Why resnet works? residuals generalize. *IEEE transactions on neural networks and learning systems*, 31(12), 5349-5362.
- [188]. Miller, V. S. (1986). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer, Berlin, Heidelberg.
- [189]. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(17), 203-209.

- [190]. Ponomarev S and Atkison T. (2015). Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 252-260.
- [191]. Bidinger, M. (1981). Performance Metrics in machine learning. *J. Chem. Inf. Model.*, 53(9), 1689-1699.
- [192]. Courtney, P., Michel, O., Cangelosi, A., Tikhanoﬀ, V., Metta, G., Natale, L., & Kernbach, S. (2009). Cognitive systems platforms using open source. In *Performance evaluation and benchmarking of intelligent systems*, (pp. 139-168). Springer, Berlin, Heidelberg.
- [193]. Meystel, A. M., & Messina, E. R., “Measuring the performance and intelligence of systems”. In *Proceedings of Performance Measurement of Intelligent Systems (PerMIS)*, Gaithersburg, 2000, pp.1-172, 2000.
- [194]. H. Alkahtani, T. H. H. Aldhyani, and M. Al-Yaari, “Adaptive anomaly detection framework model objects in cyberspace,” *Applied Bionics and Biomechanics*, vol. 6660489, p. 14, 2020.
- [195]. T. Aldhyani and M. Joshi, “Intelligent time series model to predict bandwidth utilization,” *International Journal of Advanced Computer Science and Applications*, vol. 14, pp. 130– 141, 2017.
- [196]. M. Tang, M. Alazab, and Y. Luo, “Big data for cybersecurity: vulnerability disclosure trends and dependencies,” *Institute of Electrical and Electronics Engineers Transactions on Big Data*, vol. 5, no. 3, pp. 317–329, 2019.
- [197]. D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, “MTHAEL: cross-architecture IoT malware detection based on neural network advanced ensemble learning,” *Institute of Electrical and Electronics Engineers Transactions on Computers*, vol. 69, no. 11, pp. 1654–1667, 2020.
- [198]. Aithal, P. S., Shailashree, V., & Kumar, P. M. (2015). A new ABCD technique to analyze business models & concepts. *International Journal of Management, IT and Engineering*, 5(4), 409-423.
- [199]. Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems. *International Journal in Management and Social Science*, 4(1), 95-115.

- [200]. Shenoy, V., & Aithal, P. S. (2017). Quantitative ABCD Analysis of IEDRA Model of Placement Determination. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 103-113.
- [201]. Mendon, S., & Aithal, P. S. (2022). Quantitative ABCD Analysis of Organic Food Product and its Impact on Purchase Intention. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 7(1), 254-278.
- [202]. Kumari, P., & Aithal, P. S. (2022). Stress Coping Mechanisms: A Quantitative ABCD Analysis. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 6(2), 268-291.
- [203]. Prabhu, N., & Aithal, P. S. (2023). Quantitative ABCD Analysis of Green Banking Practices and its Impact on Using Green Banking Products. *International Journal of Applied Engineering and Management Letters (IAEML)*, 7(1), 28-66.
- [204]. Raj, K., & Aithal, P. S. (2022). Assessing the Attractiveness & Feasibility of doing Business in the BoP Market—A Mixed Method Approach using ABCD Analysis Technique. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 6(2), 117-145.
- [205]. Frederick, D. P., & Salins, M. (2022). Quantitative ABCD Analysis of Online Shopping. *International Journal of Applied Engineering and Management Letters (IAEML)*, 6(1), 313-329.
- [206]. Nayak, P., & Kayarkatte, N. (2022). Education for Corporate Sustainability Disclosures by Higher Educational Institutions—A Quantitative ABCD Analysis. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 7(1), 465-483.
- [207]. Nandini Prabhu, G., (2023). Quantitative ABCD Analysis of Integrating Corporate Social Responsibilities with Green Banking Practices by Banks from Customers' Attraction and Retention Perspectives in Selected Indian Banks. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(2), 1-37.
- [208]. Madhura, K., & Panakaje, N., (2023). The Power of Social Media on Online Buying Behaviour of the Fashion Products: A Quantitative ABCD Analysis. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(3), 90-118.
- [209]. Namreen Asif, V. A., & Ramesh Pai (2023). A Quantitative ABCD Analysis of Coffee Industry Stakeholders. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(3), 287-313.

- [210]. Aithal P. S, Shailashree V. T., Suresh Kumar P. M., (2015a) "A New ABCD Technique to Analyze Business Models & Concepts", *International Journal of Management, IT and Engineering*, 5 (4), pp 409 - 423.
- [211]. Aithal P. S. & Suresh Kumar P. M., (2015b) Black Ocean Strategy - A Probe into a New type of Strategy used for Organizational Success, *GE International Journal of Management Research*, 3 (8), pp. 45 - 65.
- [212]. Aithal P. S., Shailashree V.T., & Suresh Kumar P.M., (2015c) Application of ABCD Analysis Model for Black Ocean Strategy, *International Journal of Applied Research*, 1 (10) pp 331 – 337.
- [213]. Aithal P. S., Shailashree V.T., & Suresh Kumar P. M., (2015d) ABCD analysis of NAAC Accreditation System, Submitted to *International Journal of Management, IT and Engineering*, 2015.
- [214]. Aithal P. S. & Suresh Kumar P. M., (2015e) Enhancement of Graduate attributes in Higher Education Institutions through Stage Models, IMPACT: *International Journal of Research in Business Management*, 3 (3) pp 121 – 130.
- [215]. Aithal P. S., Shailashree V. T., & Suresh Kumar P. M., (2015f) ABCD analysis of Stage Model in Higher Education, Communicated to *International Journal of Management, IT and Engineering*, 2015.

LIST OF JOURNAL PUBLICATIONS

1. Prabhu, Sangeetha, & Bhat, Subramanya (2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(2), 40-64.
2. Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 149-159. DOI: <https://doi.org/10.5281/zenodo.6349848>
3. Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with Bait Based Approach for Mitigation. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 243-258. DOI: <https://doi.org/10.5281/zenodo.6530129>
4. Sangeetha Prabhu, & Nethravathi, P. S., (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 176-183. DOI: <https://doi.org/10.5281/zenodo.6350841>
5. Prabhu, S., PS, N., Spulbar, C., & Birau, F. R. (2022). Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation. *Annals of the University of Craiova, Mathematics and Computer Science Series*, 49(1), 174-182.
6. Prabhu, Sangeetha, & Nethravathi, P. S., (2023). ABCD Analysis of Cyber Attack Detection and Mitigation Model. *International Journal of Engineering & Scientific Research*, 11(10), 7-15.

Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature

Sangeetha Prabhu¹ & Subramanya Bhat²

¹Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India

²College of Computer Science and Information Science, Srinivas University, Mangalore, India

E-mail: sangeethaprabhu96@gmail.com

Area of the Paper: Information Technology.

Type of the Paper: Review Paper.

Type of Review: Peer Reviewed as per [C|O|P|E|](#) guidance.

Indexed In: OpenAIRE.

DOI: <http://doi.org/10.5281/>

Google Scholar Citation: [IJCSBE](#).

How to Cite this Paper:

Prabhu, Sangeetha, & Bhat, Subramanya (2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(2), 40-64.

DOI: <http://doi.org/10.5281/>

International Journal of Case Studies in Business, IT and Education (IJCSBE)

A Refereed International Journal of Srinivas University, India.

© With Authors.



This work is licensed under a [Creative Commons Attribution Non-Commercial 4.0 International License](#) subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature

Sangeetha Prabhu¹ & Subramanya Bhat²

¹Research Scholar, College of Computer Science and Information Science, Srinivas
University, Mangalore, India

²College of Computer Science and Information Science, Srinivas University, Mangalore,
India

E-mail: sangeethaprabhu96@gmail.com

ABSTRACT

Cyber-attacks are becoming more common and over the last decade, many attacks have made top news, targeting manufacturing firms and governmental organisations. Such attacks have triggered substantial financial damage and they've been trying to obstruct key public sector operations. Furthermore, as the Internet of Things (IoT) has arisen, the number of Internet-connected devices is increasingly growing and being an easy target of cyber-attacks. To counter cyber-attacks, information security researchers rely extensively on intrusion detection systems (IDSs) that can identify suspicious activities by comparing patterns of documented attacks or detecting anomaly-based activities. This survey aims to tackle Trust, Protection, identification and activity on wide scale networks and Internet of Things. The proposed research aims at developing a practically deployable cyber security solution to one or more of the cyber-attacks. Multi-Stage Attacks (MSAs), APT, DoS attacks, wireless injection attacks, botnets or other malicious activities will be investigated. In this literature survey, we are highlighting the work Performed throughout the area of cyber security by various researchers, various types of cyber-attacks and its stages, various approaches to prevent cyber-attacks, different challenges faced by a preventer, and some gaps in the research. This literature review is carried out by using the secondary data obtained from peer-reviewed journals and other sources on the web. This review aims to explain Detecting Malicious Activities in Network Traffic.

Keywords: Cyber Security, Mitigation, Internet of Things, Machine Learning, Malicious Activities.

1. INTRODUCTON :

We're never going to envisage the world without the Internet at present. In every commercial enterprise, research institutes, academic institutions, economy, defence, businesses, etc., all are purposely or inadvertently focused on the Internet. In government bodies, services are delivered via the internet to any individual person in the country, as rural areas cannot operate offices for all government plans. Via these services, people are thus related to the Internet. Digital retail has become one of the decade's largest growing sectors, with customers ordering items online and selling and purchasing products from regular foodstuffs to heavy and costly appliances on the Internet (Verma et al., 2015) [1]. Online retail has now seen a huge rise in online money transfer, with internet banking, cash deposits and additional bills being paid to them. The Web continues to endure this period on a regular basis and keeping it seamless and safe is among the most appropriate methods for educational organizations.

Cyber Security can be an option characterized as the protection of virtual space systems, data and networks. This applies to the techniques used for preventing information from being stolen, compromised or targeted. Because of heavy dependency on computers in a capitalist world industry that stores and transmits an abundance of people's sensitive and vital information, cyber protection is a critical feature and many companies need insurance. We live in a digital age that recognizes how insecure our personal data is than ever before. We all live in a networked environment, from internet

banking to government infrastructure, where information is stored on computers and other devices (Buczak, Anna L. Guven, 2016) [2]. A part of the data may be sensitive information, whether it involves intellectual property, personal information, financial data or other types of data for which unauthorized entry or disclosure can have negative consequences. Cyber-attack is now an international problem and has raised many fears that hacks and other security assaults could place the global economy in danger. The organization transmits sensitive data across networks and to other devices throughout the course of business operations, and cyber security determines the information and the methods used to process or store it to secure it. Since a case of cyber strikes increases, businesses and organizations need to take measures to protect their confidential business and personal information, particularly those that deal with information related to national security, financial records or health.

Cyber security is a complex problem that involves multi-dimensional, multi-layered interventions and responses across several domains (Hoque, Sazzadul Mukit, 2012) [3]. This has proven a problem for governments as it includes numerous departments and ministries. It is more complicated because of the stable and the positive varied nature of the risks and the failure to devise an appropriate solution in the lack of particular measure perpetrators. Thanks to the rapid growth of information technology (IT) and related commercial applications, Cyberspace has grown significantly in its short lifetime. Advances in information and communications technology have revolutionized government-developed science, educational, and commercial infrastructures (Roopak et al., 2019) [4]. IT services is an important part of core services supporting national resources such as electricity, telecommunications, defence systems, emergency communication systems, power grids, space, financial systems, land records, transportation, law enforcement, security and air traffic control networks, basic public services and utilities, to name just a few. Both of these infrastructures are increasingly dependent on data relays for communication and business transactions. The operational stability and safety of critical information infrastructure is vital to the country's economic security (B, 2014) [5]. More problems are raised by the changing design of the telecommunications network. The extension of wireless connectivity to individual computers and networks is making it increasingly difficult to establish physical and logical network boundaries. The risks are introduced by growing interconnectivity and accessibility to computer-based systems which are central to the economy of the country.

Interconnectedness has become key to branches of government, education, essential infrastructure and culture. Various sensitive regional, public, private, and military infrastructural facilities may be susceptible to attacks as they still rely on outdated traditional approaches to security rather than sophisticated, robust, cyber defence (Seissa et al., 2017) [6]. Cybercrimes, cyber attacks and cyber terrorism are indeed concerns that govern data security. Cyber terrorism and traditional terrorism share several main features, and a similar aim called terrorism. Cyber terrorism, however, continues to be a significant phenomenon and a lot of discussion about its exact sense, goals, attributes, risk factors and protective methods. Cyber terrorism and cybercrime are sometimes used synonymously, or cyber terrorism may be used to cover cyber-terrorism, blurring the difference among them, notably for the wider populace (Seissa et al., 2017) [6]. Cyber attacks continue to be listed as one of the highest priority global threats to national security. Cyber-attack, whether it happens as a confrontation between nations, as a terrorist or as a criminal act, is an attack in cyberspace aimed at breaching a computer system or network but also at breaching physical systems as was the case with the Stuxnet worm. In both terrorist and military purposes, the same tactics of a hacker attack are implemented. (Duic et al., 2017) [7] break cyber-attacks into phases which they find to be basically the same as traditional criminal offense phases:

1. The very first phase of an attack is to search potential victims. By monitoring the execution of normal target operations, valuable knowledge that is collected and calculated through the applications and hardware used;
2. The second stage of the assault is one of intrusion. There isn't anything that can be done against the target before the attacker gets into the network apart from preventing the availability or connections to those services offered by the target;
3. The next move is to describe and disseminating internal incentives by an overview of the tools and the right of access to the system's restricted and essential parts;
4. The intruder does system damage in the fourth phase or steals certain data;

In addition, they suggest that cyber attacks today mainly consist of:

1. Malware via internet browser attachments, e-mail or other vulnerabilities of the system;
2. DoS to restrict the usage of computers and networking systems;
3. Deletion or transfer (leaving a message) for propaganda purposes to government and commercial websites or to interrupt the informing;
4. Unauthorized intrusion into networks for theft of sensitive and/or proprietary information, Misuse of information collected/use of channel to start attacks on other networks.

Cyber risks definitely redefine such words under these transformational conditions and contrasting perceptions and understandings of security in general and international security. A new global The information security ideology will have to be built in line with the proposals to boost security on the one side, and the existence of cyber threats and motives of actors who initiate them on the other side (Durand & Wegener, 2020) [8].

More than 80 percent of total trading transactions are conducted online today, and this sector has demanded a high level of protection for open and best transactions. The scope of Cyber Security not only extends to the security of enterprise-wide IT systems, yet even to the bigger digital networks they depend on, including cyber space itself and critical infrastructures (M. Wu et al., 2017) [9]. Cyber security plays a major role both in IT development and Internet services. Improving cyber security and securing sensitive information infrastructures are crucial to the protection and economic well-being of each country. Society has become dependent on cyber systems across the entire spectrum of human activities, including trade, banking, energy, health care, communications, entertainment, and national security (H. T. Nguyen & Franke, 2012) [10]. Recent research results also show that the degree of worldwide awareness since 2006 for data security and personal information has increased. Internet viewers are scared of giving away plenty of personal information and prefer to be resisted because there is no real need to maintain their personal information. Cyber security depends on the precautions conservatives take and make important decisions on the choices they make when setting up, maintaining & using the machines and the Internet. Cyber-security includes physical defence of personal information and technology tools (both hardware and software) from unauthorized access obtained by technical means. Albert Einstein was quoted as saying-Problems with the same degree of consciousness that produced them cannot be solved (Zamani, Mahdi Movahedi, 2015) [11]. The issue of end-user errors cannot be solved by incorporating more technology; it must be solved with a concerted initiative and collaboration between the group of interest in information technology as well as the general business community along with vital support from top management.

2. OVERVIEW OF CYBER ATTACKS :

Cyber security is a rapidly growing field that needs a lot of attention due to remarkable developments in IoT networks, cloud and web technology, mobile world, online banking, smart grid, etc. Cloud is becoming more appealing to hackers due to its open nature and the quantity of traffic created by the cloud. For example, the most prevalent cybercrime attacks after data theft are distributed denial of service (DDoS) attacks. TCP and/or UDP flood attacks can drain cloud resources, absorb much of their bandwidth, and damage a complete cloud project in a short time (Hoque, Sazzadul Mukit, 2012) [3]. These security threats include the creation and deployment of an efficient intrusion program that will protect the cloud from zero-day attacks that have just arisen. The most common challenges traditional methods face is that IDS generates false alarms and does not use appropriate standards or parameters to assess threats. This may contribute to the problem of misuse.

Faster transition of data made the network an Interesting and allow access goal for attackers to hack and play with different kinds of attacks. Consequently, many intrusion detection strategies have developed to secure distributed services in the cloud by detecting the various forms of attack on the network (G. Kim et al., 2014) [12]. The big benefit for the population of attackers today is the availability of open access to infrastructure and broad file and knowledge sharing networks. And so, each other day they prepare more and more new kinds of attacks. Software manufacturers who don't pay enough attention to their security modules create vulnerabilities not just to their device but also to the overall system and often become vulnerable to one malicious application for the entire network(Borkar et al., 2018) [13].

3. RESEARCH OBJECTIVE AND METHODOLOGY :

Cyber Security ensures the confidentiality of computer-connected systems, software, hardware and information from cyber attacks. Without a protection policy in line, attacker can easily access your system and misuse your private information, customer data, business intelligence and much more. This analysis is being carried out with the aim of properly understanding the definition of cybercrime and cyber protection and of providing effective and appropriate remedies to address these concerns in today's Internet world. In addition to this, the purpose of the study is to provide a framework for new opportunities for analysis. The following tools are important for the achievement of the desired objective:

1. What are the different types of cyber attacks?
2. What are the various aspects of a targeted cyber attack?
3. What are the various perspectives to Cyber Attack Detection?
4. What are the theoretical constructs of the Cyber Security System?
5. What are the different approaches to predict and avoid network attacks using machine learning algorithms?
6. What are the specific issues of a developer to mitigate cyber attacks?
7. What are the benefits of avoiding cyber-attacks?
8. What are the various works done in the field of cyber security in order to prevent cyber attacks?

4. LITERATURE REVIEW :

There have been a large number of studies in the literature on the issue of cyber security. For general information security strategies, there are diverse common approaches. We've concentrated on using artificial intelligence and machine learning approaches to cyber security issues in this segment.

(Chowdhury et al., 2017) [14] suggested a new method of botnet detection, node-based topology within a network. The technique suggested would be able to detect anomaly by looking for a small number of nodes. This methodology is based on a clustering of self-organizing maps (SOM), which is part of a family of unsupervised system. This analysis used CTU-13 databases, the largest dataset containing nodes labelled with bot. This analysis also used another detection algorithm, supporting the vector machine (SVM), for comparison.

(Neethu B, 2014) [5] Represents PCA architecture for the Naive Bayes collection of features to build a network intrusion detection program. KDDCup 1999 benchmark data collection for intrusion detection is chosen for experiments in this study. The findings demonstrate that the technique efficiency achieves a higher detection rate, less time consuming and has a low cost factor compared to the approach focused on neural network and tree algorithms. Moreover, the proposed program has an accuracy of around 94 per cent.

(Kozik et al., 2014) [15] Proposed a new method for identification web applications targeting cyber-attacks. This The strategy was related to the machine-learning algorithms Naive Bayes, AdaBoost, Part, and J48. Additionally, HTTP Dataset from CSIC 2010 is used to test the proposed model. The study focused specifically on solutions which use HTTP protocols to communicate with servers clients. The authors believed this model could get the higher percentage of detection while getting lower false positive rate. At the same time, the findings have shown that the J48 strategy is the best solution to this problem and about 0.04 is the true-positive value.

(Zamani, Mahdi Movahedi, 2015) [11] reflect different intrusion detection models. These models are divided in this analysis on the basis of classical artificial intelligence (AI) and computational intelligence (CI) such as genetic algorithms and fuzzy logic. They performed various experiments, and compared the efficiency of their algorithms. The findings of the experiment suggest that best results were obtained with decision tree algorithm.

(Hoque, SazzadulMukit, 2012) [3] developed a genetic-algorithm-based intrusion detection system (IDS) to accurately detect various types of network intrusion. The proposed model used knowledge evolution theory for filtering the traffic data and thus decreasing the complexity. Alternatively, the KDD99 benchmark dataset was used to test model performance. The experimental results indicate that a fair detection rate has been achieved for this model.

In order to detect the presence of a botnet and identify the bots, (J. Wang & Paschalidis, 2017) [16] suggested a novel approach with two phases. First stage is relevant to the awareness of anomalies by leveraging large differences in an empirical distribution. Additionally, this stage proposes two

Strategies for the creation of empirical distribution. First methodology is flow-based method that estimates the histogram of quantized flows and the latter is a graph-based method that estimates the grade distribution of graphs of node interaction. Second stage uses social network culture in a graph to detect the bots, capturing associations of interactions between nodes over time. They used real-world botnet traffic for the experiments which is a CTU-13 dataset.

(Wijesinghe et al., 2015) [17] concentrate on the identification by examining network traffic flows of a number of families in the botnet. Their method proposed It's in two pieces. Firstly, they identify appropriate dataset models with more specific features to detect botnet from IP flows. Second part used IP flow data to detect unlabeled botnet behaviours. They used publicly accessible IPFIX dataset in this analysis. This technique is a new concept, and has led to botnet detection studies based on IP flow data. (Haddadi, Fariba Cong, 2015) [18] evaluated various approaches to botnet identification, depending on the model used and the type of data used. Bot Hunter and Snort are two methods focused on public-rule schemes. Other methods are based on Data processing methods, including packet payload and traffic Flow-based strategies. This analysis makes use of five botnet data sets accessible to overall public, such as CAIDA, ISOT etc. Several experiments were conducted using C4.5, KNN (k-nearest neighbours), SVM, and Bayesian networks. Experimental findings indicate flow-based system performance is higher or comparable to the findings published in the literature.

4.1 TYPES OF CYBER ATTACKS

It is necessary to declare this tenderness of virtual vulnerability as the evil result of this rapid leap in technological competence that usually defines this age. This lack in prudent security features that can be described as the debauch misuse of this inherent vulnerability is abused by hackers and some other cyber intrusion. You can illustrate the various types of cyber threats as follows:

1. **Malware** - Malware can be described as a coordinated convergence of cyber and virtual threats of various kinds, and typically consists of Trojan and other similar viruses(Akin et al., 2020)[19]. It can be illustrated as the systematically designed instruction code that usually comes up with the rogue intent to hack the confidential information in the immune set. This also holds the power to demolish the entire collection of knowledge. Malwares typically appear in the virtual scenario coupled with the attachments containing malicious emails, and the consequent download of the attached links that herald vulnerability-related issues.
2. **Phishing attacks** - These assailant kinds typically ask a foreign agent for a reliable metric of information. In addition, often it comes with a request to register in a given connection that was endowed with the previous attachment. On that topic, what can be seen as an efficient index of Virtual intrusion seems to be some of the attachments request personal and sensitive data. In the past few days, this program has developed into a more advanced and elegant version where it allows users to switch to a third interface and eternal intrusions allow them to steal the knowledge accessible from foreign servers and users (Zhang,Ningxia Yuan, 2012) [20]. So, managing their malicious intent has become really simple and useful for the hacker.
3. **Password attacks** - Generally this kind of attacks are characterized by the intruder's intent to break the user's enforced password by merely initiating access to the user's device. Generally, this kind of attacker doesn't add some kind of debauch instructions and malicious codes. In addition, it does not misuse any tools to achieve its goals. In this case, a specific program is typically implemented that violates the prey user's password in a stably guided manner. It normally breaks a user's system's enforced password. There are certain specific program-related applications which possess the ability to initiate brute force attack. This form of program is typically developed and commissioned to crack the target user's password.
4. **DoS Attacks** - Typically, this sort of assailants imparts vehemence to chaos the ideals of a specific Network. In background, the approach by which DoS attacks are inflicted is unique in application since the intruders transmit a deep volume of network signal (Kato & Klyuev, 2014) [21]. This aids congestion network traffic by overloading this. These forms of threats are considerably the most common form of cyber threats as it indulges the user in overcoming the network blockage imposed by the virtual intruder and meanwhile the hacker uses multiple networks to gain access to the preserved information.

5. **MITM attack** - MITM stands for Man in the Middle where the attacker is intending to impersonate the various end nodes within a common service interface and information sharing. These forms of attacks are typically defined and interpreted throughout the Banking sector and financial industries, and are likely to target the online transaction interface. Usually, such attacks earned it access via a non-illusive wireless access node. Since they enjoy this app interchange facility, they have enabled access to all the related metrics of user-owned knowledge.
6. **Malvertising** - In such an attack, the automated attacker pressures the user to compromise with the fixed workstations while adding multiple criminal intent instructions. This malice is likely to occur if the user is prompted to access any questionable advertising index. These were a common practice for potential intruders to upload questionable and malicious material into the celestial system to confuse users and contaminate their collection of information at the same time. Clicking on the infectious connection will move the user to a different third-party interface and grab the confidential text (R. Islam & Abawajy, 2013) [22]. It can be described as a virtual hijack mechanism and the stolen information as a ransom to achieve the cyber security necessary
7. **Eavesdropping** - This can be proven as a virtual overhearing environment where the possible attacker is vulnerable to secretly listening to other private exchanges. This is usually practised among a particular network's diverse and shared hosts. This is not the serious kind of virtual hazard and can be solved by following a few simple acts.
8. **Click jacking** - This kind of assailants typically target the user's normally used virtual interface by simply using some celestial malicious instructions in the form of cryptic codes (Smadi et al., 2015) [23]. Deep down, this process is generally described as a cheap trick from the website of the hacker that makes inexpensive use of tricks and makes the user Click the button with apprehension. To redirect the respective user to another web page, this button is further conditioned. This sort of intruder can also be described as the possible hijackers who are vulnerable to stealing any valuable information from the user's network.

4.2 STAGES OF CYBER-ATTACK

Aimed cyber attacks have no specific pattern of intervention, and therefore there is no chain of events that is absolutely accurate. An assault may be a one-time incident that lasts for minutes, or a segment of ongoing intrusions that extend weeks or even years, taking into account several technological and individual vulnerabilities, like unpatched websites that involuntarily trigger malware downloads, code-injection web servers or browsers that are susceptible to downloading malware-infested mail attachments. Overall, contemplating a targeted phase cyber intrusion is helpful. The targeted attacks occur across several phases:

1. **Reconnaissance** - In the early phase of an attack, an attacker makes use of social manipulation and passivity, Email Phishing, developing a waterhole or perverting removable media to gather information and learn its meaning. The hacker resumes by searching for open-source government or corporate content, scanning, gathering data about targeted networks, their operations, critical staff and targeted mail addresses (Smadi et al., 2015) [23]. To detect vulnerabilities that need to be exploited, the attacker(s) invest some time cataloguing everything they discover to obtain profound insight into what is currently being utilized against the security features of database and the learning system.
2. **Scanning** – The next step will proceed for the hacker to find a low entry point that allows network connectivity; may this be poor judgement, restricted device utilization, perception management victims, lack of security strategy or ignorance. The intruder stealthily combines in with normal traffic if a network is infected within the network, making identification increasingly hard. The attacker then starts by covertly implementing their cyber tools to isolate weaknesses in the protection within critical network connections (Duic et al., 2017) [7]. The tracking system will search the systems probing area, searching for weaknesses to generate a server elevation cyber graph. This may be the move be done via resources that can be found conveniently across the network. Searching for weaknesses is typically a long process and, regardless of how big the network is, it can take months.
3. **Arbitrary code execution** – Malicious actors may remotely build unauthorized network adapters or configuration issues on your device to install malicious programs such as Remote Access Trojans

(RAT), root kits, and insert keystroke authentication software to acquire credentials for higher authorized access on the network, and also get passwords that will allow them to access all areas of the device. The intruder begins expanding after obtaining a set of appropriate systems on the preservation of the impact.

4. **Access and Escalation** – Now as the hacker has attained unrestricted control of the target system, they may try to push for lateral expansion and establish a strong presence. Many attackers hide in the Network's darkest regions, and stay inactive as they try to come and go. Some will choose to buckle across the network and identify the important parts they are hunting for genuine to accomplish their goal, such as sensitive information, private information, property rights or computer communications mechanisms that degrade or disrupt network activity at will.
5. **Data Collection, Exfiltration, and Exploitation** - The reputation of the network has been greatly undermined by this point. Once an intruder thinks they have gained safe access to the system, they can now alter or transfer confidential data to any spot they wish. The attacker may use or leak the stolen data with third parties or even the Internet for more targeted hackers (Zahid et al., 2020) [24]. The ultimate goal of their mission is achieved and it is typically too hard for the breached enterprise to defend itself by this time.
6. **Clean up** – Not all attackers take the final step, some merely detach, and unworried about the victim possibly finding out just what happened or choosing to leave underneath a calling card to make a fuss about their achievement. Highly qualified attackers attempt to remove any forensic evidence that suggests a violation in all network systems (Seissa et al., 2017) [6]. They can erase / overwrite documents, erase embedded data, clear log files, disable alarms, roll back up software upgrades, unplug backups or erase hard disks. They would do their utmost to mask or delete any signs that the accident has ever happened, making it appear as a code error left behind secret backdoors anywhere they want to go back to, or breaching the systems further.

4.3 ARCHITECTURE OF CYBER ATTACK DETECTION SYSTEM

Safety is a necessary aspect of rising network infrastructure nowadays by increasing network systems. Network IDS provide a defence model for all hazardous security threats to any network (Aburrous et al., 2010) [25]. The IDS could detect and block network traffic relevant to the attack. Control of network is a complex model. Implementing IDS may cause network delays. Many network IDS centred on software are being developed. Yet the model has a high-speed traffic problem. Application architecture offers an overview of software modules, relation between each component and software application high-level design (Zamani, Mahdi Movahedi, 2015) [11]. Although these systems are very different in the techniques that each system implements, they also gather information and analyze it. The majority of these systems rely on the infrastructure of popular architecture (as shown in figure 1). The following fundamental architectural components are as outlined below (Axelsson, 2015) [26]:-

1. The processing of data is responsible for gathering information from the grid as well as the machines being tested.
2. Detector ID algorithm builds sensor information to detect suspicious attack incidents.
3. Knowledge base contains information obtained by sensors; this is accomplished by structured input, input profiles, etc. in pre-processed format. A security expert or network expert often delivers that data.
4. Configuration device provides the latest Intrusion Detection Systems status data.
5. The solution part starts with a discovery of an attack. These responses could be programmed either as active or may include a human interaction also called inactive.

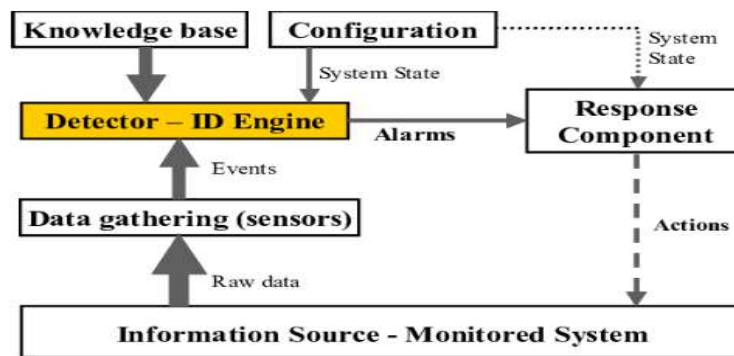


Fig. 1: Shows a popular Intrusion Detection Device design structure (Axelsson, 2015) [26].

4.4 APPROACHES FOR ATTACK DETECTION

Machine learning and evolutionary algorithms can typically be used to identify and forecast attacks, as well as statistical methods and correlation rules. Similarly, most solutions to mitigation of attacks are done by the study of traffic to detect and drop (or block) a malicious operation (Ibor et al., 2018) [27]. That is shown in Figure 2.

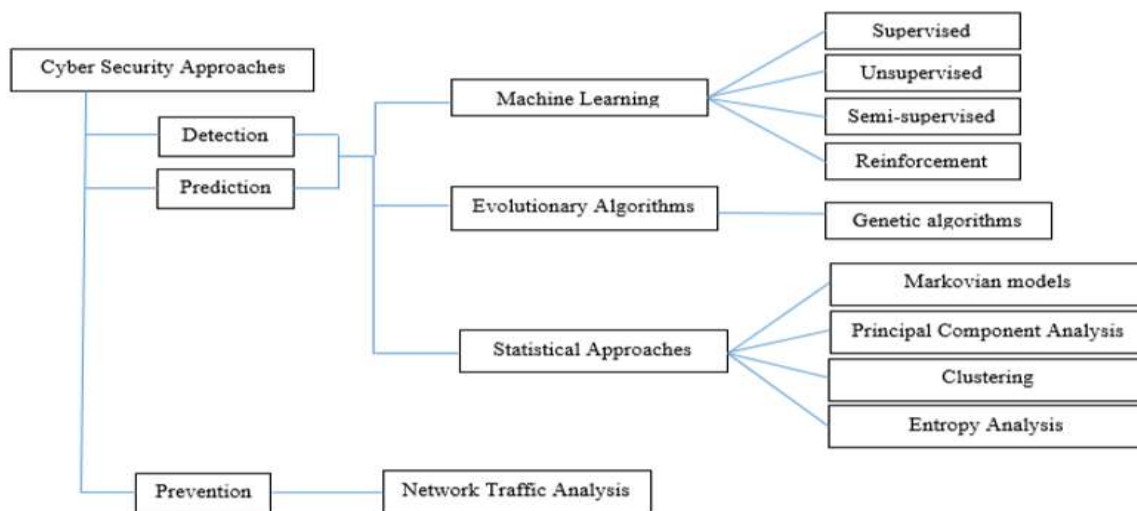


Fig. 2: Summary of Cyber Security Approaches (Ibor et al., 2018) [27].

Detection of cyber-attacks is a growing strategy for preventing a threat. To announce the presence of an attack pattern or profile in a network, it includes reacting to an unexpected contact. Intrusion prevention is one of the core techniques for identifying cyber-attacks. Intruder detection is, according to (Aissa & Guerroumi, 2016) [28], the method of detecting an intruder or an characteristic attack in a continuous flow of connections. Detection of intrusion occurs with the use of intrusion detection systems.

Systems for detecting intrusion are divided into three strategies. These include approaches to abuse (signature-based), anomaly, and hybrid detection, respectively. Although identification of abuse utilizes the signatures of documented attacks to help identify intrusions, identification of anomalies uses profiles of regular network behaviour to report intrusions when a change from the usual profile is detected. Combining the two approaches produces a hybrid approach (G. Kim et al., 2014) [12].

Several studies are published in public view about cyber-attack identification. Some of these methods, though, have been relatively ineffective in identifying attacks although others have resulted in high computational resources usage. Likewise, much of the methods proposed in the current literature are computationally infeasible and can only survive as masterpieces of science. Subsequent articles will address more public domain solutions to cyber-attack identification, as well as demonstrate the technique, strengths and limitations of each strategy.

4.4.1 DETECTION BY MACHINE LEARNING APPROACH

Machine learning methods have been introduced in recent decades become common in detecting cyber-attacks. Machine learning is especially efficient in evaluating data and predicting the outcome of such events based on the sample inputs available which are used to create an acceptable model for making the right decisions. The key tasks of machine learning algorithms are to use training data to identify and predict the existence or absence of an acquired case (Azab et al., 2016) [29]. The use of machine learning in the latest prevention of cyber-attacks environment has helped boost the method of identification to a strong stage of precision. In this paper four kinds of machine learning techniques are discussed. These include methods of controlled, unmonitored, semi-supervised and validated instruction.

4.4.1.1 SUPERVISED LEARNING APPROACH:

Supervised learning is a component of pattern recognition that uses a collection of named instances known to be training data with the target output correspondingly. A statistic system for categorizing new data sources throughout the training phase is generated from the named instances. This is done through injecting a certain machine-learning algorithm into the named instances. Some of these approaches to machine learning as illustrated in (Buczak, Anna L. Guven, 2016) [2] include decision trees such as C4.5 and ID3 algorithms, Artificial Neural Network, Hidden Markov Model (HMM), Support Vector Machine (SVM), K-Nearest Neighbour (KNN), and Naïve Bayes.

Web pages are one part of cyberspace that's vulnerable to malicious attacks. With an ever-expanding web footprint in all application types, with the increasing use of web pages material for practices such as social media communications, online banking, e-commerce, e-government, and many others, the need for an efficient approach to identifying fraudulent web pages cannot be overemphasized.

The ability to quickly alter the source code of web pages by adding malicious code as observed today that contributed to a different category of malicious websites that could intensify the environment of assault and mislead users into revealing sensitive personal data. To this end, (Huseynov et al., 2014) [30] Drew up a digital approach for the identification of fake web sites which use methods to abuse and analysis of anomalies. The hybrid malicious web page detection technique hierarchically combines the violation and identification of anomalies modules so that abuse detected module analyzes every web page at first instance. This system often makes use of the algorithm of the decision tree to identify misleading web sites by contrast the properties of those Pages of established trends on web page. When the first stage is complete, the unclassified pages are fed into the anomaly detection system to detect new instances of malicious pages with the aid of one-class SVM.

With the integrated solution focused on the use of both the intrusion and anomaly detection Ways of preventing network threats, efficiency was strengthened with a decrease in time complexity, resulting in a higher identification accuracy of up to 98.2% and low level of false warning of 1.7%. In this case, the using algorithm for decision tree for forecasting instances comes with its own drawbacks. Decision trees may be unreliable if the exact information is not used, and as such a small shift in the input data may result in major tree changes. It is not suitable for identifying intrusions as the resulting diagnosis may be completely inaccurate with disastrous implications for vital network infrastructure. A 3-step method is laid out in (Lin et al., 2015) [31] for the realization of a novel feature representation strategy based on CANN approaches. This method incorporates two estimated and combined distances, which represent the distance between the database and cluster core in the first case, while the second range in same class is determined in terms of the data point and its closest neighbours.

Using the classifier k-Nearest Neighbour (kNN), the resulting one-dimensional distance-based feature It used for presentation each data point throughout the sample field chosen to achieve attack detection. A clustering algorithm is used initial state to remove cluster centres, and the number of training samples from testing set is indeed a feature of a group number. In the second level, A new feature on component is generated to represent a data point by calculating and summing the distances in two dimensions viz-a-viz between the data points in the dataset and the cluster centres, as well as an individual data point in a related cluster and its closest neighbours. Finally, to devise new data is the retrieval of cluster centres and closest neighbours. The k-NN classifier is learned and evaluated using the combination of assessments and advanced training sets to find new and unknown instances even in string connection. It's been observed in experiment that the CANN solution was efficient with respect to k-NN and SVM classifiers with respect to the six-dimensional data set used, and demonstrated substantially high detection precision with a marginal false positive rate (Bhamare et al., 2017) [32]. Conversely, by

evaluating the nineteen dimensions dataset, CANN obtained the same success levels as the k-NN and SVM classifiers. Some of the shortcomings found in the system includes CANN's failure to identify root (u2r) applications, and root to local (r2l) attacks. This may not be unconnected for use of one-dimensional distance-based feature representation to develop and evaluate the framework which will essentially detect the various attack classes. In doing so, the function space is believed not to exhaustively represent the patterns of u2r and r2l attacks. A multiple learning strategy that considers the cluster centre and nearest neighbour approach (CANN) to be enhanced as described in (Lin et al., 2015) [31] is further elaborated in (Shapoorifard & Shamsinejad, 2017) [33]. The technique, dubbed ICANN, deploys two supervised algorithms for machine learning, that is, the classification algorithm k-Means and the algorithm k-Nearest Neighbour.

4.4.1.2 UNSUPERVISED LEARNING APPROACH

Unsupervised learning operates by finding trends used as the training data in an unlabeled dataset to make the correct classification a collection of decisions in different cases. This typically includes clustering to classify the groups that instances belong to. (Song et al., 2013) [34] addressed an anomaly detecting method with an unsupervised learning approach that is capable of dynamically tuning and maximizing the value of parameters to arrive at better categorized instances that either represents an attack string or a usual link. The proposed approach implements after-the-training sorting of cases, which involves such phrases as sampling, clustering, and modelling. Filtering achieves the necessary normal data sub-set, which is then partitioned into clusters k. Such k clusters reflect standard traffic data patterns, such as HTTP, FTP, and SMTP. The one class SVM is used for the generation of k SVM models also called k hyper spheres for classification for each regular cluster (Zarca et al., 2020) [35]. k model is then paired with new instances to decide whether such an existing case inside the predefined hyper sphere, in which case it is a natural relation, then the state of attack is flagged up.

Usage of unsupervised way of learning offers an efficient strategy for classifying new instances using the threshold at the time of model building to distinguish normal and attack results. A major downside of the strategy can be clearly established at this point, based on the assumption that typical links differ on heterogeneous networks, and as such building profiles of normal activity will dramatically deteriorate. This major variation in one network's behavioural patterns and characteristics from other networks will result in an inconsistent model that will inevitably require an effective assessment of the tuning parameters and adaptation to satisfy the needs of a given network setting. A fixed-width clustering algorithm generates clusters in function space at the point of training the construct. Anomalous clusters are known if there are fewer training traffic samples than a given threshold on these samples. In comparison, in the testing stage, matching a specific traffic sample to a cluster processing is carried out to confirm an anomalous trend of life or not (Ravikumar & Govindarasu, 2020) [36]. The major downside to this approach is the intense demands for computing sensor nodes that can contribute to large overheads on host network.

4.4.1.3 SEMI-SUPERVISED LEARNING APPROACH

(Ashfaq et al., 2017) [37] suggest that semi-supervised learning takes into account all labelled and unlabeled samples for a proper classification. Similarly, (Aissa & Guerroumi, 2016) [28] states that using a pre-labelled sample, semi-supervised machine learning methods models human behaviour. Semi-supervised learning then incorporates the influence of both supervised and unsupervised in-process of learning methods of creating a model for classification of new instances of a dataset. Additionally, (Aissa & Guerroumi, 2016) [28] suggested a two-stage semi-supervised computational method for identifying abnormalities in the network. The methodology uses prelabelled typical instances to construct a probabilistic model. The formula is then used using a fixed criterion to measure variance from normal behaviour. The second stage uses an iterative method to reduce the false rate, which boosts the resemblance gap and dispersion rate of the probabilistic model's initial classifications (Aissa & Guerroumi, 2016) [28]. (Han et al., 2016) [38] suggested a semi-supervised learning approach in cloud-based systems as a countermeasure for co-resident attacks. The remedy has established a framework for defence which makes it computationally costly for co-resident intrusion is being successful on a virtual environment with a cloud computing environment. The problem was modelled with users categorized using clustering analysis and semi-supervised SVMs as a 2-player safety game (Xie et al., 2014) [39]. Users are regarded in accordance with the adjustment in the method of virtual machine allocation as high risk (malicious), medium risk (uncertain) and low risk (legal). It helps the

defence system increase the potential cost of an attacker to accomplish a computationally costly method of attack. The method achieved progress by raising the attacker's overall expense to two orders of magnitude as a countermeasure for attacks on co-residence. Nonetheless, in practice it is not easy to have a single datacenter to using the describe method the various situations of multiple datacenters that are likely to accommodate colocation and co-resident attacks.

4.4.1.4 REINFORCEMENT LEARNING APPROACH

Reinforcement learning is a machine learning technique that enables the learning of a software entity like a sensor node by experience with its surroundings. (Alsheikh et al., 2014) [40] claims that trying to improve learning is key in the sense of pattern recognition since it makes software agents to construct experiences from their encounters with the world in order to take the right long-term rewards behaviour. Similarly, (Xu et al., 2014) [41] stated that reinforcement learning agents transfer messages in an initially unknown context and use the acquired knowledge to redefine policies of action to increase their rewards. The authors suggest that reinforcement learning is appropriate for solving sequential problems that can be modelled as Markov decision processes (MDPs) and as such appropriate for understanding problems with learning power. Supervised learning algorithms typically find these questions impossible to understand.

(Shamshirband et al., 2014) [42] used Fuzzy Q-learning to detect and avoid WSN intrusions. To predict DDoS attacks, the technique utilizes a mixture of cooperative game theory and fuzzy Q-learning algorithms. For a 3-player strategy game, the solution models sinkholes, a base station and an intruder and the machine is triggered when a torrent of packets is aimed at the target node. At this level, the received packets are calculated against a common alarm event threshold in WSN and the solution applies cooperative security countermeasures for the sink hole and base station if such a threshold is breached. For performance assessment, low-energy adaptive clustering hierarchy (LEACH) was simulated with NS-2 simulator to demonstrate the approach's accuracy in detection and defence. The solution architecture allows the sink hole and base station to react to a random attack while selecting the most appropriate technique to detect and respond. To predict potential attacks, the IDPS amends the learning criteria regularly in a process described as lifetime self-learning of past attacks using fuzzy Q-learning (Xia et al., 2010) [43]. With the method considering DDoS just fights the flooding, its effectiveness against other types of attempts can be hard to find out. The model therefore requires a holistic improvement to effect enhanced decision-making capabilities, particularly with regard to truncating novel attacks.

4.4.2 DETECTION BY GENETIC ALGORITHMS APPROACH

Genetic algorithms (GAs) are a hybrid part of evolutionary algorithms (EAs), effectively meta heuristics described by the natural selection mechanism. A genetic algorithms' most critical role is rooted in generating optimization solutions and searching problems based on such bio-inspired operators as mutation, crossover, and pick. Accordingly, (Hoque, Sazzadul Mukit, 2012) [3] suggested an intrusion prevention method focused predominantly on the use of genetic algorithms. In order to minimize the complexity attributable to classification, the genetic algorithm approach is tuned to detect various forms of attacks based on evolution theory to information evolution with a consequence filtering the captured traffic data. The approach's efficacy was assessed using three variables, which include fitness function, individual representation, and GA parameters. In the proposed solution, two specific functions are applied to attain the purpose of the algorithm. These include the pre-calculation and identification processes. The training data were present in the pre-calculation process to construct a collection of chromosomes and is used in the next shift for comparisons. Detection is accomplished in the second stage by constructing a population to evaluate the method and ultimately the test data is estimated using certain measurement processes such as discovery, convergence, and mutation. A fitness function then determines the fitness of the sample population for every chromosome. Experimental Experiments showed that the approach is worked well against different intrusion types including test, Root to Local (R2L), Denial of Service (DoS) and User to Root (U2R) attacks. Measuring a chromosome's fitness with the standard deviation equation with distance restricted the approach's efficiency with respect to identification and false positive frequency. For this respect the use of a more effective heuristic may be very useful for a better detection method.

(Rastegari et al., 2015) [44] Proposed creating statistical guidelines for identification of attacks. The system relies on necessity to closely examine data about internet traffic in order to directly identify

unwanted traffic using a genetic algorithm due to the similarities between regular and attack patterns. Using statistical continuously valued input data, the algorithm is optimized to develop simple interval dependent laws. Then, each rule is assessed using a fitness function in conjunction with a new individual representation. During the learning process improved rule sets are created in this way. Then, the rules produced are used to identify the data points. The chromosome configuration is formulated according to pattern to follow rules with a mutable feature set and fitness mechanism that is capable of rewarding inter-rule cooperation. This also includes a mechanism to assess the degree of exclusivity at the selection stage in an adaptive manner to generate succinct rule sets. During the pre-processing phase, setting data normalization is done to generate normal and crime records for training and evaluating the emerging rule-based classifier. Pre-processing often calls an optional stage of selection of features that functions to provide seed rules for the initial population of rules. This is accompanied by the assessment step, where a conventional fitness system evaluates component rules while a higher-level system selects rule sets that operate in the detection process together.

One major strength of the proposed approach is the non-dependence of packet header category features like destination and origin IP addresses (Huang & Zhu, 2019) [45]. This means that the method leverages network traffic statistical capabilities to detect any unusual activity present in the traffic stream, and as such is ideal for detecting novel attacks. Similarly, the use of concise rule sets, that are analyzed through the genetic algorithm and identified to comply when specifically covering the quest field, leaves the rule sets small and effective in detecting proven and novel assaults. Considering the number of rule sets included within the regular grouping and attack cases, likewise the metrics of fitness and efficiency, it is important to consider miniature limit values shift. Unfortunately, the current model is oblivious to these improvements because no testing models are nearby making it unable to execute and classify the type of intrusion that infiltrates a network even at this given point in time in a multi-class scenario.

4.5 ADVANTAGES & CHALLENGES OF CYBER ATTACK PREVENTION

As every other living room, the system has its own advantages and challenges. Though it improves the life of a man in almost all ways, be it education, housing, connectivity, smart cities etc. There are different obstacles that we must address so as not to turn technology into our own enemy. Cyber security faces a greater challenge than any other technology continuum. Cyber criminals have also begun to misuse technology-controlled tools to accelerate cyber-crimes like fraud and robbery (S. N. Islam et al., 2018) [46]. With security protocols still being developed and developing driven steadily, these cyber-attacks are very difficult to prevent.

Advantages:

1. Networks, computers and documents are protected from unauthorized access.
2. Protection of Important Data – Knowledge is one of the enterprise's most valuable properties. Its Protection is key aspect of the structure in information technologies. Integrating a security solution can provide protection for all information.
3. Stay ahead of Competitors – Implementing Security Strategies in competition puts company competitive. IT Protection System blends with enterprise systems that already exist. Protecting data acts like icing on the cake.
4. This builds strong credibility and profile. Improved confidence among stakeholders in the security arrangements for your information.
5. Faster recovery times should a disruption occur. It guarantees that vital market activities proceed in the event of natural disasters or high-impact health accidents.
6. It ensures laws and regulations are adhered to. Improved company credentials with proper safety checks in place.
7. Improved security of knowledge and maintenance of company continuity.

Challenges:

1. **Ransomware Evolution:** Ransomware is a form of Ransomware that locks the data on a victim's device, and demands payment before the ransomed data is released. Connection rights restored to the survivor, following positive payment. Ransomware is the bane of data professionals, cyber security, information technology and executives. Ransomware attacks in cybercrime areas are on the rise day by day. To defend the company, IT practitioners and corporate owners need a strong

response plan against Ransomware attacks (Zimba et al., 2018) [47]. It requires careful preparation to retrieve data and service from companies and consumers, as well as reporting any violations against the Notifiable Data Breaches program.

2. **Block chain Revolution:** Block chain technology is the most important technological invention for the time span. It is the first time we already have a perfect one native digital medium in human history for peer-to - peer exchange of value. The block chain is a system that makes for crypto currencies such as Bitcoin. The block chain is a vast global platform that allows two or more parties to make a transaction or do business without needing a trusted third party (Narang et al., 2014) [48]. With regard to cyber security, it is difficult to predict what block chain systems will offer.
3. **IoT Threats:** IoT is an interrelated network of physical devices that can be connected via the Internet. The linked hardware devices have a unique identifier (UID) and are able to transmit data over a network without any human-to - human or computer-to-computer interface criteria (Duic et al., 2017) [7]. The firmware and software running on IoT devices makes consumers and companies highly vulnerable to cyber-attacks. While planning IoT stuff, the use of cyber security and for commercial purposes is not kept in mind.
4. **AI Expansion:** AI's primary advantage in our information defence approach is the opportunity to secure and defend an infrastructure before the malware attack begins, thus minimizing the effect. In a moment when a threat impacts a business, AI takes immediate action against the malicious attacks. IT business leaders and information security management teams view AI as a future protective control that will allow our company to stay ahead of the cyber security development curve.
5. **Serverless Apps Vulnerability:** Serverless software and apps are applications that rely on third party cloud storage or back-end services such as Google Cloud feature, Amazon Web Services (AWS) lambda, and so on. The serverless applications allow cyber criminals to quickly distribute attacks on their network as the users access the software on their computer locally or off-server. The serverless applications do little to keep out our data from the attackers. The serverless technology does not help if an attacker achieves access to our data by vulnerability such as leaked passwords, a compromised insider or then serverless by some other way (Barraclough et al., 2013) [49]. Typically, the applications without servers are small in size. It helps developers get their applications started fast and easily. They don't need to think about the network that underlies them. The web-services and data processing software are the most popular serverless applications.

4.6 SUMMARY OF RELATED WORK

Table1: Review of findings from 2010-2020 presented by various authors.

Sl. No.	Author(s)	Year	Inventions/Findings/Results
1	Aburrous et al. [25]	2010	Proposed a distinctive phishing website solution using Data Mining and Fuzzy logic combination to save Internet users when performing online purchases.
2	Coskun et al. [50]	2010	Propose a tool used by shared contacts to identify local members of an unstructured botnet.
3	Xia et al. [43]	2010	Developed A scheme for detecting a DDoS flood attack using blurred logic
4	Wang et al. [51]	2010	Design a peer-to - peer hybrid botnet that consists of servant and client bots.
5	S. X. Wu & Banzhaf [52]	2010	Focused on Computational Intelligence approaches and intrusion detection applications.
6	Nappa et al. [53]	2010	Recommend a parasitic botnet protocol that exploits Skype network overlays.
7	Zhong & Yue [54]	2010	Uses fuzzy c-means and Apriori techniques to construct a model and detect unknown attacks on the DDoS.
8	H. V. Nguyen & Choi [55]	2010	Detects only known attacks by using k-nearest neighbour technique

9	Xiang et al. [56]	2011	Detects DDoS flooding attacks effectively using new data metrics
10	Fedynyshyn et al. [57]	2011	Suggested a solution for using persistence to identify and classify C&C channels into their architecture (HTTP, IRC, or P2P) by monitoring the traffic of individual host.
11	Saad, Sherif traore,issa ghorbani [58]	2011	A comparison was made between five machine learning techniques commonly used for the detection of decentralized botnets.
12	Zhang et al. [59]	2011	Propose a botnet P2P communication technique by fingerprinting malicious and benign traffic.
13	Y. Wu [60]	2011	Used the decision tree and traceback for offender location using corresponding traffic flow patterns
14	Raj Kumar & Selvakumar [61]	2011	RBPBoost combines an ensemble of classifier outputs and a cost minimization strategy for Neyman Pearson to make a final classification decision during DDoS attack detection and get a high DR
15	Karimazad & Faraahi [62]	2011	Uses neural RBF networks and achieves weak FAR
16	Udhayan & Hamsapriya [63]	2011	Uses an SSM to identify DDoS attacks within consecutive time intervals based on sampling of flow
17	Sa, n.d.[64]	2011	Proposed an agent-based model for the classification of normal and attack activities in each topology cluster, using two-tier hierarchical network topology
18	Zang et al. [65]	2011	Suggested hierarchical and k-mean clustering for the detection of C&C botnets.
19	Gupta et al. [66]	2012	Uses an ANN to predict zombie numbers in a DDoS attack
20	Garasia et al. [67]	2012	By applying four main phases called traffic representation, separation filtering, and detection, the Apriori association algorithm used to identify the presence of a C&C channel for HTTP botnets.
21	Jeyanthi & Sriman Narayana Iyengar [68]	2012	Detects attacks by DDoS by entropy-based analysis
22	François et al. [69]	2012	A technique for detecting complete DDoS flooding attack. Supports even gradual deployment on actual networks
23	H. T. Nguyen & Franke [10]	2012	Proposed System for Adaptive Intrusion Detection (A-IDS). This model is capable of detecting various types of attacks in heterogeneous and adverse network environments.
24	Zhang and Yuan [20]	2012	Proposed phishing detection approach which makes use of the neural network as a technique of machine learning.
25	Warriach [70]	2013	Developed an approach by proposing Hidden Markov Models (HMMs) to identify and classify data and system fault types.
26	Lee & Kim [71]	2013	Exploring the design and mitigation of botnets using URL Shortening Services (USS) for alias fluxing.
27	Zhao et al. [72]	2013	Addressed the ability to detect botnet traffic by tracking a small portion of the flow and by creating a classifier on identified botnets to identify unknown botnets.
28	R. Islam & Abawajy [22]	2013	Proposed an exclusive Multi-Tier Classification Model approach along with the method of extracting phishing email features weighing the contents of the text and message header and selecting feature by priority level.

29	Barraclough et al. [49]	2013	Innovative approach to phishing attack identification and effective countermeasures; Neuro-Fuzzy Logic with five inputs.
30	Sharma & Parihar [73]	2013	Used SVM classifier for wormhole detection, black hole and selective forwarding attacks.
31	Louvieris et al. [74]	2013	Proposed an effect-based IDS function identifier using Naive Bayes as a selection tool.
32	Kaur, Gursheen Singh [75]	2014	The behavioural shift of sensor nodes was analyzed using data mining techniques and mechanisms were developed to classify variable black holes.
33	Xie et al. [39]	2014	A novel anomaly detection system using the Support Vector Machine (SVM) and ADFFA-LD is proposed for experimentation
34	Kato & Klyuev [21]	2014	Analyzed a large number of network traffic packets and used the patterns of DDoS attacks for each IP address to implement a DDoS attack detection program.
35	Huseynov et al. [30]	2014	Comparison of K-means algorithm with Ant Colony System algorithm to detect decentralized botnets.
36	Shamshirband et al. [42]	2014	Fuzzy Q-learning (FQL) approach used to detect flooding attacks.
37	Stevanovic & Pedersen [76]	2014	Built a new botnet detection method focused on flow-level network traffic analysis, and supervised MLAs to catch malicious botnet traffic patterns.
38	Narang et al. [48]	2014	Instead of a conventional 5-tuple flow-based detection approach, a 2-tuple conversation-based approach, port-oblivious, protocol oblivious and deep packet inspection is not necessary.
39	Smadi et al. [23]	2015	Proposed a data mining algorithm-based phishing detection model using features extracted from various sections of emails.
40	Rao & Ali [77]	2015	Suggest a solution to phishing attacks by suggesting a combination of whitelist and tactics focused on visual similarity.
41	Wijesinghe et al. [17]	2015	Proposed traffic analysis techniques use fixed IP flows in various products and IPFIX to build a standardized framework for detecting a variety of bot families.
42	Bhuyan et al. [78]	2015	Suggested an empirical analysis using various knowledge metrics to resolve critical security problems, such as identification of low and high-rates DDoS attacks
43	Hoque et al. [79]	2016	Presented a system to track DDoS attacks utilizing new statistical test called FFSc.
44	Bhamare et al. [32]	2016	Focused on imbalance of huge amounts of research on supervised ML techniques and their applicability to real-time scenarios, and concluded that supervised ML techniques need substantial rework to improve cloud security performance.
45	Azab et al. [29]	2016	Researchers suggested methods to detect C&C channel traffic as DPI, DNS request behaviour, time, correlation and machine learning
46	He et al. [80]	2017	Formulated a machine-learning based DDoS attack detection method to avoid source-side attacks in the cloud.
47	Alejandre et al. [81]	2017	Suggested selection of a set of features for detecting botnets in the C&C phase using the GA as an optimizer

			algorithm and the C4.5 classification to evaluate individuals in the GA.
48	M. Wu et al. [9]	2017	Physical data machine learning methods for the detection of Cyber Physical attacks in CMS are developed and implemented.
50	Zimba et al. [47]	2018	Modelled various multi-stage crypto Ransomware attacks emanating from various sources of CI infiltration and validated with WannaCry attacks.
51	Islam et al. [46]	2018	Investigated the effect of the EMS attacker's false data injections while optimizing the attack signal to gain full benefits from legitimate participants while preserving the supply-demand balance on the local energy market.
52	Kim & Park [82]	2018	Proposed an FPGA-based Network Intrusion Detection System (NIDS) for IEC 61850 industrial network works designed specifically for substation automation.
53	Ilavendhan & Saruladha [83]	2018	Studied VANET security problems and multiple network layer assaults in VANET
54	Ferreira [84]	2019	Focused on the malicious URL, hackers have various techniques and algorithms to blur their URLs in order to bypass defences.
56	Huang & Zhu [45]	2019	Developed multi-stage incomplete information Bayesian game system with the existence of Advanced Persistent Threats (APTs) to develop proactive and adaptive defence strategies for critical infrastructure networks.
57	Roopak et al. [4]	2019	The CNN+LSTM hybrid model studied performs better than the rest of the machine learning algorithms and deep learning models.
58	Akin et al. [19]	2020	Built a unified software-defined network (SDN) automation solution sufficient to prevent cyber-attacks at the root of the attack
59	Zahid et al. [24]	2020	A mitigation mechanism was developed to reduce risks on the application layer related to authentication, data integrity, data freshness, confidentiality, and non-repudiation.
60	Ravikumar & Govindarasu [36]	2020	Proposed identification of anomalies using Machine Learning and model based mitigation to ensure secure and robust operation of the WADC system.
61	Zarca et al. [35]	2020	Set out a novel solution for managing dynamically virtual IoT HoneyNets to mitigate cyber attacks in IoT networks enabled by SDN / NFV.
62	Durand & Wegener [8]	2020	Analysed how cyber threats could be carried out be avoided from security and a profit / production perspective causing problems for a chemical company.

5. DISCUSSION :

Increased dependence on information technology and the internet of things makes it important that IT professionals are alert to growing cases of cyber attacks with the sole purpose of being proactive in order to react as rapidly as possible when IT infrastructure is under attack and also introduce mitigation measures to avoid more attacks(Ferreira, 2019)[84]. One of cyber security's most problematic elements is the rapidly and constantly evolving nature of the security risks. Cyber-criminals evolve their hacking techniques rapidly. We strike rapidly, making defence more important than ever before in due time. Consequently, having an awareness of the threat is one of the first steps involved in implementing a successful information security strategy.

Cybercriminals today use many sophisticated methods to escape detection as they hack into corporate networks to steal intellectual property secretly (Seissa et al., 2017) [6]. They also encode their threats using complicated algorithms to avoid detection by intrusion prevention systems. If a target has been broken, attackers may attempt to download and install malware onto the compromised device. In many cases the malware used is a newly evolved version that is not yet exposed to conventional anti-virus solutions. The development of Ids is the best way to secure devices and networks for the detection of intruders (S. X. Wu & Banzhaf, 2010) [52]. Hence IDS 'role was not just that to detect intruders but also to track intruders attack. A specific framework shall be drawn up to protect data and services from unauthorized access, harm and denial of use. The security perspective should be prepared for any system based on the expected results.

6. RESEARCH GAP :

Some of the concerns we found about the study gap are:

Research gap 1: Data mining techniques to enable intrusion prevention are being developed for cyber analytics. Techniques used before like a firewall, and IDS failed to identify, without his knowledge, the real-time attackers that occurred in the manager's absence. Recognizing the attacker in real time is difficult, because it can create multiple IP and packet attacks. A computer network is a combination of Software and Hardware. Each component carries risks, poor health, and shortfalls. Ransomware attack leaves data unprotected. Those who learn programming and programs can quickly find out from the log files about the different operations being carried out on the systems.

Research gap 2: A framework for detecting intrusion of PS-Poll DOS infiltration in 802.11 networks, application of a distinct system of real-time events. This technique makes use of RTDES to monitor Denial of Service attack in real-time on a single event system. High accuracy and detection rate are one of the major advantages but frame shortages are one of the major disadvantages.

Research gap 3: Network Intrusion Detection (ID) is tackled by unattended and unattended hybrid mining-a detailed ISCX case study. This proposes a detection of hybrid intrusion (kM-RF) which the alternate approach usually outperforms in terms of the false alarm volume, accuracy and detection times. ISCX (a typical intrusion detection dataset) is used to determine the efficacy of kM-RF and an in-depth analysis is conducted to test the effects of any observed pre-processing features or characteristics. It also uses a special pre-treatment approach for categorical transformation methods or numerical data attributes and generates more raw data segregated classes. Some new features or applications to find payloads, clustered attacks and IP scans and a mix of kMeans and random forest classifiers to prevent further interference effectively.

Research gap 4: The approach involves a technique for solving the problem of malicious attack detection by reviewing the online data sets. This is done by the use of a Bayesian classifier which is incrementally naive. In comparison, active learning allows the problem to be solved by using a limited collection of specified data points, which are also very costly to obtain.

Research gap 5: Deep learning that can create better and more effective intrusion detection architecture is used. The aim approach is to distinguish normal behaviour from anomalous activity in the network. The IDS (Intrusion Detection System) is one of the methods used to detect unwanted network or device activity and protecting the machine from network attacks. Attacks are observed in the system by distinguishing between actions and functionality of the rising and irregular networks. This work also defines numerous methods used in experimental analysis to produce IDS.

Research gap 6: The constant introduction of new and emerging threats targets and challenges a wide range of companies around the world. For this reason, the scientific community has drawn attention to the existence and improvement of the Intrusion Detection Systems efficiency. This is a groundbreaking way of monitoring malicious behaviour in terms of DDoS and Ransomware cyber threats using deep learning techniques. Due to the exponential growth of Mobile apps and their use by most Internet users, cyber security achievement, data protection and safe communication are deemed necessary. At the same time, increased exposure to much more advanced cyber threats has been noticed through the Internet and computer networking in the digital world of academia and industry, with financial costs particularly in Small-Medium Enterprises (SMEs).

Research gap 7: Self using Novel Network Intrusion Prevention Software Organizing an improved neural vector system network with assistance has been proposed. Because of its architecture, the

proposed program does not have a secure solution that is neither signed nor based on rules, and is highly effective in minimizing known and unknown risks.

Research gap 8: For multifunctional efficiency, detection accuracy and performance in real time of detecting abnormal activity within industrial networks are effectively increased. The novel apps are dual to quickly pick a node with a high security coefficient as the centre of the cluster and align the multi-function data in a cluster around the centre. Experimental findings indicate that in terms of the detection rate and time compared to other algorithms the suggested algorithm is of high quality. The sensitivity of detecting suspicious data in the networking sector exceeds 97.8%, and the incorrect identification result dropped by 8.8%. Detection devices for intrusion detection can effectively identify and track events involving intruders although it is challenging with network security technologies. The usage of intrusion prevention devices for industrial networks would thus remove the restrictions of traditional network protection methods, thereby perfecting the entire network of industrial safety systems.

7. RESEARCH AGENDA :

1. Which are the best Machine Learning Algorithms to combat cyber attacks?
2. What technology will enhance the privacy of a wide network of users exchanging data?
3. What system can prevent cyber attacks and protect the data over the network?
4. What new development framework can be equipped to integrate a cyber security program with the best use of machine learning algorithms?
5. What Machine Learning Technology can be proposed for cyber defence, rising applications, hardware, and networking and storage complexities?

8. CONCLUSION :

As technology tends to grow, the world is increasingly becoming a global village with almost all operating on the virtual worlds influencing most aspects of human life, enabling development, removing barriers to trade and allowing people across the globe to connect, collaborate and share ideas. Yet by the day hackers become more advanced. This puts the responsibility on the IT Experts to secure the IT infrastructure and users, hence necessity to be attentive and efficient in reacting to cyber attacks as well as proactive in ensuring that cyber threats are mitigated against them in their entirety. Cyber crime is increasing, and as such, cyber security needs to grow even faster if we hope to keep users online and, on the system, safe. The main aim of cyber security is the protection of harmful cyber-crime networks, applications and users over the internet.

Awareness of information security is crucial to rising cybercrimes and encouraging cyber protection. Currently there are so many uses of techniques, methods and tools to detect intrusion in the computer network and ongoing research is being done to make them even better to recognize intrusion. Yet new threats have emerged concurrently which will be hard for Handel as they want to change their behaviour. Within this paper we explained various techniques of machine learning applied to detect intrusions. Through the study, we argue that the approaches to machine learning are fit to identify anomalies through proper training, but the performance may vary according to different algorithms. Machine learning algorithms should also be applied in a manner that is sufficient to improve detection accuracy.

REFERENCES:

- [1] Verma, P., Makwana, A. & Khan, S. (2015). Cyber Security: a Survey on Issues and Solutions. *International Journal of Advanced Research in Engineering and Technology*, 6(4), 976–6480.
- [2] Buczak, Anna L. Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, 18(2), 11543–1176. <https://doi.org/10.1007/BF01018580>
- [3] Hoque, Sazzadul Mukit, A. Naser, A. (2012). An Implementation of Intrusion Detection System Using Genetic Algorithm. *International Journal of Network Security & Its Applications*, 4(2), 109–120. <https://doi.org/10.5121/ijnsa.2012.4208>
- [4] Roopak, M., Yun Tian, G. & Chambers, J. (2019). Deep learning models for cyber security in IoT

- networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 452–457. <https://doi.org/10.1109/CCWC.2019.8666588>
- [5] Neethu, B. (2014). Classification of Intrusion Detection Dataset using machine learning Approaches. *International Journal of Electronics and Computer Science Engineering*, 34(3), 1044–1051. <https://doi.org/10.3969/j.issn.0253-2417.2014.03.013>
- [6] Seissa, I. G., Ibrahim, J. & Yahaya, N. (2017). Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review. *International Journal of Science and Research (IJSR)*, 6(1), 180–186. <https://doi.org/10.21275/art20163936>
- [7] Duic, I., Cvrtila, V., & Ivanjko, T. (2017). International cyber security challenges. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 1309–1313. <https://doi.org/DOI:10.23919/MIPRO.2017.7973625>
- [8] Durand, H. & Wegener, M. (2020). Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods. *Mathematics*, 8(4). <https://doi.org/10.3390/math8040499>
- [9] Wu, M., Song, Z. & Moon, Y. B. (2017). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of Intelligent Manufacturing*. <https://doi.org/10.1007/s10845-017-1315-5>
- [10] Nguyen, H. T. & Franke, K. (2012). Adaptive Intrusion Detection System via online machine learning. *12th International Conference on Hybrid Intelligent Systems, HIS*, 271–277. <https://doi.org/10.1109/HIS.2012.6421346>
- [11] Zamani, Mahdi Movahedi, M. (2015). Machine Learning Techniques for Intrusion Detection. *ArXiv*. <https://doi.org/10.4018/978-1-7998-2242-4.ch003>
- [12] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4 PART 2), 1690–1700. <https://doi.org/10.1016/j.eswa.2013.08.066>
- [13] Borkar, A., Donode, A., & Kumari, A. (2018). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). *Proceedings of the International Conference on Inventive Computing and Informatics, ICICI 2017, Icici*, 949–953. <https://doi.org/10.1109/ICICI.2017.8365277>
- [14] Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H., Marufuzzaman, M., & Bian, L. (2017). Botnet detection using graph-based feature clustering. *Journal of Big Data*, 4(1). <https://doi.org/10.1186/s40537-017-0074-7>
- [15] Kozik, R., Choraś, M., Renk, R., & Hołubowicz, W. (2014). A Proposal of Algorithm for Web Applications Cyber Attack Detection. *IFIP International Conference on Computer Information Systems and Industrial Management*, 8838. https://doi.org/10.1007/978-3-662-45237-0_61
- [16] Wang, J., & Paschalidis, I. C. (2017). Botnet Detection Based on Anomaly and Community Detection. *IEEE Transactions on Control of Network Systems*, 4(2), 392–404. <https://doi.org/10.1109/TCNS.2016.2532804>
- [17] Wijesinghe, U., Tupakula, U., & Varadharajan, V. (2015). An enhanced model for network flow based botnet detection. *Conferences in Research and Practice in Information Technology Series*, 159(January), 101–110.
- [18] Haddadi, Fariba Cong, D. Le. (2015). On the Effectiveness of Different Botnet Detection Approaches. *Lecture Notes in Computer Science*, 9065, 421–436. <https://doi.org/10.1007/978-3-319-17533-1>
- [19] Akin, G., Bük, O., & Uçar, E. (2020). An inter-domain attack mitigating solution. *Turkish Journal of Electrical Engineering and Computer Sciences*, 28(2), 757–772. <https://doi.org/10.3906/elk->

[1904-179](#)

- [20] Zhang, Ningxia Yuan, Y. (2012). Phishing Detection Using Neural Network. *CS229*. <https://doi.org/10.19026/rjit.6.2164>
- [21] Kato, K. & Klyuev, V. (2014). An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine. *International Journal of Intelligent Computing Research*, 5(3), 464–471. <https://doi.org/10.20533/ijicr.2042.4655.2014.0060>
- [22] Islam, R., & Abawajy, J. (2013). A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications*, 36(1), 324–335. <https://doi.org/10.1016/j.jnca.2012.05.009>
- [23] Smadi, S., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2015, December). Detection of phishing emails using data mining algorithms. In *2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (pp. 1-8). IEEE.
- [24] Zahid, M., Inayat, I., Daneva, M. & Mehmood, Z. (2020). A security risk mitigation framework for cyber physical systems. *Journal of Software: Evolution and Process*, 32(2), 1–15. <https://doi.org/10.1002/smr.2219>
- [25] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, 37(12), 7913–7921. <https://doi.org/10.1016/j.eswa.2010.04.044>
- [26] Axelsson, S. (2015). *Intrusion Detection Systems : A Survey and Taxonomy* *Intrusion Detection Systems : A Survey and Taxonomy*. April 2000, 1–6. <https://doi.org/10.20944/preprints202006.0065.v1>
- [27] Ibor, A. E., Oladeji, F. A. & Okunoye, O. B. (2018). A Survey of Cyber Security Approaches for Attack Detection, Prediction, and Prevention. *International Journal of Security and Its Applications*, 12(4), 15–28. <https://doi.org/10.14257/ijisia.2018.12.4.02>
- [28] Aissa, N. B. & Guerroumi, M. (2016). Semi-supervised Statistical Approach for Network Anomaly Detection. *Procedia Computer Science*, 83(Fams), 1090–1095. <https://doi.org/10.1016/j.procs.2016.04.228>
- [29] Azab, A., Alazab, M., & Aiash, M. (2016). Machine learning based botnet identification traffic. *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 1788–1794. <https://doi.org/10.1109/TrustCom.2016.0275>
- [30] Huseynov, K., Kim, K. & Yoo, P. D. (2014, January). Semi-supervised botnet detection using ant colony clustering. In *Symp. Cryptography and Information Security (SCIS), Kagoshima, Japan*.
- [31] Lin, W. C., Ke, S. W. & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, 78(1), 13–21. <https://doi.org/10.1016/j.knosys.2015.01.009>
- [32] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2017). Feasibility of Supervised Machine Learning for Cloud Security. *ICISS 2016 - 2016 International Conference on Information Science and Security*, 31–35. <https://doi.org/10.1109/ICISSEC.2016.7885853>
- [33] Shapoorifard, H., & Shamsinejad, P. (2017). A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques. *International Journal of Computer Applications*, 166(3), 13–16. <https://doi.org/10.5120/ijca2017913948>
- [34] Song, J., Takakura, H., Okabe, Y. & Nakao, K. (2013). Toward a more practical unsupervised anomaly detection system. *Information Sciences*, 231, 4–14. <https://doi.org/10.1016/j.ins.2011.08.011>
- [35] Zarca, A. M., Bernabe, J. B., Skarmeta, A., & Calero, J. M. A. (2020). *Virtual IoT HoneyNets to*

- mitigate cyberattacks in SDN / NFV-enabled IoT networks.* 8716(c), 1–15.
<https://doi.org/10.1109/JSAC.2020.2986621>
- [36] Ravikumar, G., & Govindarasu, M. (2020). Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning. *IEEE Transactions on Smart Grid*, 3053(c), 1–1.
<https://doi.org/10.1109/tsg.2020.2995313>
- [37] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H. & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, 378, 484–497.
<https://doi.org/10.1016/j.ins.2016.04.019>
- [38] Han, Y., Alpcan, T., Chan, J., Leckie, C., & Rubinstein, B. I. P. (2016). A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Transactions on Information Forensics and Security*, 11(3), 556–570.
<https://doi.org/10.1109/TIFS.2015.2505680>
- [39] Xie, M., Hu, J. & Slay, J. (2014). Evaluating Host-based Anomaly Detection Systems : Application of the One-class SVM Algorithm to. *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 978–982. <https://doi.org/10.1109/FSKD.2014.6980972>
- [40] Alsheikh, M. A., Lin, S., Niyato, D. & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys and Tutorials*, 16(4), 1996–2018. <https://doi.org/10.1109/COMST.2014.2320099>
- [41] Xu, X., Zuo, L. & Huang, Z. (2014). Reinforcement learning algorithms with function approximation: Recent advances and applications. *Information Sciences*, 261, 1–31.
<https://doi.org/10.1016/j.ins.2013.08.037>
- [42] Shamshirband, S., Patel, A., Badrul, N. & Mat, L. (2014). Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. *Engineering Applications of Artificial Intelligence*, 2008, 1–14.
<https://doi.org/10.1016/j.engappai.2014.02.001>
- [43] Xia, Z., Lu, S. & Li, J. (2010). *Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic A brief review of self-similarity.* 34, 497–507.
- [44] Rastegari, S., Hingston, P. & Lam, C. P. (2015). Evolving statistical rulesets for network intrusion detection. *Applied Soft Computing Journal*, 33, 348–359.
<https://doi.org/10.1016/j.asoc.2015.04.041>
- [45] Huang, L. & Zhu, Q. (2019). Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. *Performance Evaluation Review*, 46(2), 52–56.
<https://doi.org/10.1145/3305218.3305239>
- [46] Islam, S. N., Mahmud, M. A. & Oo, A. M. T. (2018). *Impact of optimal false data injection attacks on local energy trading in a residential microgrid.* 4(1), 30–34.
<https://doi.org/10.1016/j.ict.2018.01.015>
- [47] Zimba, A., Wang, Z. & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, 4(1), 14–18.
<https://doi.org/10.1016/j.ict.2017.12.007>
- [48] Narang, P., Ray, S., Hota, C. & Venkatakrisnan, V. (2014). PeerShark: Detecting peer-to-peer botnets by tracking conversations. *Proceedings - IEEE Symposium on Security and Privacy, 2014-Janua*, 108–115. <https://doi.org/10.1109/SPW.2014.25>
- [49] Barraclough, P. A., Hossain, M. A., Tahir, M. A., Sexton, G. & Aslam, N. (2013). Intelligent phishing detection and protection scheme for online transactions. *Expert Systems with Applications*, 40(11), 4697–4706. <https://doi.org/10.1016/j.eswa.2013.02.009>
- [50] Coskun, B., Dietrich, S., & Memon, N. (2010). Friends of an enemy: Identifying local members of peer-to-peer botnets using mutual contacts. *Proceedings - Annual Computer Security Applications*

- Conference, ACSAC, 131–140. <https://doi.org/10.1145/1920261.1920283>
- [51] Wang, P., Sparks, S., & Cou, C. (2010). An advanced hybrid peerto-peer botnet. *IEEE Transactions on Dependable and Secure Computing*, 7(2), 113–127. <https://doi.org/10.1109/TDSC.2008.35>
- [52] Wu, S. X., & Banzhaf, W. (2010). *The use of computational intelligence in intrusion detection systems : A review*. 10, 1–35. <https://doi.org/10.1016/j.asoc.2009.06.019>
- [53] Nappa, A., Fattori, A., Balduzzi, M., Dell’Amico, M., & Cavallaro, L. (2010). Take a deep breath: A stealthy, resilient and cost-effective botnet using skype. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6201 LNCS, 81–100. https://doi.org/10.1007/978-3-642-14215-4_5
- [54] Zhong, R., & Yue, G. (2010). DDoS Detection System Based on Data Mining. *Proceedings of the Second International Symposium on Networking and Network Security*, 1, 062–065. <http://academypublisher.com/proc/isnns10/papers/isnns10p62.pdf>
- [55] Nguyen, H. V., & Choi, Y. (2010). Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 4(3), 640–645. <https://doi.org/10.5281/zenodo.1072908>
- [56] Xiang, Y., Li, K., & Zhou, W. (2011). *Low-Rate DDoS Attacks Detection and Traceback* by. 6(2), 426–437.
- [57] Fedynyshyn, G., Chuah, M. C. & Tan, G. (2011). Detection and classification of different botnet C&C channels. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6906 LNCS, 228–242. https://doi.org/10.1007/978-3-642-23496-5_17
- [58] Saad, Sherif traore, Issa ghorbani, Ali. (2011). Detecting P2P Botnets through Network Behavior Analysis and Machine Learning. *Ninth Annual International Conference on Privacy, Security and Trust Detecting*. <https://doi.org/10.1109/PST.2011.5971980>
- [59] Zhang junjie, Perdisci Roberto, Lee Wenke, X. L. and S. U. (2011). Detecting Stealthy P2P Botnets Using Statistical Traffic Fingerprints’.pdf. *2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*. <https://doi.org/10.1109/DSN.2011.5958212>
- [60] Wu, Y. (2011). *DDoS detection and traceback with decision tree and grey relational analysis Huei-Ru Tseng Wu Yang * and Rong-Hong Jan*. 7(2), 121-136.
- [61] Raj Kumar, P. A. & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, 34(11), 1328–1341. <https://doi.org/10.1016/j.comcom.2011.01.012>
- [62] Karimazad, R. & Faraahi, A. (2011). An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks. *2011 International Conference on Network and Electronics Engineering*, 11, 44–48.
- [63] Udhayan, J. & Hamsapriya, T. (2011). Statistical segregation method to minimize the false detections during DDoS attacks. *International Journal of Network Security*, 13(3), 152–160.
- [64] Sa, M. & Rath, A. K. (2011). A Simple Agent Based Model for Detecting Abnormal Event Patterns in a Distributed Wireless Sensor Networks. *International Journal of Computer Science and Security, (IJCSS)*, 4(6), 580-588.
- [65] Zang, X., Tangpong, A., Kesidis, G. & Miller, D. J. (2011). Botnet Detection Through Fine Flow Classification. *Science*, 0915552, 1–17.
- [66] Gupta, B. B., Joshi, R. C. & Misra, M. (2012). ANN based scheme to predict number of zombies in a DDoS attack. *International Journal of Network Security*, 14(2), 61–70.
- [67] Garasia, S. S., Rana, D. P. & Mehta, R. G. (2012). HTTP botnet detection using frequent patternset mining. *International Journal of Engineering Science & Advanced Technology*, 2(3), 619-624.

- [68] Jeyanthi, N. & Sriman Narayana Iyengar, N. C. (2012). An entropy based approach to detect and distinguish DDoS attacks from flash Crowds in VoIP Networks. *International Journal of Network Security*, 14(5), 257–269.
- [69] François, J., Aib, I. & Boutaba, R. (2012). FireCol: A collaborative protection network for the detection of flooding DDoS attacks. *IEEE/ACM Transactions on Networking*, 20(6), 1828–1841. <https://doi.org/10.1109/TNET.2012.2194508>
- [70] Warriach, E. U. (2013). *Fault Detection in Wireless Sensor Networks: A Machine Learning Approach*. <https://doi.org/10.1109/CSE.2013.116>
- [71] Lee, S. & Kim, J. (2013). Fluxing botnet command and control channels with URL shortening services. *Computer Communications*, 36(3), 320–332. <https://doi.org/10.1016/j.comcom.2012.10.003>
- [72] Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A. & Garant, D. (2013). Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security*, 1–15. <https://doi.org/10.1016/j.cose.2013.04.007>
- [73] Sharma, A. K. & Parihar, P. S. (2013). An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2(7), 249–256.
- [74] Louvieris, P., Clewley, N. & Liu, X. (2013). Effects-based feature identification for network intrusion detection. *Neurocomputing*, 121, 265–273. <https://doi.org/10.1016/j.neucom.2013.04.038>
- [75] Kaur, Gursheen Singh, M. (2014). Detection of Black Hole in Wireless Sensor Network based on Data Mining. *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, 2014, 457461. <https://doi.org/10.1017/CBO9781139058452.002>
- [76] Stevanovic, M. & Pedersen, J. M. (2014). An efficient flow-based botnet detection using supervised machine learning. *2014 International Conference on Computing, Networking and Communications, ICNC 2014*, 797–801. <https://doi.org/10.1109/ICCNC.2014.6785439>
- [77] Rao, R. S. & Ali, S. T. (2015). A computer vision technique to detect phishing attacks. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 596–601. <https://doi.org/10.1109/CSNT.2015.68>
- [78] Bhuyan, M. H., Bhattacharyya, D. K. & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, 51, 1–7. <https://doi.org/10.1016/j.patrec.2014.07.019>
- [79] Hoque, N., Bhattacharyya, D. K. & Kalita, J. K. (2016). A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. *2016 8th International Conference on Communication Systems and Networks, COMSNETS 2016*, 1, 1–2. <https://doi.org/10.1109/COMSNETS.2016.7439939>
- [80] He, Z., Zhang, T. & Lee, R. B. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 114–120. <https://doi.org/10.1109/CSCloud.2017.58>
- [81] Alejandre, F. V., Cortés, N. C., & Anaya, E. A. (2017). Feature selection to detect botnets using machine learning algorithms. *2017 International Conference on Electronics, Communications and Computers, CONIELECOMP 2017*. <https://doi.org/10.1109/CONIELECOMP.2017.7891834>
- [82] Kim, J. & Park, J. (2018). FPGA-based network intrusion detection for IEC 61850-based industrial network. *ICT Express*, 4(1), 1–5. <https://doi.org/10.1016/j.icte.2018.01.002>
- [83] Ilavendhan, A. & Saruladha, K. (2018). Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express*, 4(1), 46–50.

<https://doi.org/10.1016/j.ict.2017.12.002>

- [84] Ferreira, M. (2019). Malicious URL detection using machine learning algorithms. In *Proc. Digit. Privacy Security Conf.* (pp. 114-122).

A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model

Sangeetha Prabhu¹ & Nethravathi P. S.²

¹Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

² Professor, College of Computer and Information Sciences, Srinivas University, Mangalore, India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

Subject Area: Computer Science.

Type of the Paper: Review based Research Analysis.

Type of Review: Peer Reviewed as per [C|O|P|E](#) guidance.

Indexed In: OpenAIRE.

DOI: <https://doi.org/10.5281/zenodo.6349848>

Google Scholar Citation: [IJAEML](#)

How to Cite this Paper:

Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 149-159. DOI: <https://doi.org/10.5281/zenodo.6349848>

International Journal of Applied Engineering and Management Letters (IJAEML)

A Refereed International Journal of Srinivas University, India.

Crossref DOI : <https://doi.org/10.47992/IJAEML.2581.7000.0126>

Received on: 24/02/2022

Published on: 14/03/2022

© With Authors.



This work is licensed under a [Creative Commons Attribution-Non-Commercial 4.0 International License](#) subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model

Sangeetha Prabhu¹ & Nethravathi P. S.²

¹Research Scholar, College of Computer Science and Information Science, Srinivas
University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

² Professor, College of Computer and Information Sciences, Srinivas University, Mangalore,
India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

ABSTRACT

Purpose: *When communication networks and the internet of things are integrated into business control systems, they become more vulnerable to cyber-attacks, which can have disastrous consequences. An Intrusion Detection System is critical for identifying and blocking attacks in IoT networks. As a result, utilizing a unique Classification and Encryption approach, this article offered a novel architecture for attack node mitigation.*

Design/Methodology/Approach: *This study reviews the current status of various cyber-attack detection models and their mitigation techniques. The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or Ransomware. When tested, we use trained information or a data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of the input. When the model identifies the attacker node, it is removed via the BAIT technique from the network.*

Findings/Result: *Recognizing the importance of information security is critical to combating cybercrime and encouraging cyber security. There are numerous tactics, strategies, and equipment currently in use to detect intrusion in a computer network, and continuing research is being conducted to improve their ability to detect intrusion. The basic version of a cyber-assault detection and mitigation system using the BRELU-RESNET method was evaluated in this study.*

Originality/Value: *This review-based research article examines the present state of cyber-attack detection and mitigation, as well as the research gaps and research goals.*

Paper Type: *Review-based research analysis*

Keywords: Cyber-attack detection, BAIT approaches, Cryptosystem, Feature extraction, Deep Ensemble Model, Cyber-attack mitigation

1. INTRODUCTION :

The virtual revolution of big-scale production environments promotes the usage of massive statistics analytics in solving plant outages, equipment breakdowns, fault prediction, and ensuring cybersecurity through the extension of computer networks and interconnectivity of computer systems in cyber-physical structures [1] [2]. The topic of cyber-defense has aroused academics' interest in recent years, particularly as cyber-physical networks have evolved into extremely dangerous cyber-assaults that might endanger any section of the unexploited cyber surface [3]. This highlights the need of implementing area green identification algorithms and robust solution mechanisms that protect both the cyber and physical parts of the infrastructure - a necessary precondition for improving operational technologies [3] [4]. Many contributions have been made throughout this field of operational technologies by the process automation and control group in particular.

CPS (Cyber-Physical Systems) is a term used to describe the mixture of computational, communication, and physical components [5] [6]. Cyber-Physical Systems CPS is a modeling tool that can be used to simulate a wide range of applications, including sophisticated critical infrastructures. Indeed, the widespread integration of Cyber-Physical Systems in vital infrastructures has increased their significance in sustaining economic growth, and their stability and durability have

become essential in all facets of modern life [7] [8]. Security incidents and component faults are two of the biggest abnormalities that can disrupt CPS's daily function. Since CPS are so essential to contemporary society's day-to-day activities, they've become a tempting choice for cybercriminals. Because of their extensive use, their attack surface has grown significantly [9]. Various components of the CPS, like every other physical control device, will malfunction at the same time. Both faults and attacks can cause the machine to behave abnormally, but the consequences can be somewhat different. CPS operators may select the appropriate rehabilitation actions that mitigate the detrimental consequences of irregular behavior as they can differentiate [10]. Defining the criteria that could lead to such distinction is a difficult challenge that necessitates a thorough examination of individual components in a CPS structure before arriving at a holistic solution [11] [12].

A malfunction that influences any of CPS's components will cause it to behave abnormally (nodes). Fault detection in CPS has proven to be a difficult challenge due to the system's complexity and large size, as well as the fact that flawed activity is a complex and diverse problem [13]. Traditional CPS fault detection methods focus on the operator's knowledge, while more recent approaches, which characterize the modern IoT age, rely on sensor and alarm data. Machine learning methods and human expertise are combined in certain IoT solutions for fault diagnosis [14] [15]. Synthetic neural networks, for example, are used in defect detection in power and smart grid systems because they are adaptable systems inspired by organic systems. Radial Basis Function and Support Vector Machines are two popular methods in artificial neural networks. Other methods [16] make use of logic to avoid latent faults that can occur when a stable environment is caused by a control system for a failure condition. Existing CPS security procedures are usually classified according to the security triad of secrecy, transparency, and availability [17] [18]. A security reason is frequently linked to the right mitigation measures that are looking for an adversary to safeguard a cps machine defined by a certain device version.

The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or Ransomware. When tested, we use trained information or a data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of the input. When the model identifies the attacker node, it is removed via the BAIT technique from the network.

2. OBJECTIVES OF THE PROPOSED WORK :

From cyber-attacks, cyber defense ensures the secrecy of computer-linked structures, software, hardware, and data. Without a security policy in place, an attacker can easily gain access to your device and misuse your personal information, client information, business intelligence, and much more. This analysis is being completed with the goal of better understanding the definitions of cybercrime and cyber security, as well as proposing effective and appropriate therapies to address these issues in today's internet world. Similarly, the purpose of the examination is to give a framework for brand spanking new analysis possibilities. The following items are essential for achieving the desired result:

- (1) To review the recent cyber-attack system, and also to define the clear problem statement on the same aspect.
- (2) To introduce a new cyber-attack detection, particularly focusing on anomaly behavior from attacks like DDoS and ransomware attacks.
- (3) To introduce the deep ensemble technique for detecting the presence of attack in the network and also to mitigate it using the BAIT approach.
- (4) To process the BAIT model for mitigating the attacker from the network.
- (5) To assess the feasibility of the proposed system concerning certain performance metrics against other state-of-the-art frameworks.

3. OVERVIEW OF SYSTEMATIC LITERATURE REVIEW METHODOLOGY :

The review of literature is an important procedure that offers a strong foundation for the growth of knowledge. It makes it easier to look at areas where more research is needed [5]. The goal of this project is to undertake a comprehensive review of the literature to provide current research solutions for the development of a cyber-assault detection and mitigation device. To create a literature review framework, we used Kitchenham's [4] systematic literature review tips. The process for conducting a literature review to address the study's objectives is discussed in the subsections that follow. In the following subsections, the literature assessment framework outlines the questions for studies to

consider, the technique for discovering relevant studies, the selection of studies to include in the literature overview, the evaluation of reviewed articles, and the synthesis of study findings.

3.1 Research Queries for Study:

The following research questions were derived from the goals of the literature review and were concerned in responding to the following research problems:

Q1: What are the various tactics for detecting and mitigating cyber-attacks?

Q2: What are the most up-to-date ways for imposing a model for detecting and mitigating cyber-attacks?

Q3: What are the research gaps in cyber-attack detection and mitigation strategies?

3.2 Search strategy:

This section covers the method for generating search keywords, the search approach, the scanned databases, and seeking literature.

3.2.1 Look for keywords and approach:

The keywords we chose for our search were identified from previous experience in the field of study. The key database search string is "cyber-attack detection and mitigation" to raise awareness of the many processes that go into place to detect cyber-attacks.

3.2.2 Database searches:

We developed a list of probable databases for laptop technological know-how study using the Google search engine. The following indexed databases were searched:

- Research Gate
- IEEE Xplore
- Science Direct
- Google Scholar

Non-refereed papers were excluded because the database search option allows for a more advanced search, and we may also want to limit papers by the problem to laptop science. Between January 2001 and December 2021, the search was carried out.

3.3 Three selections of observers:

This phase indexes the technique and specific documentation used to select studies for a systematic literature evaluation for enforcing a model of attack detection and mitigation.

3.3.1. Method of deciding what to look at:

Three steps of selection are used to select papers for inclusion in the systematic literature review. (1) Preliminary research selection based on name; (2) research selection technique mostly based on evaluating the abstract concept; and (3) Research selection procedure primarily based on reviewing the abstract concept. (4) Fourth method of selection is based on the general content of the article. The range of articles being reviewed at each stage of the choice procedure is shown in table 2.

Table 2: shows the number of papers reviewed at each stage of the selection process.

Stages	Selection Process	Total Papers
Phase 1	Based on the title	632
Phase 2	By reviewing the abstract concept	153
Phase 3	By reading the full article	75
Phase 4	Studies selected	28

Except for convention proceedings, we started with 632 papers from the database search in section 1 and selected 153 papers for the next section of paper screening. In section 3, 75 papers had relevant ideas that necessitated a thorough reading of the articles, and 28 papers were chosen as the very last to be reviewed.

3.3.2. Documentation of the studies chosen:

Before the selection of papers for review, redundant papers were identified using advanced database keyword searches. Studies research assessed at each aspect of the screening system were documented

in distinct spreadsheets in the excel spreadsheet utility for each segment of the decision technique. Non-refereed publications were eliminated because the database search option allows for a more advanced search, and we may also want to limit papers by the problem to laptop science. Between January 2003 and December 2021, the search was carried out.

3.4 Three options for observation:

This phase indexes the method and documentation used to select research for a comprehensive literature evaluation for imposing a model of attack detection and mitigation.

3.4.1. Choosing a look is done in a certain way:

Three steps of selection are used to select papers for inclusion in the systematic literature review. (1) Preliminary research selection based on name; (2) research selection technique mostly based on evaluating the abstract concept; and (3) research selection procedure primarily based on reviewing the abstract concept.

4. OVERVIEW OF RELATED WORK :

This section gives an extensive review of the cyber-attack detection and mitigation system:

Zhe et al. [19] proposed an RNN-based kingdom reconstruction approach for state estimation of nonlinear strategies after the discovery of cyber-assaults on sensor data in 2020. The suggested approach was adopted to detect cyber-attacks in closed-loop operations using machine-learning-based detection systems, and an RNN model was created to recreate process states using fraudulent state measures to quantify control behavior. The RNN-based configuration re-creator was used in real-time inside LMPC and LEMPC to give correct balance analysis and ensure closed-loop consistency of the nonlinear techniques upon cyber-assault detection. Using a chemical procedure context and min-max, surge, and geometric cyber-attacks, the country's re-efficacy constructors in reassembling system states for both LMPC and LEMPC were demonstrated.

Georgios et al. [20] investigated an Energy-Aware Smart Home system's internal connectivity climate in 2020. In EASH, the issue of distinguishing between equipment failure and network attacks was described in terms of their impact on communication. The relationship between these abnormality sources was shown, and a machine learning-based architecture for the differentiation issue was developed. The suggested method was calibrated in both a simulation and a real-time testbed setting, and it demonstrated a positive classification performance of over 85%. Obtained from experimental findings, a quantitative description of the considered classes was given, as well as functionality used in the suggested method to increase classification accuracy.

In 2018, Wang et al. [21] proposed a two-stage sparse cyber-assault model for smart grids with complete and partial network data that was situation-based. The presented cyber-attacks were successfully detected, and a unique security technique based on interval nation estimation was implemented. To maximize the function variable's variance cycles, the top and decreasing limits of each country variable were represented as a twin optimization issue using this strategy. Furthermore, the stacked auto-encoder, a well-known deep learning set of rules, was used to collect nonlinear and non-stationary data in electric-powered load outcomes. Such features were then used to increase predictive performance for electric loads, resulting in state variables with a narrow width. A parametric Gaussian distribution was used to represent the variance of forecasting errors. Comprehensive studies on numerous IEEE benchmarks have been used to show the validity of the current cyber-attack models and security mechanisms.

In 2019, Defu et al. [22] proposed a device learning-based completely attack detection version for energy structures that was taught using data and logs obtained via phasor size units. The findings demonstrate that the data processing method could increase the model's precision, and the AWV model could efficiently identify 37 different types of power grid behaviors. The feature development engineering was completed, and the data was then sent to various machine learning models, with the random forest being selected as AdaBoost's simple classifier. Finally, various comparison criteria were used to equate the proposed model to other ones. The experimental findings show that this model can reach a 93.91 percent accuracy rate and a 93.6 percent identification rate, which is better than eight recently established techniques.

In the year 2020, Perez et al. [23] suggested a flexible modular architecture for detecting and mitigating LR-DDOS threats in SDN environments. The intrusion detection system was trained in the structure using six system mastering (ml) models, and their overall performance was assessed using the dos dataset from the Canadian Institute of Cybersecurity. Despite the challenges of detecting LR-

DoS attacks, the results of the analysis show that this approach accomplished a detection rate of 95%. The eminent virtual gadget's OS controller is utilized to keep our simulated environment as close to genuine production networks as possible. All attacks experienced by the intrusion prevention detection device inside the testing topology are mitigated by the intrusion prevention detection device. This demonstrates how effective our system is at recognizing and stopping LR-DDOS attacks.

The unattended detection of anomalies based on the statistical correlation between measurements was proposed by Karimipour et al. [24] in 2019. The objective of the adopted model was to develop a configurable anomaly detection engine for high-scale intelligent networks that distinguished between an actual failure and a disorder and an intelligent cyber-attack. To reduce computation complexity while finding causal relationships across subsystems, the strategy presented utilizes symbolic dynamic filtering. The simulation results of IEEE 39, 118, and 2848 bus structures confirm the approach's performance under a variety of operating situations. The findings demonstrate that 99% of the positive and false-positive rates are genuinely positive and less than 2%.

In 2020 Wei et al. [25] established a recovery strategy for the optimal re-closure of the trickled transmission lines. In specific, a framework for deep strengthening learning (RL) has been created to enable the strategy to adapt the unpredictable cyber-attack scenarios and to take decision-making capabilities in real-time. In this context, an environment has been created for simulating energy device dynamics and generating training data during the assault-recovery process. The profound RL strategy to determine the optimal lock-up time was trained with this information. Numerical outcomes demonstrate that the approach utilized would minimize cyber-attack effects in different circumstances. Ismail et al. [26] investigated energy theft inside the dg domain in the year 2020. In this attack, malevolent clients hack the smart meter to monitor their renewable dg devices and exploit their records so that it declares more power to the grid. Deep system learning has been investigated as a means of detecting such harmful behavior. This research found that combining dg smart meters, weather reviews, and SCADA metering parameters in a deep co-evolutionary-neural network yields the greatest detection rate (99%) and the lowest false alarm rate ($\approx 0\%$).

5. IDEA BEHIND IMPLEMENTATION OF A CYBER ATTACK DETECTION AND MITIGATION MODEL :

It's becoming more difficult to prioritize and respond to threats as there are more digital operations and a more complex threat landscape. The consequences of an event are extended to third parties and the cloud through digital transformation. As a result, with threat identification and remedy integrations, it is critical to include integrated hazard control as part of the mitigation strategy. Before displaying unusual actions that could suggest a compromise, ML algorithms learn about their environment and organize baseline norms. However, if the cy is continually reinventing itself to meet business agility needs and the dynamic environment lacks a consistent baseline, the set of rules will be unable to establish what is normal and will raise red flags for seemingly innocuous behaviors. The most common critique of ml-detection software is the "impossible" number of signs it generates thousands of alarms each day, thereby handing out a denial-of-service attack to analysts. While a real alert will make its way to a security analyst's queue, this effective correlation will take the arrival of a black box and leave nothing more than a ticket that says "alert." From there, an analyst will have to sift through logs and activities to figure out what caused the movement.

6. CURRENT APPROACHES FOR IMPLEMENTING CYBER ATTACK AND DETECTION MODEL :

Table 1 shows the reviews on cyber-attacks-based machine learning techniques. Initially, the RNN model was deployed in [19], which presents small deviation, reliable correction, and maximum destabilizing effects; however, the starting state reconstruction was not limited. ANN classifier [20] was used to increase the classification performance, low energy failure, and less packet drop failure, but the proposed study stated that the outcomes of the classification should be changed to include/remove attributes from descriptive datasets. Moreover, a stacked auto-encoder (SAE) model was deployed in [21] that offers high detection accuracy, MAPE, and robustness. However, an algorithm for the solution of the L0-norm minimization problem must be created. Likewise, the AWW model was exploited in [22], which offers a better classification effect, high accuracy, improved precision, maximum recall, and higher F1 score. However, the related data must be increased and a deep learning model combined with big data analytics must be created. The SDN model has been used

in [23] with maximum accuracy, false alarm rate, high precision, improved retrieval, and maximum F1; but the proposed model does not include newer Machine Learning or deep learning techniques. In addition, the DBN model was introduced in [24], which offers better accuracy, true positive rate, and less FPR. However, the proposed scheme's success rate does not depend on the attack scenarios. Deep reinforcement learning (RL) framework was suggested in [25] that offers to minimize cyber-attack impacts, low MSE, and improve the system stability. However, the training data did not include the data produced in Scenario 1 and Scenario 2. Finally, in [8], the hybrid C-RNN detector model offered the lowest detection rate and false alert but the solidity of the adopted detector against new cyber-attacks was seen not in the training period of the detector. For cyber-assaults-based entire system mastering tactics in the gift to work effectively, such constraints must be taken into mind.

Table 1: summary of current approaches being used in cyber-attacks detection and mitigation

Author	Adopted methods	Features	Challenges
Zhe <i>et al.</i> [2020][19]	RNN model	<ul style="list-style-type: none"> • Small deviation • Reliable correction • Maximum destabilizing effects 	<ul style="list-style-type: none"> • The starting state reconstruction was not limited.
Georgios <i>et al.</i> [2020] [20]	ANN classifier	<ul style="list-style-type: none"> • Improved classification accuracy • Low Energy Failure • Less Packet Drooped failure 	<ul style="list-style-type: none"> • The classification findings will benefit from the addition/removal of features from the illustrative datasets.
Wang <i>et al.</i> [2018] [21]	SAE model	<ul style="list-style-type: none"> • High detection accuracy • MAPE • Robustness 	<ul style="list-style-type: none"> • The development of an algorithm to solve the L0-norm minimization problem must be prioritized.
Defu <i>et al.</i> [2019][22]	AWV model	<ul style="list-style-type: none"> • Better classification effect • High accuracy • Improved precision • Maximum recall • Higher F1 score 	<ul style="list-style-type: none"> • The amount of relevant data must be increased, and progress on a deep learning platform that is integrated with Big Data analytics must be undertaken.
Pérez <i>et al.</i> [2020] [23]	SDN model	<ul style="list-style-type: none"> • Maximum accuracy • False alarm rate • High precision • Better recall • Maximum F1-measure. 	<ul style="list-style-type: none"> • The proposed model did not incorporate the more recent ML and deep learning strategies.
Karimipour <i>et al.</i> [2019] [24]	DBN model	<ul style="list-style-type: none"> • Better accuracy • True positive rate • Less FPR 	<ul style="list-style-type: none"> • The proposed scheme success rate does not depend on the attack scenarios.
Wei <i>et al.</i> [2020] [25]	Deep RL framework	<ul style="list-style-type: none"> • Minimize cyber-attack impacts • Low MSE • Improve the system stability 	<ul style="list-style-type: none"> • The training facts no longer included the statistics created in scenario 1 and state of affairs 2.
Ismail <i>et al.</i> [2020] [26]	Hybrid C-RNN detector model	<ul style="list-style-type: none"> • Highest detection rate • Lowest false alarm 	<ul style="list-style-type: none"> • The resilience of the following detector was put to the test in opposition to fresh cyber-attacks that were not existent at the time of the detector's training.

7. RESEARCH GAP :

The internet has evolved into a key infrastructure for both businesses and individual users, and its security has become a major concern. Protection is also a significant component in inspiring the purchaser confidence required to achieve commercial success for the new technologies that are emerging in today's connected world. Regression may be used to solve fraud detection in cybersecurity. It determines fraudulent transactions once a model is discovered from the historical transaction database, mostly based on observable attributes of recent transactions. System analysis methodologies are commonly used to solve a variety of cybersecurity issues. Advances in the realm of device understanding and deep mastery have the potential to provide viable answers to cybersecurity challenges. However, understand which set of rules is appropriate for particular usefulness. To keep the solution resistant to malware attacks and achieve high detection rates, multi-layered processes are required. When it comes to resolving cybersecurity difficulties, the choice of a selected version is crucial.

Research gap 1: ANN classifier method entails evaluating online data sets to solve the problem of malicious attack detection. This is accomplished by utilizing an iteratively naïve Bayesian classifier. Active learning, on the other hand, allows the problem to be solved using a limited set of specified data points, which are also very expensive to obtain.

Research gap 2:: Any statistically-based fully discriminating technique must effectively describe the baseline network conduct, which is extremely difficult to do given the dynamic nature of today's networks. Person conduct modeling tactics are a problem in almost all of the jobs. Data mining of internet server logs to simulate the baseline surfing behavior of genuine users is a time-consuming and error-prone task.

Research gap 3: The public of the available replies is mere of educational relevance because they are aware of detecting DDOS attacks with a high detection rate or a low false alarm rate. Only a few of these have been put into practice in real-time.

Research gap 4: Some academics have attempted to employ simulation and emulation-based research to synthesize datasets using a set of benchmark DDOS attack gear, however, those datasets are missing important site visitor elements. In an ideal world, the collected community hint would contain a balanced mix of practical heritage traffic and assault site visitors, with no preference for one type of traffic over the other. However, because there is no established formula for effectively modeling net visitors, it is difficult to ensure a proper mix of regular and assaultive visitors in a real-world dataset.

8. METHODOLOGY :

The Cyber-Physical System (CPS) connects the physical and electronic worlds and is typically used for industrial manufacturing control systems (ICS) to allow people to understand all types of necessary information in real-time. The use of CPS in places like power generation grids and waste-water treatment plants has a lot of promise. However, CPS security concerns are distinct from conventional cybersecurity concerns in that they concern confidentiality, integrity, and availability. This proposal intends to introduce a novel DDoS and ransomware attack detection as well as a mitigation model. The input data is first subjected to the identification process, which distinguishes the types of attacks as well as detects their presence. The detection phase will include feature extraction and attack detection. Flow-based features like flow rate, flow byte, total forward packet, and total backward packet are extracted from the raw data collected. Moreover, the sequential frequent pattern features are extracted using the Apriori framework. To make the detection more precise, an ensemble classifier will be constructed by enclosing the Support Vector Machine 1 (SVM 1), SVM 2, and Neural Network (NN) and optimized Deep Convolutional Neural Network (DCNN). The ensemble classifier's SVM 1, SVM 2, and NN will be trained with the extracted features. Then, the outcome from SVM 1, SVM 2, and NN will be fed as input to optimized CNN, whose weights will be fine-tuned via a new hybrid optimization model such as SeaLion Optimization (S) algorithm and Whale Optimization Algorithm (WOA). EHO [27] is a modern swarm-based meta-heuristic search approach that is motivated by elephant communities led by a female matriarch. WOA [28] is a modern optimization strategy for solving optimization problems that use three operators to mimic humpback whale foraging activity such as searching for food, encircling prey, and using bubble nets. The suggested work's design is shown in Figure 1.

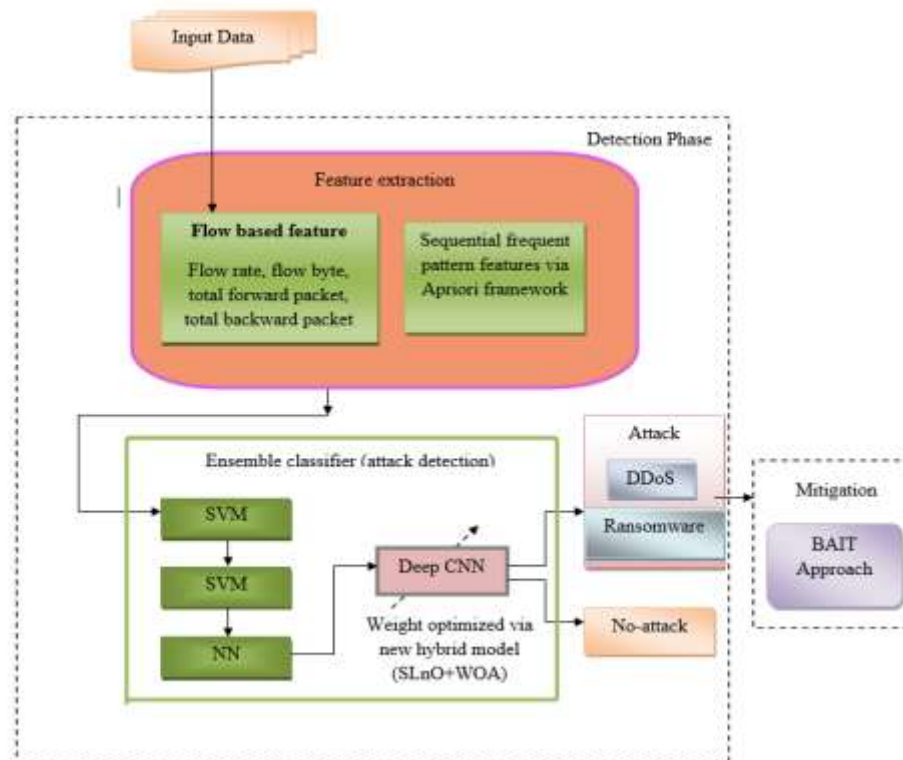


Fig. 1: Architecture of proposed work [29]

9. EXPECTED OUTCOME OF THE PROPOSED STUDY :

The suggested model, which is based on cyber-attacks and uses machine learning methods, will be simulated in MATLAB, and an experiment will be conducted. The proposed model would be compared to other state-of-the-art models in terms of accuracy, recall, precision, false alarm rate, and F1measure, among other metrics.

10. CONCLUSION :

The majority of current intrusion detection algorithms are unable of dealing with the dynamic and complicated nature of cyber-attacks on laptop networks. As a result, green adaptive strategies such as various gadget researching techniques can result in decreased false alarm rates, greater detection costs, and reasonable calculation and verbal exchange fees. The work has proposed a novel approach of BRELU-ResNet based Cyber-Attack Detection System with a BAIT-based approach for mitigation. This approach involved several operations for the efficient detection of cyber-attacks. Overall, the proposed cyber-assault detection methodology outperforms current state-of-the-art methodologies and is more reliable and robust. The study may be expanded in the future with a few more advanced neural networks, as well as a focus on specific sorts of rational attacks.

REFERENCES :

- [1] Samy, A., Yu, H., & Zhang, H. (2020). Fog-based attack detection framework for the internet of things using deep learning. *IEEE Access*, 8(1), 74571-74585.
[Google scholar](#)
- [2] Subroto, A., & Apriyana, A. (2019). Cyber risk prediction through social media big data analytics and statistical machine learning. *Journal of Big Data*, 6(1), 1-19.
[Google scholar](#)
- [3] Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning. *Human-centric Computing and Information Sciences*, 9(1), 1-22.
[Google scholar](#)

- [4] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H. & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6(1), 35365-35381.
[Google scholar](#)
- [5] Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, 7(3), 366-370.
[Google scholar](#)
- [6] Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, 96(1), 227-242.
[Google scholar](#)
- [7] Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for the internet of things in a smart city. *Future Generation Computer Systems*, 107, 433-442.
[Google scholar](#)
- [8] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with a cyber-attack detection model in mobile edge computing systems. *IEEE Access*, 8(1), 185938-185949.
[Google scholar](#)
- [9] Hussain, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for the cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics*, 17(2), 860-870.
[Google scholar](#)
- [10] Aamir, M., & Zaidi, S. M. A. (2021). Clustering-based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, 33(4), 436-446.
[Google scholar](#)
- [11] Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in the industrial control system. *IEEE Access*, 8(1), 83965-83973.
[Google scholar](#)
- [12] Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). An ensemble of deep recurrent neural networks for detecting IoT cyberattacks using network traffic. *IEEE Internet of Things Journal*, 7(9), 8852-8859.
[Google scholar](#)
- [13] Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications*, 10(1), 1-22.
[Google scholar](#)
- [14] Ibor, A. E., Oladeji, F. A., Okunoye, O. B., & Ekabua, O. O. (2020). The conceptualization of Cyberattack prediction with deep learning. *Cybersecurity*, 3(1), 1-14.
[Google scholar](#)
- [15] Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyberattacks rates. *EURASIP Journal on Information security*, 2019(1), 1-11.
[Google scholar](#)
- [16] Beno, M. M., I. R, V., S. M, S., & Rajakumar, B. R. (2014). Threshold prediction for segmenting tumors from brain MRI scans. *International Journal of Imaging Systems and Technology*, 24(2), 129-137.
[Google scholar](#)

- [17] Wang, H., Ruan, J., Ma, Z., Zhou, B., Fu, X., & Cao, G. (2019). Deep learning aided interval state prediction for improving cyber security in the energy internet. *Energy*, 174, 1292-1304.
[Google scholar](#)↗
- [18] Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, 1(1), 61-67.
[Google scholar](#)↗
- [19] Wu, Z., Chen, S., Rincon, D., & Christofides, P. D. (2020). Post-cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, 159(1), 248-261.
[Google scholar](#)↗
- [20] Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber-physical systems using machine learning. *Microprocessors and Microsystems*, 77(1), 103121.
[Google scholar](#)↗
- [21] Wang, H., Ruan, J., Wang, G., Zhou, B., Liu, Y., Fu, X., & Peng, J. (2018). Deep learning-based interval state estimation of AC smart grids against sparse cyber-attacks. *IEEE Transactions on Industrial Informatics*, 14(11), 4766-4778.
[Google scholar](#)↗
- [22] Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of information security and applications*, 46(1), 42-52.
[Google scholar](#)↗
- [23] Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). Flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8(2), 155859-155872.
[Google scholar](#)↗
- [24] Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 7(1), 80778-80788.
[Google scholar](#)↗
- [25] Wei, F., Wen, Z., & He, H. (2019). Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. *IEEE Transactions on Smart Grid*, 11(3), 2476-2486.
[Google scholar](#)↗
- [26] Ismail, M., Shaaban, M. F., Naidu, M., & Serpedin, E. (2020). Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, 11(4), 3428-3437.
[Google scholar](#)↗
- [27] Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing DDoS attacks and flash events: Review, research gaps, and future directions. *Computer Science Review*, 25(1), 101-114.
[Google scholar](#)↗
- [28] Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. *Online Information Review*, 41(2), 171-184.
[Google scholar](#)↗
- [29] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with the deep hierarchical network. *IEEE Access*, 8(1), 32464-32476.
[Google Scholar](#)↗

A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with BAIT Based Approach for Mitigation

Sangeetha Prabhu¹ & **Nethravathi P. S.**²

¹ Research Scholar, College of Computer Science and Information Science, Srinivas
University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

² Professor, College of Computer and Information Sciences, Srinivas University, Mangalore,
India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

Subject Area: Computer Science.

Type of the Paper: Research analysis.

Type of Review: Peer Reviewed as per [C|O|P|E](#) guidance.

Indexed In: OpenAIRE.

DOI: <https://doi.org/10.5281/zenodo.6530129>

Google Scholar Citation: [IJAEML](#)

How to Cite this Paper:

Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with BAIT Based Approach for Mitigation. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 243-258. DOI: <https://doi.org/10.5281/zenodo.6530129>

International Journal of Applied Engineering and Management Letters (IJAEML)

A Refereed International Journal of Srinivas University, India.

Crossref DOI : <https://doi.org/10.47992/IJAEML.2581.7000.0134>

Received on: 10/04/2022

Published on: 10/05/2022

© With Authors.



This work is licensed under a [Creative Commons Attribution-Non-Commercial 4.0 International License](#) subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with BAIT Based Approach for Mitigation

Sangeetha Prabhu¹ & Nethravathi P. S.²

¹ Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

² Professor, College of Computer and Information Sciences, Srinivas University, Mangalore, India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

ABSTRACT

Purpose: *Industrial Control Systems become more vulnerable to digital attacks by merging communication groups and the Internet of Things, which could have severe implications. An Intrusion Detection System is essential in IoT businesses for identifying and stopping assaults. To ensure data privacy and security in the face of digital attacks, legislation and large enterprises should develop network security policies today. As people-based full frameworks have become more vital in today's society, they've also become targets for hostile activities, compelling both industry and research to concentrate more on dealing with local area disruption recognition issues. Contraption reviewing techniques have shown to be effective tools for resolving in-network interruption location issues.*

Design/Methodology/Approach: *This investigation yielded a very unique strategy for tackling hub moderation utilizing a Classification and Encryption method. The UNSW-NB15 dataset is acquired and divided into Data for preparation and testing from the start. The information is pre-handled and included are eliminated right away within the preparation time frame. The TWM Algorithm is then used to determine the relevant highlights from that moment onward. The BRELU-RESNET classifier then sorts the input into went after and non-went after categories. The compromised information is then saved in the security log record, and the typical data is encrypted using the ESHP-ECC computation. The shortest path distance is then calculated using Euclidean distance. Finally, the data is available. Finally, using the DSHP-ECC computation, the information is decrypted. If the information is available in the log document during testing, it is regarded as the sought-after data and is prevented from the transmission. If it is not present, then the process of digital assault recognition begins.*

Findings/Result: *The research is based on the UNSW-NB 15 dataset, which shows that the proposed method achieves an unreasonable awareness level of 98.34 percent, particularity level of 77.54 percent, exactness level of 96.6 percent, Precision level of 97.96 percent, review level of 98.34 percent, F-proportion of 98.15 percent, False Positive Rate of 22.46 percent, False Negative Rate of 1.66 percent, and Matthew's connection coefficient of 77.38*

Originality/Value: *This experimental-based research article examines the malicious activities in the cyberspace using BRELU-RESNET approach and mitigated by using BAIT based approach mechanism.*

Paper Type: *Research Analysis.*

Keywords: Cyber-attack detection, BAIT approaches, Feature Extraction, BRELU-RESNET, Attack node mitigation

1. INTRODUCTION :

Electrical and mechanical equipment, computers, and human-supervised manual processes make up industrial control systems (ICSs) [1]. They are mostly employed in industrial facilities and vital

infrastructures, such as manufacturing sectors, chemical plants, electricity production, distribution networks, and others [2, 3]. Their activities have direct consequences on the environment, human safety and health, the economy, and national security [4]. In ICS, because data is often delivered across a wired or wireless network, it is extremely vulnerable to being tampered with by malevolent attackers. [5]. Furthermore, the incorporation of the IoT in ICSs allows hackers to exploit system weaknesses to conduct cyber-attacks [6, 7]. Typical cyber-attacks against ICSs include DoS, Man in the middle attack, SQL injections, Password attacks, Phishing, and so on [8]. By influencing and disturbing the physical process, cyber-attacks against ICSs are primarily aimed at causing damage or catastrophe (such as a hazardous accident or output loss) [9]. Attack detection systems are meant to avoid such assaults by effectively monitoring events in an information system and identifying signals of security vulnerabilities [10]. The most widely used strategy for attack detection is anomaly detection, which is the act of discovering abnormal occurrences or unexpected system behavior [11-12]. However, the majority of these algorithms have only been trained on particular sorts of assaults and are unable to identify unknown or novel attacks [13].

Hence, to overcome these challenges and risks faced during attack detection, various anomaly detection algorithms are introduced. These approaches are integrated and implemented by using a variety of Machine Learning algorithms [14]. However, the majority of available algorithms ignore the unbalanced structure of ICS datasets, In real-world contexts, this leads to low detection rates or high false-positive rates. [15]. If the entire physical system was attacked at the same time, several of the present approaches would be ineffective [16]. Much research on fault-tolerant control has been conducted, and these studies can also give tools for attack-resilient control [17]. When it comes to evading surveillance and isolation, there are a few things to keep in mind, however, there are significant variations between fault-tolerant controls and attack-resistant which necessitates the use of particular approaches to solve security challenges in ICSs [18]. Thus, to offset the aforementioned problem, the work has proposed a framework called a novel approach of BRELU-ResNet based Cyber-Attack Detection System with BAIT based approach for mitigation, which guarantees the accurate detection of cyber-attacks and retains more authenticity of the network.

2. LITERATURE REVIEW :

According to the defense-in-depth strategy, Fan Zhang et al. [19] created a cyber-attack detection system that utilized data from the network, data from the host system, and data from the measured process characteristics. A multi-layer attack detection system was available saving the defenders valuable time before the physical system's unrecoverable repercussions occurred. The classic intrusion prevention layer, which included firewalls, data diodes, and gateways, was the initial protection layer. The second tier of securities ty comprised of data-driven algorithms for detecting cyber-attacks using system data and network traffic. M1 represented the classification model, while M2 denoted the big data analytics models. When attacks induced behavior divergence from normal functioning, early identification of intruders was possible with M1 and M2. If the second security measure fails to match suspicious attacks, the final security checkpoint examines the processed data and uses M3's modeling techniques to discover anomalous processes that could be triggered by a cyber-attack. The technique discovered physically damaging cyber-attacks before they had a substantial impact, according to the findings. The approach, however, was unsuccessful against modern cyber-attacks.

Abdulrahman Al-Abassiet al. [20] proposed a deep learning approach for creating balanced representations of unbalanced datasets. The representations were input into a deep learning ensemble model for detecting attacks that were created particularly for an ICS setting. Multiple unsupervised SAEs were used in the novel representations using a deep learning model from unbalanced datasets. Multiple Auto-Encoders (AE) were used in the SAE attack detection model to extract new representations from unlabelled input, resulting in various patterns. New representation from every SAE was then fed to a DNN and fused with the use of a fusion activation vector utilizing a super vector. Finally, a DT was used to distinguish models that have recently been combined and are launching attacks as a binary classifier. The strategy beat previous models that have been published in the literature, according to the findings. However, the approach was limited by a lack of backup capabilities.

Moshe Kravchik et al. [21] used 1 Dimensional Convolution Neural Networks (1D CNNs), which are classified as complete autoencoders), variation autoencoders (VAEs), and PCA, to create a technique to identify anomalies and cyber-attacks at the physical level Industrial control systems (ICS) data. In

addition, the Kolmogorov-Smirnov test was used to identify features, and the frequency components of the time-domain signals were converted and represented using a short-time Fourier transform and energy binning, and the system was modeled both in terms of duration and frequency. The approach was tested on three widely used public datasets, and the findings demonstrated that it was resistant to such evasion assaults. The attacker was obliged to forego the desired physical to prevent influencing the system discovery. However, the concept was limited by its high energy use.

Nevius Kaja et al. [22] developed a two-stage intelligent Detection Mechanism that could detect and prevent such attacks. The solution included a two-stage design based on ML methods. The work's originality was the employment of a two-stage machine learning approach in the building of IDS after four-step efficient information pre-processing. The IDS employed K-Means to identify the attacks in the initial stages, then supervised learning during the second phase to classify the assaults and reduce the number of false positives. The approach's implementation resulted in computationally efficient IDS capable of detecting and classifying assaults with increased precision while lowering the number of erroneous positives. The IDS outperformed the present in terms of technology and state-of-the-art performance. The method, however, exhibited poor detection rates and a significant percentage of false positives.

To detect intrusions, Kaiyuan Jiang et al. [23] offered a hybrid sampling and deep hierarchical network technique for network intrusion detection. To decrease noise trends in the general category, the One-Side Selection (OSS) method was used, followed by the Synthetic Minority Oversampling Technique to improve the minority samples (SMOTE). As a consequence, a balanced dataset was constructed, allowing the system to completely comprehend the characteristics of extracted features while reducing model time training. Second, to obtain spatial characteristics, a Convolution Neural Network (CNN) was employed, and a Bi-directional long short-term memory (Bi-LSTM) was used to retrieve temporal features, leading to a deep hierarchical network model. The NSL-KDD and UNSW-NB15 datasets were used to validate the findings. The method, on the other hand, had a high packet loss limit and was poor at controlling network overhead. However, the concept was limited by its high energy use.

3. OBJECTIVES :

- (1) To provide the deep ensemble technique for detecting the presence of a network assault.
- (2) To create a model of the SHP-ECC procedure for removing the attacker from the network.
- (3) To compare the proposed system's practicality with other state-of-the-art frameworks in terms of specific performance criteria.

4. METHODOLOGY :

4.1 Proposed Model for Cyber-Attack Detection and Mitigation System :

The increasing incidence of cyber-physical system (CPS) assaults in recent years has raised concerns about industrial control system cybersecurity (ICS). ICS cybersecurity attempts now depend very much on firewalls, information valves, and other intrusion detection and prevention systems, which may be insufficient to withstand rising cyber threats from persistent attackers. With the use of a deep learning method, earlier research has built a framework for identifying assaults. Although the attack node in the network was discovered, it was not disabled. As a solution to this challenge, an upgraded and formidable adversary model will be presented. As a result, employing a unique Classification and Encryption approach, a novel architecture for attack node mitigation is provided in this study. The input information is usually separated into two groups: training data and testing data. The total training data is initially pre-processed. The second stage is to extract features from the input training dataset. In the third step, the feature is optimized for selecting the important Features using TWMA. Then, the feature is trained using the proposed BRELU-RESNET Classifier. Here, the classifier classifies the data into the attack and normal data. If the data is attack data, save the Source IP Address into a secure log file using the BAIT approach. Next, if the data is normal, the data is ready for transmission. In Data Transmission, first, the data is encrypted using the ESHP-ECC algorithm. Next, the shortest path distance is calculated using Euclidean distance. In Destination, the data is decrypted using the DSHP-ECC algorithm. In testing, first, the testing data is checked in the Security Log File (SLF). If the data's originating IP address is already known, the data is stopped or an attack is detected. Figure 1 depicts a block schematic of the suggested framework.

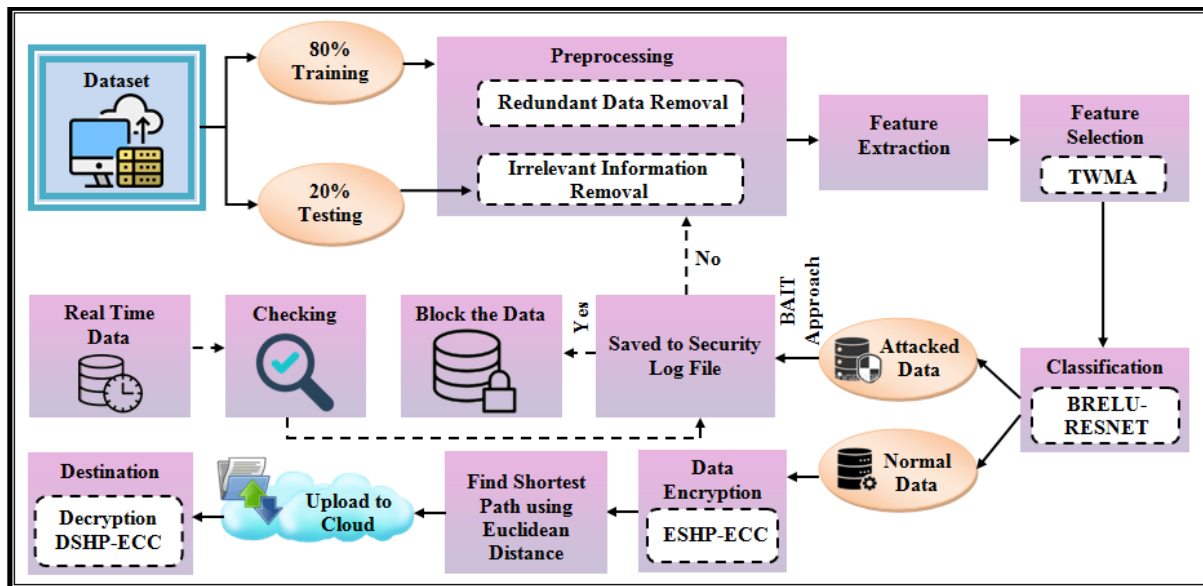


Fig. 1: The suggested cyber-attack detection and mitigation system's formwork [24]

4.2 Pre-processing :

The input dataset is separated to begin incorporating testing data and training data in the process of the cyber-attack detection technique. The data is initially in the training stage to turn the original data into data cleansing. Pre-processing is done to improve the classification's accuracy and shorten the cyberattack detection system's training period. The proposed work uses redundant data removal and irrelevant information removal as pre-processing steps.

- Redundant data means storing of same data in multiple locations. Redundant data removal is a technique to remove duplicate data from the dataset. This reduces the computational complexity and results in better generalization for the classifier [25].
- Irrelevant information removal is the process of removing the data that are not required for the detection of cyberattacks. The presence of such unrelated information may increase the processing time of the system and may result in an inaccurate attack detection rate. As a result, the system's efficiency is enhanced by removing the different data from the input dataset. The pre-processed data is then used to extract features.

4.3 Feature Extraction :

The method of extracting the number of features in a dataset by producing new features from existing ones is known as feature extraction [26]. The majority of the information from the initial set of features is contained in these additional features. Source IP address, destination port number, port number, a destination address, source bits per second, destination bits per second, transaction protocol, and so on are all extracted from the pre-processed dataset. The set of extracted features $x_{(i)}$ is mathematically articulated below,

$$x_{(i)} = x_{(1)}, x_{(2)}, \dots, x_{(n)} \quad \text{-----} \quad (1)$$

Where, n exemplifies the number of extracted features.

4.4 Feature selection by TWMA :

After feature extraction, the important features are selected using the novel Taxicab Woodpecker Mating Optimization (TWMA) technique. Woodpecker Mating Optimization (WMA) is a nature-inspired optimization algorithm developed by the mating behaviour of red-bellied woodpeckers. At the beginning of the mating period, male woodpeckers communicate with females by making a sound by pecking the trunks of the trees called drumming [27]. Depending on the quality of sound produced by the male woodpeckers, the female woodpeckers are attracted to them. Hence, the sound intensity of the male woodpeckers' drum mentions its capability to attract more female birds. By hearing the sound, the female woodpeckers move towards the male birds and the process of communication and

flow of information between them occurs. On the other hand, if the sound intensity of some other male is closer to the female, then the female bird will attract this male and move towards this male. However, the problem with WMA is slow or premature convergence due to the loss of diversity within the population. To overcome this issue, Taxicab geometry is used to update the female woodpecker's position during movement. The usage of Taxicab geometry can effectively avoid the woodpecker population falling into local optimum and also eliminates the slow or premature convergence. This enhancement made in general WMA is called TWMA. The process of TWMA is detailed as follows. **Step 1:** To begin the process of WMA, first, the woodpecker population (extracted features) is initialized as,

$$x_{(i)} = x_{(1)}, x_{(2)}, \dots, x_{(n)} \quad \text{----- (1)}$$

Where shows the woodpecker population and n is the number of woodpeckers in the population.

Step 2: After population initialization, the fitness of each woodpecker is calculated to identify the best woodpecker. Afterward, the woodpecker population is separated into male and female groups. The male birds become the search agents and the one with the highest fitness is considered as x^* (the global best solution). Here, the fitness is computed in terms of classification accuracy. The fitness evaluation $f(x_{(i)})$ is,

$$f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)}) \quad \text{----- (2)}$$

Step 3: Next, the sound intensity of the woodpecker is calculated using the below equation,

$$\delta = \frac{2\pi^2 \gamma^2 A^2 DS}{\Psi} \quad \text{----- (3)}$$

In equation (3), δ represents the sound intensity, γ indicates the sound frequency, A specifies the sound amplitude, D signifies the density of the medium in which sound is traveling, S illustrates the sound speed and Ψ mentions the area of sound.

Step 4: The sound intensity of the woodpecker may change based on the source of the sound. Some sources may emit the sound in one direction. Consider a sphere in the region of a source with a radius t , and then all the sound waves will pass through the surface of the sphere. Thus, the sound intensity (δ) in equation (3) becomes,

$$\delta = \frac{2\pi^2 \gamma^2 \chi DS}{\Psi \cdot 4\pi t^2} \quad \text{----- (4)}$$

Here, χ defines the propagation rate of sound waves and $4\pi t^2$ determines the area of the sphere. In equation (4), sound intensity depends on the distance between source and object.

Step 5: The shortest distance between source and object mentions the better sound quality received by the female woodpecker. The Taxicab distance is used to calculate the distance between the source and object, which overcomes the problem of premature convergence and obtains the global best solution. It is given below,

$$t = \sqrt{(x_m - y_f)} \quad \text{----- (5)}$$

The above equation, x_m shows the sound source position (male woodpecker) and y_f points to the listener position (female woodpecker).

Step 6: Thereafter, the female woodpecker updates its position concerning the sound intensity of the male bird. The position updation process ($y_{f,j}^{\tau+1}$) is mathematically modeled below,

$$y_{f,j}^{\tau+1} = y_{f,j}^{\tau} + r * \frac{\alpha_{f,j}^{\tau} \left(\beta_x^{\tau} (y_x^{\tau} - y_{f,j}^{\tau}) + \beta_{m,i}^{\tau} (x_{m,i}^{\tau} - y_{f,j}^{\tau}) \right)}{2} \quad \text{----- (6)}$$

Where, $j = 1, 2, \dots, m$ shows the female woodpecker population, $y_{f,j}^{\tau}$ indicates the current position of j -th woodpecker in τ th iteration, y_x^{τ} represents the position of best woodpecker, $x_{m,i}^{\tau}$ is the position of i -th male woodpecker, r is a random number with a uniform distribution in the range

$[0, 1]$, $\alpha_{f,j}^\tau$ is a self-tuned random factor of j -th woodpecker, β^{x^*} and $\beta_{m,i}$ are the attractiveness of the female bird to the male bird.

Step 7: The self-tuning random factor $\alpha_{f,j}^\tau$ is estimated using equation (7),

$$\alpha_{f,j}^\tau = r * \eta \quad \text{----- (7)}$$

$$\eta = ts \left(1 - \frac{\tau}{\tau^{\max}} \right) \quad \text{----- (8)}$$

This equation, ts defines the tangent sigmoid function, τ, τ^{\max} models the current and maximum number of iterations respectively, α has a random value in the interval -2η to 2η . If $|\alpha| > 1$, the search agent deviates from the target, which leads to exploration, and if $|\alpha| < 1$, then the female bird joins with the male bird, which leads to exploitation.

Step 8: The attractiveness (β) of male and female woodpeckers is then calculated as,

$$\beta = (1 + \delta(i, j))^{-1} \quad \text{----- (9)}$$

In (9), $\delta(i, j)$ depicts the sound intensity of i -th male woodpecker heard by the female woodpecker. It is also called the step size of a female woodpecker because it specifies the closeness of the female woodpecker towards the male, β lies in the interval 0 and 1, the lower value defines the accurate movement of the female toward the male woodpecker.

Step 9: At each cycle, the male woodpecker population decreases, and finally, only one woodpecker will remain. A large male population increases the exploration in the initial phase. Hence, the decreasing population increases the exploitation and accuracy of the solution. The population size ($x_{m,i}$) in each iteration is computed as follows,

$$x_{m,i} = \left[\text{round} \left(\frac{n}{2} * \left(1 - \frac{\tau}{\tau^{\max}} \right) \right) + 1 \right] \quad \text{----- (10)}$$

Where, n mentions the total woodpecker population, τ, τ^{\max} models the current and maximum number of iterations respectively.

Step 10: Finally, the decreased population of woodpeckers contains one woodpecker and the global best woodpecker x^* . Thus, equation (6) can be modified as,

$$y_{f,j}^{\tau+1} = y_{f,j}^\tau + r * \left\langle \alpha_{f,j}^\tau \cdot (y_{x^*}^\tau - y_{f,j}^\tau) \cdot \beta_{m,i} \right\rangle \quad \text{----- (11)}$$

Step 11: During the movement of the female woodpecker towards the male, there is a possibility of deviation in direction; as well female birds might be attacked by other woodpeckers or hunting birds on the way. Thus, the female bird may change their path randomly to protect itself from danger. This random change in the pathway is called Run Away. This random escaping movement of the woodpecker consists of two types of movements, which are based on the sound intensity of x^* the male bird. The two types of movements (μ) are,

$$\mu = \begin{cases} R & \beta \geq \xi \\ P & \text{else} \end{cases} \quad \text{----- (12)}$$

Where, R, P specifies the runaway movement and x^* runaway movement respectively.

$$\xi = 0.8 \cdot \frac{\sum_{j=1}^{m-1} \beta_{x^*}^j}{m-1} \quad \text{----- (13)}$$

Here, ξ mentions the threshold for the sound intensity.

Step 12: The position of the female woodpecker obtained from the runway is updated below,

$$\tilde{y}_{f,j} = L - (L - U) * r \quad \text{----- (14)}$$

In equation (14), $\tilde{y}_{f,j}$ is the position of j -th the woodpecker after the runaway, r is a random number in the uniform distribution $[0, 1]$ and L, U illustrates the upper and lower bounds of variables in that order.

Step 13: The x^* runaway movement is denoted further,

$$P = \phi * \left(1 - \frac{\tau}{\tau_{\max}}\right) \quad \text{-----} \quad (15)$$

In equation (15), ϕ is the runaway coefficient. The position of a female woodpecker from x^* runaway movement ($y_{f,j}^{x^*}$) is modelled by,

$$y_{f,j}^{x^*} = y_{f,j}^{\tau} + P^{bit} \langle y_{x^*}^{\tau} - y_r \rangle \cdot B \quad \text{-----} \quad (16)$$

$$P^{bit} = \begin{cases} 1 & r \leq P \\ 0 & \text{else} \end{cases} \quad \text{-----} \quad (17)$$

The above equation, r exemplifies a random number in the uniform distribution $[0, 1]$ and B is a random number $[-1, 1]$. The process continues until the stopping criterion is met by comparing the position of i -th the woodpecker with the former position and the position of the best woodpecker. Then, the better position is replaced with the other position. Finally, the optimal solution is obtained, that is, the selected best features ($X^{(k)}$) articulated further,

$$X^{(k)} = X^{(1)}, X^{(2)}, \dots, X^{(K)} \quad \text{-----} \quad (18)$$

Where, K shows the percentage of traits that have been chosen for further study classification. The pseudocode of the proposed TWMA technique is publicized below.

Pseudocode for Proposed TWMA Technique:

Input: Extracted Features $x_{(i)}$

Output: Selected features ($X^{(k)}$)

Begin

Create the initial population of woodpeckers

Compute $f(x_{(i)}) = f(x_{(1)}, x_{(2)}, \dots, x_{(n)})$

Obtain x^* based on $f(x_{(i)})$

While (stopping condition is not satisfied) **do**

Partition $x_{(i)}$

For $1 \leq i \leq n$

Determine the sound intensity δ

Compute Taxicab distance

Choose $x_{m,i}$ (i -th male woodpecker)

Evaluate β^{x^*} and $\beta_{m,i}$

Analyze $\alpha_{f,j}^{\tau} = r * \eta$

Update woodpeckers' position ($y_{f,j}^{\tau+1}$)

Calculate sound intensity threshold ξ

If $\beta^{x^*} > \xi$

Estimate $\tilde{y}_{f,j} = L - (L - U) * r$

Else

Find out x^* runaway movement ($y_{f,j}^{x^*}$)

End if

Appraise the new position of $y_{f,j}$

Renew x^*
 End for
 $\tau = \tau + 1$
 End while
 Obtain global best solution $(X^{(k)})$
 End

4.5 Classification by means of BRELU-RESNET classifier :

Next, the selected features $(X^{(k)})$ are fed into the BRELU-RESNET classifier to classify the attacked data from non-attacked data. ResNet is used for classification because it overcomes the problem of degradation caused due to rise in network depth [28]. Convolutional layers, batch normalization layers, max pooling, flattening layer, and activation layers are all included in ResNet's design. The selected features are inputted to the ResNet, firstly, the input is convoluted with the 2*2 filter in the convolutional layer, and it produces the output with reduced feature dimension. The outcome from the convolutional layer is then sent into the batch normalization layer, which stabilizes the network's training time while decreasing the number of timestamps. Convolutional and batch normalization are separated into three levels. The data is then sent to the max-pooling layer, which downsamples the data [29]. Finally, the fully connected layer in the network comprises of average pooling layer and softmax layer to classify the outputs. However, RESNET has an overfitting problem due to the randomized nature of the activation function. Therefore, in the proposed work, instead of random value, Bernoulli's value is used in the Leaky Rectified Linear Unit activation function in the RESNET classifier. This modification in baseline RESNET is termed as BRELU-RESNET. The general structure of the ReSNet network is cited in figure 2.

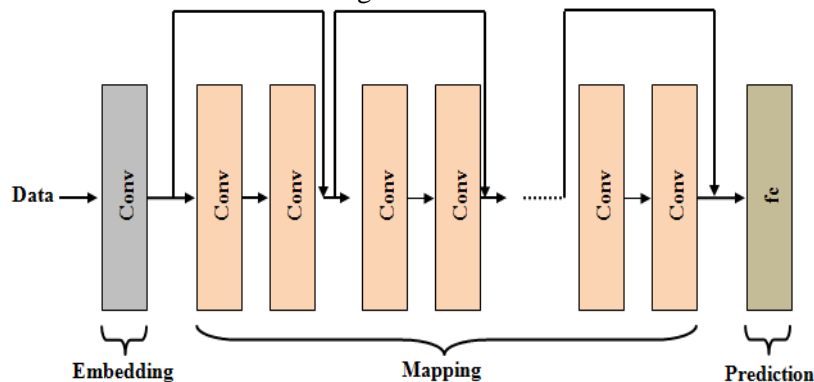


Fig. 2: RESNET architecture [24]

- Let $(X^{(k)})$ be the input features and a filter (Γ) of size (a, b) is used in the convolution layer. The convolution formula can be as seen in the equation below,

$$conv(X^{(k)} * \Gamma) = \sum_{k=1}^K (X^{(k)} - a, X^{(k)} - b) \cdot \Gamma(a, b) \quad \text{----- (19)}$$

- The activation function is an important part of neural networks. The BRELU activation function $(f(X^{(k)}))$ used in the proposed system is expressed as,

$$f(X^{(k)}) = \max(0, b(X^{(k)})) \quad \text{----- (20)}$$

Where, $b(X^{(k)})$ is known as Bernoulli's distribution function, defined by

$$b(X^{(k)}(p, o)) = p \cdot o + (1 - p)(1 - o) \quad \text{----- (21)}$$

The above equation, p, o differentiates the probability and possible outcome of $(X^{(k)})$.

- The network layers in the BERLU-RESNET are capable of approximating any function asymptotically. The approximation of residual function $\partial X^{(k)}$ is,

$$\partial X^{(k)} = f(X^{(k)}) * X^{(k)} \quad \text{----- (22)}$$

Here, $f(X^{(k)})$ is the target function which is formulated further,
 $f(X^{(k)}) = \partial X^{(k)} + X^{(k)}$ ----- (23)

Hence, the output of the classifier separates the attacked data from the normal data and then the attacked data is stored in the security log file using the BAIT approach. While the normal data is encrypted using the Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC) algorithm [30]. Next, the shortest path between each node is calculated for transferring the data in the cloud efficiently.

4.6 Attack Mitigation System Based on BAIT Approach :

The malicious node is duped into sending the erroneous route request to the decoy route request using the BAIT mechanism. The goal of this method is to both identify and mitigate attack nodes. Malicious nodes, in general, market themselves as the most efficient and quickest path to their targets. In addition, the rogue node sends the source a route request packet, which is illegal. As a result, the source node in the proposed task sends the fake request to the destination address via the nearest node. When a malicious node receives a request, it answers even if it is not the target node. This request is fed into the flow table search. After then, the attack is identified and mitigated. When a malicious node sends a response, the source node compares it to the destination address. The source node deems the node malicious and denies the response request if the addresses do not match. The data flow will continue to flow normally if no attacker nodes are found. When a route request packet arrives at a non-attack intermediate node, it is transmitted to the destination node along with the address. You may feel assured that you will transfer the data once the shortest route between the source and the destination has been determined. The test data is compared to the security log file first during the test. The data will be prohibited for further processing if the source IP address of the information is already in the security log file. The cyber-attack detection and prevention process is carried out if it does not exist in the security log file. Figure 3 depicts the BAIT approach's overall structure.

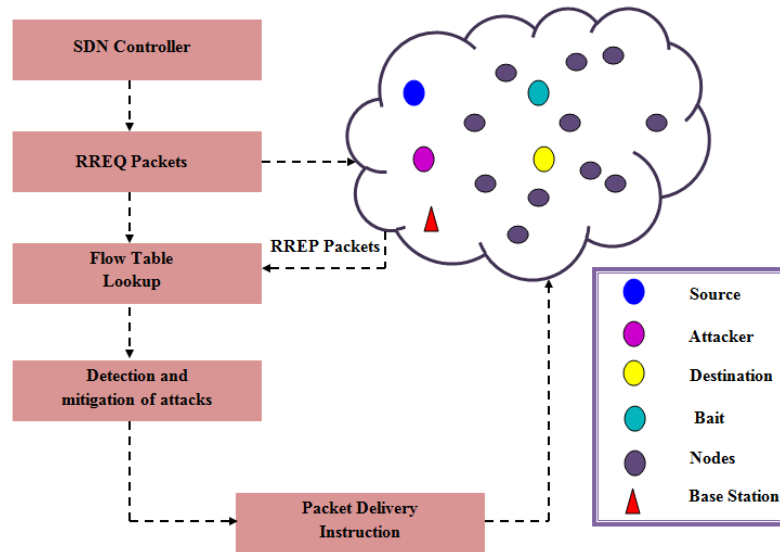


Fig. 3: General structure of BAIT [24].

4.7 Data Encryption using ESHP-ECC mechanism :

Elliptic-curve cryptography (ECC) is a public-key cryptosystem based on the elliptic curve hypothesis, which is a secure asymmetric encryption scheme used for data security. It generates public and private keys for each user through the elliptic curve properties. These keys are then used to encrypt and decrypt the data. In a conventional ECC technique, the keys are generated randomly. So, the attackers may easily hack the key information. In order to overcome this issue, the probability of ones and zeros are generated based on the randomly generated key value. Also, the key values are converted into a hash value using the secure hash method. Due to the alterations in the general ECC, the proposed technique is called as Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC) algorithm. The encryption process of ESHP-ECC is detailed below,

- At first, the elliptic curve equation used for key generation is given by,

$$Y^2 = X^3 + aX + b \quad \text{-----} \quad (24)$$

In (24), a, b denotes the integers.

- Then, a random number (η) is generated from $[1, n-1]$ and the probability of ones and zeros of this random number is calculated, defined as the private key. After that, the public key (ρ) is calculated as,

$$\rho = \eta * B \quad \text{-----} \quad (25)$$

Here, B describes the point on the elliptic curve.

- Thereafter, these public and private keys are converted into a hash value using a secure hashing method. Secure Hashing Algorithm (SHA) is a cryptographic hash function that takes the keys as the input and produces a 160-bit (20-byte) hash value. The private and public keys after hashing are represented as η'' and ρ'' accordingly.
- Consider, M be the message to be transmitted and it has the point Q on the elliptic curve. Randomly select σ from $[1, n-1]$. Two ciphertexts ($C^{(1)}, C^{(2)}$) are calculated using equations (26), (27),

$$C^{(1)} = \sigma * B \quad \text{-----} \quad (26)$$

$$C^{(2)} = Q + \sigma * \rho \quad \text{-----} \quad (27)$$

Where, ($C^{(1)}, C^{(2)}$) defines the encrypted message that is transmitted to the cloud server through the shortest path.

4.8 Shortest Pathway Calculation :

Let, ($x_i = x_1, x_2, \dots, x_N$) be the number of sensor nodes available to transmit the encrypted message. The shortest path between each sensor node is identified for efficient data transmission as well as to reduce the computational time. Therefore, Euclidean distance $E^{(d)}$ is used to calculate the distance. It is formulated as follows,

$$E^{(d)} = \|(x_i - x_j)\|^2 \quad \text{-----} \quad (28)$$

In this equation, x_j mentions the j -th node. After computing the distance, the shortest pathway obtained is used to transmit the encrypted message. This encrypted message is further decrypted at the receiver side using Decrypted Secure Hash Probability-based Elliptic-curve cryptography (DSHP-ECC) algorithm.

4.9 Decryption through DSHP-ECC :

The encrypted message in equation (27) is decrypted using the below equation,

$$Q = C^{(2)} - \eta * C^{(1)} \quad \text{-----} \quad (29)$$

Where, Q specifies the original message.

5. RESULTS :

The detailed analysis of the outcome of the suggested structure is explained in this section. To demonstrate the work's efficacy, the performance analysis, as well as the comparative analysis, is carried out. The implementation of the proposed methodology is done by using MATLAB, and the data are obtained from the UNSW-NB15 dataset, which is publically available on the internet.

5.1 Dataset description :

The Australian Cybersecurity Center's (ACCS) Network Scope Lab used the IXIA Perfect Storm engine to build a mix of operations using unprocessed network packets from the UNSWNB 15 dataset. Modern synthetic assaults and genuine modern normals UNSWNB154.csv, UNSWNB154.csv, UNSWNB153.csv, and UNSWNB152.csv are four CSV files containing a total of two million and 540,044 records: UNSWNB154.csv, UNSWNB151.csv, UNSWNB153.csv, and UNSWNB152.csv.

The training set has 175,341 records, whereas the test set contains 82,332 records, comprising normal and attack records.

5.2 Performance Analysis of the proposed BRELU-ResNet mechanisms :

The suggested BRELU-ResNet is compared with existing methodologies such as Artificial Neural Network (ANN), Convolution Neural Network (CNN), Adaptive Network-based Fuzzy Inference System in terms of sensitivity, False positive rate (FPR), accuracy, False negative rate (FNR), precision, recall, specificity, F-Measure, and Matthews correlation coefficient (MCC) (ANFIS). The comparative analysis is also done with the existing techniques to state the effectiveness of the model.

Table 1: Performance analysis of proposed BRELU-ResNet based on sensitivity, specificity, and accuracy.

Techniques	Performance metrics (%)		
	Sensitivity	Specificity	Accuracy
Proposed BRELU-ResNet	98.34	77.54	96.6
CNN	97.81	63.62	94.58
ANN	95.78	58.84	93.23
ANFIS	91.17	44.42	90.61

Table 1 demonstrates the performance analysis of the proposed BRELU-ResNet with various existing techniques, such as CNN, ANN, and ANFIS in terms of sensitivity, specificity, and accuracy.

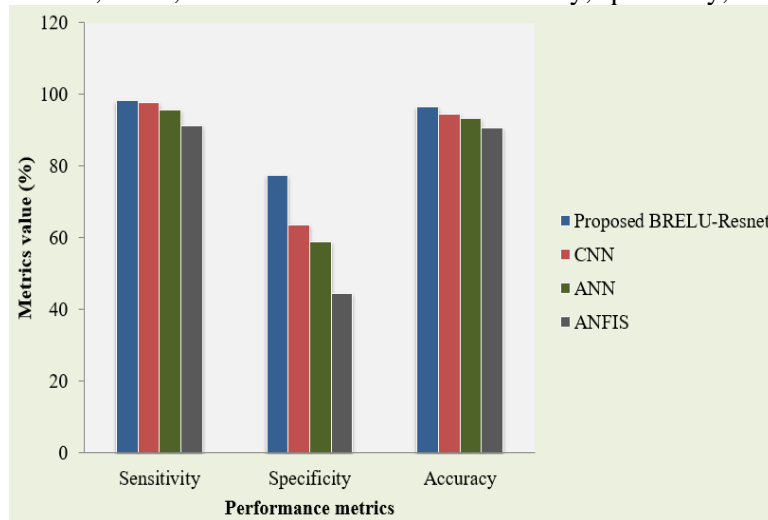


Fig. 4: Comparative analysis of proposed BRELU-ResNet based on Sensitivity, specificity and accuracy.

A clear view of tabulation 1 is given in figure 4. Figure 4 shows the comparative analysis of the proposed work. This comparative analysis clearly states that the proposed framework tends to attain higher Sensitivity, Specificity and accuracy values that range between 77.54%-98.345 whereas the existing techniques CNN, ANN, and ANFIS, attain the metrics values that range between 44.42%-97.81%, which is comparatively lower than the proposed BRELU-ResNet. As a consequence, the suggested strategy outperforms previous state-of-the-art methods and produces more notable outcomes in a variety of challenging situations.

Table 2: Performance analysis of proposed BRELU-ResNet based on precision, F-measure, and recall.

Techniques	Performance metrics (%)		
	Precision	Recall	F-measure
Proposed BRELU-ResNet	97.96	98.34	98.15
CNN	96.26	97.81	97.03
ANN	96.9	95.78	96.34
ANFIS	92.49	97.17	94.77

Tabulation 2 comprises the value of the performance metrics, like precision, F-Measure, and recall of the proposed BRELU-ResNet and the other existing works, like CNN, ANN, and ANFIS.

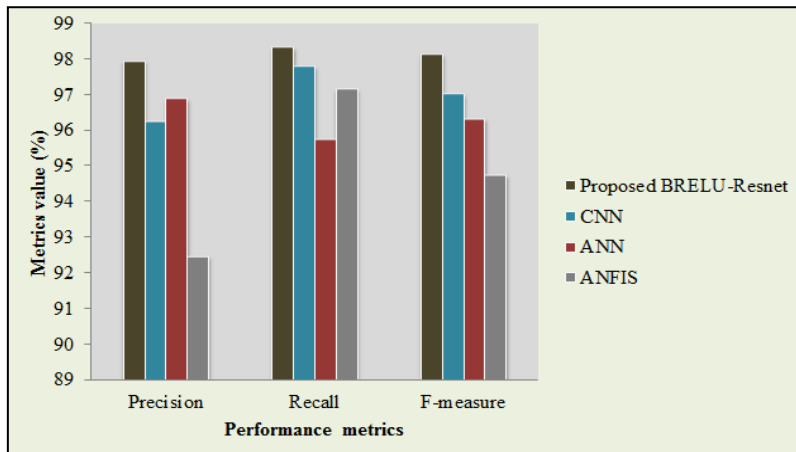


Fig. 5: Comparative analysis of proposed BRELU-ResNet based on precision, recall, and F-Measure.

A clear view of tabulation 2 is given in figure 5. Figure 5 shows the comparative analysis of the proposed work. This comparative analysis clearly states that the proposed framework tends to attain higher precision, recall, and F-Measure values that range between 97.96%-98.34% whereas the existing techniques CNN, ANN, and ANFIS, attain the metrics values that range between 92.49%-97.81%, which is comparatively lower than the proposed BRELU-ResNet. As a consequence, the suggested strategy outperforms previous state-of-the-art methods and produces more notable outcomes in a variety of challenging situations.

Table 3: Performance analysis of proposed BRELU-ResNet with respect to FPR, FNR, and MCC.

Techniques	Performance metrics (%)		
	False Positive Rate	False Negative Rate	Matthews Correlation Coefficient
Proposed BRELU-ResNet	22.46	1.66	77.38
CNN	36.38	2.19	66.24
ANN	41.16	4.22	51.12
ANFIS	55.58	2.83	50.6

Table 3 depicts the performance evaluation of the proposed BRELU-ResNet and other existing techniques with respect to FPR, FNR, and MCC.

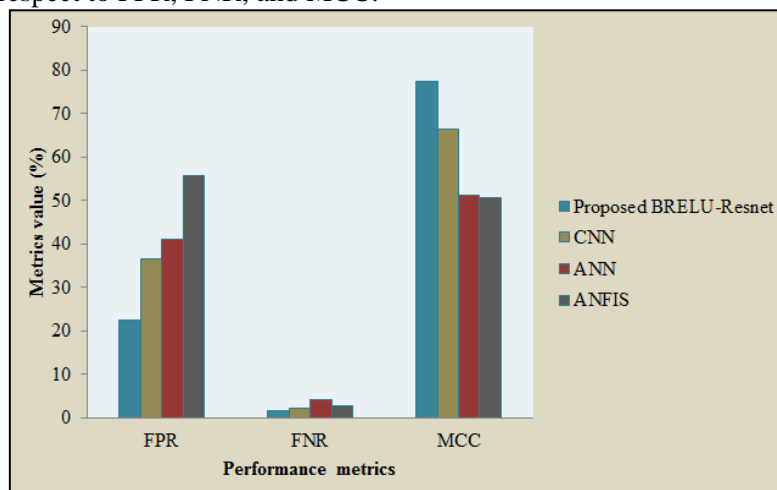


Fig. 6: Comparative analysis of proposed BRELU-ResNet in terms of FPR, FNR, and MCC.

Figure 6 compares the evaluation metrics such as FPR, FNR, and MCC of the proposed work with the existing works. The significance of the model is determined by the low value of FPR and FNR rates and the high value of MCC. In accordance with the above-mentioned statement, the FPR and FNR rates of the proposed work are low and the MCC rate achieved by the proposed work is higher than the existing approaches. Hence, the proposed method outperforms the other state-of-art methods and delivers better outcomes in the cyber-attack detection process.

6. DISCUSSION :

The proposed strategy achieves an over the top responsiveness level of 98.34 percent, particularity level of 77.54 percent, exactness of 96.6 percent, Precision level of 97.96 percent, review level of 98.34 percent, F-proportion of 98.15 percent, False Positive Rate of 22.46 percent, False Negative Rate of 1.66 percent, Matthew's relationship coefficient of 77.38 percent, according to the results obtained in the previous area, classified information. As a result, it can be deduced that the proposed methodology actually identifies digital assault; as a result, the organization's privacy is improved as well as more solidified, and it outperforms present methodologies. As a result, the suggested BReLU-ResNet-based Cyber-assault Detection architecture, which includes a BAIT-based far-reaching mitigation mechanism, protects the cloud server against gatecrashers. According to the claim, the proposed strategy achieves a level of awareness of 98.34 percent, particularity of 77.54 percent, and exactness of 96.6 percent, whereas current procedures such as CNN, ANN, and ANFIS achieve a level of responsiveness of 94.92 percent, explicitness of 55.62 percent, and precision of 92.80 percent, respectively. As a result, when compared to current works, the proposed BReLU-ResNet achieved better measurement rates. The meaning of the increased rate of accuracy, F-measure, and review is not totally clear. The methodology proposed, according to the claim, achieves 97.96 percent accuracy, 98.34 percent review, and 98.15 percent F-measure. Regardless, the current work achieves the average accuracy, review, and F-measure rate of 95.21 percent, 96.92 percent, and 96.04 percent, respectively. When compared to the intended task, this is a modest number. As a result, the proposed BReLU-ResNet reduces complexities and enhances the consistency of the digital assault recognition process. FPR and FNR's lower value effectively eliminates the misclassification or mis-expectation error. According to this claim, the proposed technique achieves 22.46 percent FPR and 1.66 percent FNR values. In any event, the existing methods' typical FPR and FNR upsides are 44.37 percent and 3.08 percent, respectively. The greater the MCC value, the more powerful the model; in this case, the proposed strategy obtains 77.38 percent of MCC, while the present methods obtain a typical MCC value of 55.98 percent. As a result, it is discovered that the proposed work is more reliable and outperforms existing approaches.

7. CONCLUSION :

The work has proposed a novel approach of BReLU-ResNet based Cyber-Attack Detection System with a BAIT-based approach for mitigation. This approach involved several operations designed to check cyber-attacks quickly. The work is pre-processed, feature extracted, feature selected, and classified for intrusion detection. The classification phase efficiently detects whether the data is normal or attack. If the data is normal, then the data transmission process begins. To ensure security, the encryption and decryption process is performed by the means of the SHP-ECC algorithm. The experimental analysis is then carried out, which includes performance analysis and a comparison study of the offered methodologies in terms of various performance measures to test the proposed algorithm's efficacy. The developed approach can handle various uncertainties and render more promising results. The publically available datasets called UNSW-NB 15 dataset is used for the analysis, in which the proposed method achieves 98.34% of sensitivity, 77.54% of specificity, 96.6% of accuracy, 97.96 % of Precision, 98.34% of recall, 98.15 % of F-measure, 22.46% of False Positive Rate, 1.66 % of False Negative Rate, 77.38 % of Matthew's correlation coefficient.

REFERENCES :

- [1] Noorizadeh, M., Shakerpour, M., Meskin, N., Unal, D., & Khorasani, K. (2021). A cyber-security methodology for a cyber-physical industrial control system testbed. *IEEE Access*, 9(1), 16239-16253. [Google Scholar](#)

- [2] Elnour, M., Meskin, N., Khan, K., & Jain, R. (2020). A dual-isolation-forests-based attack detection framework for industrial control systems. *IEEE Access*, 8(1), 36639-36651. [Google Scholar](#)
- [3] Paridari, K., O'Mahony, N., Mady, A. E. D., Chabukswar, R., Boubekour, M., & Sandberg, H. (2017). A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. *Proceedings of the IEEE*, 106(1), 113-128. [Google Scholar](#)
- [4] Barrère, M., Hankin, C., Nicolaou, N., Eliades, D. G., & Parisini, T. (2020). Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *Journal of information security and applications*, 52(1), 102471. [Google Scholar](#)
- [5] Yang, J., Zhou, C., Yang, S., Xu, H., & Hu, B. (2017). Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(5), 4257-4267. [Google Scholar](#)
- [6] Adepu, S., & Mathur, A. (2018). Assessing the effectiveness of attack detection at a hackfest on industrial control systems. *IEEE Transactions on Sustainable Computing*, 6(2), 231-244. [Google Scholar](#)
- [7] Abana, M. A., Peng, M., Zhao, Z., & Olawoyin, L. A. (2016). Coverage and rate analysis in heterogeneous cloud radio access networks with device-to-device communication. *IEEE Access*, 4(2), 2357-2370. [Google Scholar](#)
- [8] Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane III, C. D., & Dixon, W. E. (2019). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics*, 16(6), 4281-4292. [Google Scholar](#)
- [9] Ponomarev, S., & Atkison, T. (2015). Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 252-260. [Google Scholar](#)
- [10] Guo, H., Pang, Z. H., Sun, J., & Li, J. (2021). An output-coding-based detection scheme against replay attacks in cyber-physical systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(10), 3306-3310. [Google Scholar](#)
- [11] Han, S., Xie, M., Chen, H. H., & Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE systems journal*, 8(4), 1052-1062. [Google Scholar](#)
- [12] Lu, K. D., Zeng, G. Q., Luo, X., Weng, J., Luo, W., & Wu, Y. (2021). Evolutionary deep belief network for cyber-attack detection in industrial automation and control system. *IEEE Transactions on Industrial Informatics*, 17(11), 7618-7627. [Google Scholar](#)
- [13] Genge, B., Siaterlis, C., Fovino, I. N., & Masera, M. (2012). A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers & Electrical Engineering*, 38(5), 1146-1161. [Google Scholar](#)
- [14] Baldoni, S., Battisti, F., Carli, M., & Pascucci, F. (2021). On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. *IEEE Access*, 9(1), 41787-41798. [Google Scholar](#)
- [15] Sui, T., Mo, Y., Marelli, D., Sun, X., & Fu, M. (2020). The vulnerability of cyber-physical system under stealthy attacks. *IEEE Transactions on Automatic Control*, 66(2), 637-650. [Google Scholar](#)
- [16] Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems. *IEEE Internet of Things Journal*, 8(17), 13712-13722. [Google Scholar](#)
- [17] Lv, Z., Han, Y., Singh, A. K., Manogaran, G., & Lv, H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics*, 17(2), 1496-1504. [Google Scholar](#)

- [18] Haller, P., & Genge, B. (2017). Using sensitivity analysis and cross-association for the design of intrusion detection systems in industrial cyber-physical systems. *IEEE Access*, 5(1), 9336-9347. [Google Scholar](#)
- [19] Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7), 4362-4369. [Google Scholar](#)
- [20] Al-Abassi, A., Karimipour, H., Dehghantaha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, 8(1), 83965-83973. [Google Scholar](#)
- [21] Kravchik, M., & Shabtai, A. (2021). Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA. *IEEE Transactions on Dependable and Secure Computing*, 10(1), 1-18. [Google Scholar](#)
- [22] Kajaet, N., Shaout, A., & Ma, D. (2019). An intelligent intrusion detection system. *Applied Intelligence*, 49(9), 3235-3247. [Google Scholar](#)
- [23] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, 8(1), 32464-32476. [Google Scholar](#)
- [24] Prabhu, S., & Nethravathi, P. S. (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 176-183. [Google Scholar](#)
- [25] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. *IEEE Access*, 8(1), 185938-185949. [Google Scholar](#)
- [26] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176. [Google Scholar](#)
- [27] Hussain, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics*, 17(2), 860-870. [Google Scholar](#)
- [28] Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning. *Microprocessors and Microsystems*, 77(1), 103121. [Google Scholar](#)
- [29] Ibor, A. E., & Epiphaniou, G. (2015). A hybrid mitigation technique for malicious network traffic based on active response. *International Journal of Security and Its Applications*, 9(4), 63-80. [Google Scholar](#)
- [30] Akyazi, U., & Force, T. A. (2014). Possible scenarios and maneuvers for cyber operational area. *European Conference on Cyber Warfare and Security*, 1(10), 1-7. [Google Scholar](#)

Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions

Sangeetha Prabhu¹ & Nethravathi P. S.²

¹Research Scholar, College of Computer Science and Information Science, Srinivas
University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

²Professor, College of Computer and Information Sciences, Srinivas University, Mangalore,
India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

Subject Area: Computer Science.

Type of the Paper: Research Article.

Type of Review: Peer Reviewed as per [C|O|P|E](#) guidance.

Indexed In: OpenAIRE.

DOI: <https://doi.org/10.5281/zenodo.6350841>

Google Scholar Citation: [IJAEML](#)

How to Cite this Paper:

Sangeetha Prabhu, & Nethravathi, P. S., (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 176-183. DOI: <https://doi.org/10.5281/zenodo.6350841>

International Journal of Applied Engineering and Management Letters (IJAEML)

A Refereed International Journal of Srinivas University, India.

Crossref DOI : <https://doi.org/10.47992/IJAEML.2581.7000.0128>

Received on: 20/02/2022

Published on: 15/03/2022

© With Authors.



This work is licensed under a [Creative Commons Attribution-Non-Commercial 4.0 International License](#) subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions

Sangeetha Prabhu¹ & Nethravathi P. S.²

¹Research Scholar, College of Computer Science and Information Science, Srinivas
University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

²Professor, College of Computer and Information Sciences, Srinivas University, Mangalore,
India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

ABSTRACT

Purpose: *Because of the apparent rapid advancement in the field of information and communication technology and its constant connection to the internet, customer and organizational data have become vulnerable to cyber-attacks, necessitating the explanation of solutions to ensure the security and protection of information throughout the industry. Today, it is critical for governments and major corporations to implement cybersecurity systems to ensure the confidentiality and security of data in the face of cyber-attacks. As community-based fully systems have become more important in today's society, they've become targets for malicious actions, prompting both industry and the research community to place a greater emphasis on resolving community intrusion detection difficulties. In network intrusion detection challenges, gadget examining algorithms have proven to be a valuable tool.*

Design/Methodology/Approach: *This research provided a fully unique architecture for attack node mitigation as a result of the use of a novel type and encryption mechanism. First, the UNSW-NB15 dataset is received and separated into training and testing data. Within the Training section, information is first and foremost pre-processed, and capabilities are extracted. The relevant features are then chosen using the Taxicab Woodpecker Mating algorithm (TWMA). The BReLU-ResNet classifier is then used to classify the attacked and non-attacked data. The typical statistics are encrypted using the ESHP-ECC method, which is then saved in the security log report. Following that, the shortest distance will be calculated using Euclidean distance. Finally, the information is decrypted utilizing a set of ideas known as DSHP-ECC. If the entry appears in the log record while testing, it is marked as attacked statistics and will not be communicated. The method of detecting cyber-assaults will continue if it is not detected.*

Findings/Result: *The analysis is based on the UNSW-NB 15 dataset, which shows that the proposed approach achieves an excessive security level of 93.75 percent.*

Originality/Value: *This experimental-based research article examines the malicious activities in the cyberspace and mitigated by using a SHP-ECC mechanism.*

Paper Type: *Research Article*

Keywords: Cyber-attack detection, Attack node mitigation, BAIT approaches, Feature extraction, Future Community Intrusions, SHP-ECC Mechanism.

1. INTRODUCTION :

Cyber security is a major concern for a wide range of businesses, agencies, government entities, and individuals all around the world. According to Buczak and given in [1], cyber security is the total of all technology and methods for tracking and preventing unauthorized access, modification, misuse, and denial of service to computer networks and assets. This also involves inclinations to give access to labeled content, as well as community-on-hand infrastructure. Most networks are connected via the internet and provide a means of replacing information, intelligence, software, and hardware. Computer

infrastructure attacks are becoming a more serious threat [2]. Cyber detection on a network is a critical component of system security. Although the computer networking paradigm has been important in terms of the exchange of valuable property for improved operational efficiency, it has also been a constant source of malware transmission, increasing cyber-attacks in the online world.

Computer security refers to the protection of computer systems from risks to their confidentiality, integrity, and availability. Confidentiality means that records are disclosed in the most honest way feasibility policy; integrity means that records aren't lost or damaged, and the device functions properly; and availability means that device offerings are available when they're needed. Computer structures, computer networks, and the data they carry are all checked using computing structures. The improvement and augmentation of cyber-attack detection structures have been stimulated by these dangers, as well as others that are expected to emerge in the future [3].

This shift in the risk landscape is the result of the increased threat of cyber-attacks, which are regularly gaining control of all household, organizational, and business capacities. Because of the impact of cyber strain, akyazi [4] says in work that cyber-assault risks are linked to the ability to change device or database parameters, which is a good way to create a kinetic effect for escalating attacks, as well as the proclivity to disrupt labeled contents. Preventive and reactive tactics are included in cyber-attack defense. Those approaches, which can be classified as active or passive, are utilized in the context of usage – they could be direct countermeasures or cyber-attack mitigation processes. Denning [3] noted in his work that the value of cyber defense measures is rooted in the ability to address both active and passive threats, which have become the standard in the cyber world.

Cybercriminals regularly target Industrial control systems as a target. The majority of the people who work in these areas exhibit intricate business techniques and vital infrastructures that provide power, water, shipping, production, and other crucial services [5]. There was a period when those systems were essentially dumb, and those who were automated employed protocols that were exclusive to the device and resided on networks that included the outdoors. The landscape has shifted, and as a result, the majority of business management systems in use today connect to the internet either directly or indirectly. As with any other linked device, this exposes them to vulnerabilities. Downtime or invasion of an ICS network, on the other hand, might result in massive outages, hundreds of impacted consumers, or even a national tragedy. ICS protection is a framework for defending structures against both incidental and purposeful threats. A complex network of interactive manipulation structures or a limited number of controllers can make up a business control system. These structures collect data from far-flung sensors that measure and show process factors [6]. An ICS sends commands and receives signals from a variety of unique components, ranging from control valves to stress gauges.

Several anomaly detection techniques are then incorporated to tackle the problems and hazards encountered throughout the assault detection process. These strategies are combined and used through the use of a variety of machine learning algorithms [7]. However, the bulk of existing algorithms overlooks the unbalanced structure of ICS datasets, resulting in a low detection rate or large false-positive rate in real-world scenarios [8]. Several of the current strategies would be rendered ineffective if the entire physical device was assaulted at the same time [9]. Many studies on fault-tolerant management have been undertaken, and the results of these studies can be used to develop equipment for assault-resistant management [10]. There are several factors to keep in mind when it comes to escaping surveillance and isolation, there are numerous variations between fault-tolerant controls and assault-resistant controls, necessitating the employment of exact ways to tackle protection difficulties in ICSs [11]. To address the aforementioned issue, the work proposes a framework known as a unique approach of BRELU-RESNET principally based cyber-assault detection device with BAIT-based strategy for mitigation, which ensures accurate detection of cyber-assaults while maintaining better community authenticity.

The remaining portion of the paper is organized as follows: the second phase goes deeper into the problem. Studies that may be relevant to the method under consideration. The recommended methodology referred to as a single way of BRELU-RESNET principally based cyber-attack detection system with bait-based completely strategy for mitigation, is explained in Section three. Phase 4 depicts the suggested technique's outputs and dialogue based on overall performance criteria. Phase five is the final section of the report, and it concludes with suggestions for further research.

2. LITERATURE REVIEW :

Following the revelation of cyber-attacks on sensor data in 2020, Zhe et al [12] recommended an RNN-based completely state reconstruction approach for nonlinear tactic nation estimate. The recommended technique was used to locate cyber-assaults in closed-loop operations utilizing system-gaining knowledge-based detection structures, and an RNN version was built to replicate technique states using fictitious country metrics to assess manipulative behavior. Internal to LMPC and LEMPC, an RNN-based configuration re-structor was used in real-time to provide precise stability evaluation and ensure closed-loop consistency of nonlinear procedures during cyber-assault detection. Through min-max, surge, and geometric cyber-assaults, the re-efficacy constructor's in reassembling process states for both LMPC and LEMPC was demonstrated using a chemical way context.

Georgios et al [13] investigated an Energy-Aware Smart Home system's internal connectivity climate in 2020. In EASH, the issue of distinguishing between equipment failure and network attacks was described in terms of their impact on communication. The relationship between these abnormality sources was shown, and a machine learning-based architecture for the differentiation issue was developed. The suggested method was calibrated in both a simulation and a real-time testbed setting, and it demonstrated a positive classification performance of over 85 percentage. Obtained from experimental findings, a quantitative description of the considered classes were given and functionality was used in the suggested method to increase classification accuracy.

In the year 2020, Perez et al [14] presented a flexible modular structure for detecting and mitigating LR-DDoS attacks in SDN environments. The intrusion detection system (IDS) was trained in the framework using six machine learning models, and their overall performance was assessed using the DoS dataset from the Canadian Institute of Cybersecurity. Despite the difficulties of identifying LR-DoS attacks, the results of the study demonstrate that this technique has a 95 percent detection rate. The OS controller on the Mininet digital system is utilized to keep the simulated environment as close to real production networks as possible. All attacks experienced by employing the intrusion detection system inside the testing topology are mitigated by the intrusion prevention detection machine. This demonstrates how good the system is at recognizing and preventing LR-DDoS attacks.

The unattended detection of anomalies based on the statistical correlation between measurements was proposed by Karimipour et al [15] in 2019. The adopted version's goal was to create a configurable anomaly detection engine for large-scale intelligent networks that could distinguish between a real malfunction, attack and, a smart cyber-attack. The method suggested using symbolic dynamic filtering to reduce computing complexity while finding causal relationships between subsystems. The results of simulations of IEEE 39,118 and 2,848 bus systems show that the technique performs well under a variety of situations. The data shows that 99 percent of the high accuracy and false-high-quality rate are mean with less than 2 percent being substandard.

Behal et al [16] investigated energy robbery in the DG domain in the year 2020. Malicious clients breach the smart meter in this attack to reveal their renewable DG units and exploit their information, allowing you to claim extra energy from the grid. A deep learning system has been used to uncover such harmful behavior. The integration of DG smart meters, weather data, and SCADA metering elements in a deep co-evolutionary-neural network yielded the highest detection rate of 99.3 percent and the lowest false alarm rate of 0.22 percent, according to this study.

3. OBJECTIVES :

- (1) To introduce the deep ensemble technique for detecting the presence of attack in the network.
- (2) To process a SHP-ECC mechanism model for mitigating the attacker from the network.
- (3) To assess the feasibility of the proposed system concerning certain performance metrics against other state-of-the-art frameworks.

4. METHODOLOGY :

4.1 Proposed Model for Cyber-Attack Detection and Mitigation System:

In recent years, the increasing incidence of cyber-physical system attacks has raised the priority of industrial control system cybersecurity. The current state of ICS cybersecurity is based mostly on firewalls, and other intrusion prevention technologies, which will not be sufficient to combat escalating cyber threats from influenced attackers [17]. With the help of a deep learning method, the previous research effort built a framework for identifying attacks. Even though the network's attack nodes had been identified, they were not turned down. Earlier research suggested that a framework for

cyber and physical systems had been devised. Cyber-attacks have been recognised and treated in the framework using ensemble deep learning algorithms that are specifically tailored for SGCS. A deep presentation-learning arrangement has also been developed for chance management employing a single symmetric presentation from the asymmetric dataset. The correctness of models was determined to be 91.62 percent [18]. As a solution to this difficulty, an enhanced and effective adversary version will be provided. As a result, developing a unique category and encryption technique, this research proposes a single architecture for attack node mitigation. To begin with, the input records are divided into two categories: Training records and testing information. The general training statistics are pre-processed in the beginning. Functions are extracted from this input training dataset in the second stage. The feature is optimized for deciding on the important capabilities when using TWMA in the third stage. The proposed BReLU-RESNET classifier is then used to train the characteristic. The classifier divides the records into two categories: attack and normal data. If the data is about an attack, use the BAIT method to save the source IP address into a safe log record. Following that, if the facts are ordinary, they are ready to be transmitted. The statistics are initially encrypted using the ESHP-ECC set of rules during record transmission. Following that, to calculate the shortest route distance Euclidean distance is used. The records are decrypted using the DSHP-ECC method at the destination node. The testing data are checked first in the security log report when checking out. If the information's source IP address is already known, the statistics will be prohibited or an attack will be detected. Figure 1 represents the proposed framework's block diagram.

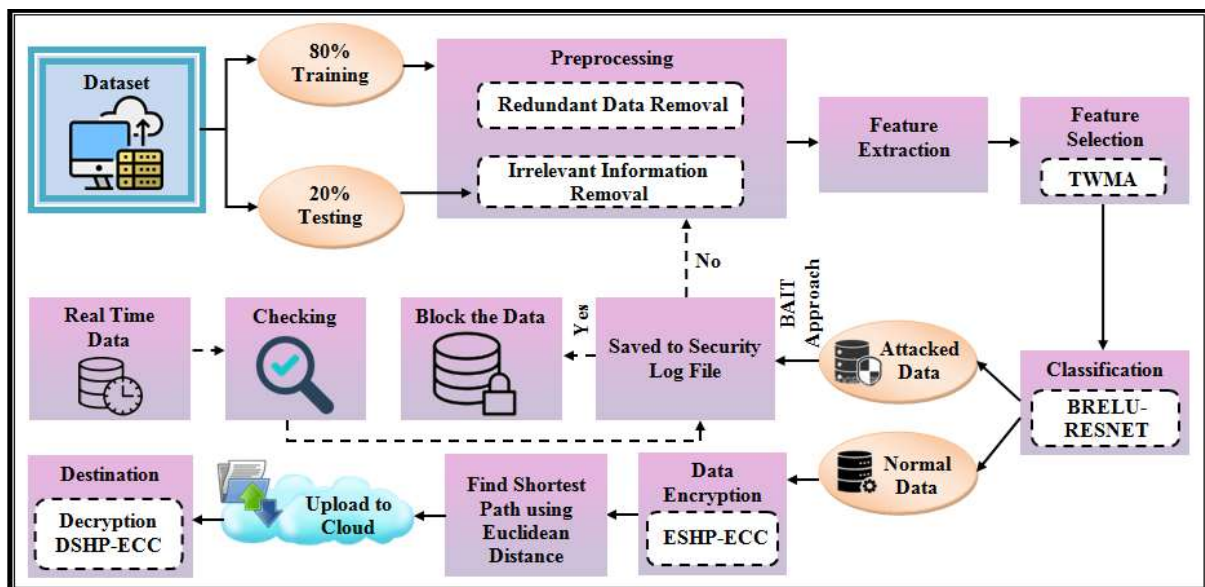


Fig. 1: The suggested cyber-attack detection and mitigation system's structural layout [19]

4.2 Data Encryption and Decryption Using SHP-ECC Mechanism:

Elliptic-Curve Cryptography (ECC) is a public-key cryptosystem based on the elliptic curve hypothesis, which is a secure unequal encryption strategy used for data security [20]. Using the elliptic curve residences, it produces public and private keys for each user. After that, the material is encrypted and decrypted using those keys. The keys are created at random in a normal ECC technique. As a result, the attackers may be able to hack the crucial information with ease. The probability of ones and zeros is generated mostly based on the randomly generated key fee in order to cope with the problem. Additionally, the relaxed hash technique is used to convert the key values into hash values. The proposed technique is referred to as encrypted because to changes inside the fashionable ECC. The relaxed hash technique is also used to turn the key values into a hash value. The recommended approach is known as Encrypted Comfortable Hash Possibility-Based Totally Elliptic-Curve Cryptography (ESHP-ECC) set of regulations due to the changes inside the current ECC. The keys are then decrypted using the Decrypted At Ease Hash Possibility-Based Elliptic-Curve Cryptography (DSHP-ECC) method.

5. RESULTS :

This section defines the precise evaluation of the proposed framework's very last outcome. The overall performance analysis, as well as the comparative analysis, are used to demonstrate the model's effectiveness. The proposed technique is implemented in Matlab, and the data are taken from the UNSW-NB 15 dataset, which is freely available on the internet.

5.1 Performance Evaluation of the Proposed SHP-ECC Mechanism:

The suggested SHP-ECC is compared to other current works such as Rivest, Shamir, Adleman, AES, and DES in terms of a variety of overall performance criteria, such as security stage, encryption time, and decryption time.

Table 1: Performance analysis of the proposed SHP-ECC based on the security level

Techniques	Security level (%)
Proposed SHP-ECC	93.75
RSA	6.25
AES	87.5
DES	12.5

Table 1 depicts the security rates achieved by the proposed SHP-ECC method and the existing works like RSA, AES, and DES.

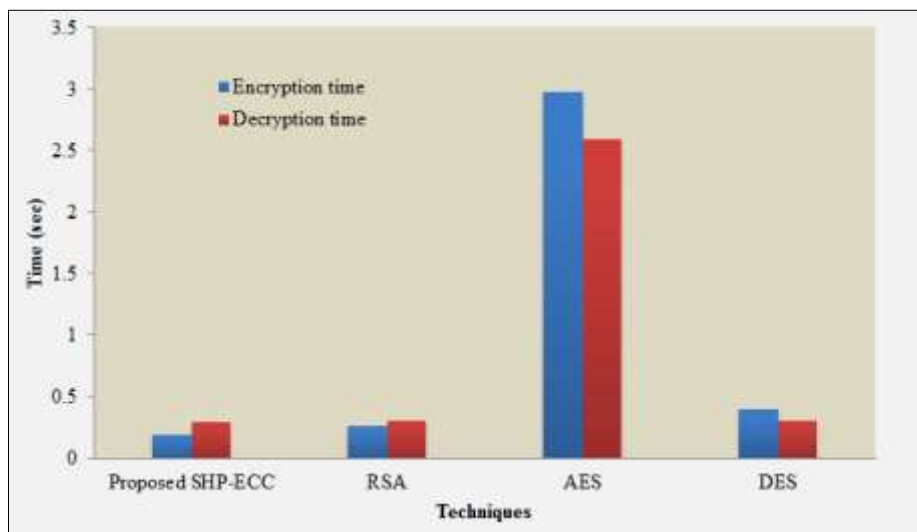


Fig. 2: Comparative analysis of the proposed SHP-ECC in terms of encryption and decryption time.

Figure 2 shows the comparison of encryption time and decryption time attained by the proposed SFP-ECC and the other exiting algorithms like RSA, AES, and DES. The efficiency of the model is determined by the low consumption of encryption and decryption time.

6. DISCUSSION :

According to the results obtained in the previous section, the tabulated data, it is known that the proposed method accomplishes a high-security rate of 93.75 percent. But the existing works exhibit the security level at an average of 35.41 percent. This is relatively low when compared to the proposed work. Hence it is concluded that the proposed work efficiently performed the encryption and decryption process and mitigates the external attack. Thus, the proposed SHP-ECC safeguards the cloud server against intruders. As per the statement, the proposed method encrypts and decrypts the data at the time of 0.1980606 seconds, and 0.3009068 seconds. But the existing works require an average of 1.218806 seconds to encrypt the data and 1.07358133 seconds to decrypt the data.

Therefore, the proposed SHP-ECC efficiently performs the encryption and decryption process with less consumption of energy and also ensures the security of the data access.

7. CONCLUSION :

The paper proposes a unique BRELU-ResNet-based Cyber-attack Detection system with a BAIT-based comprehensive mitigation mechanism. Several operations were concerned about the effectiveness of this technique in detecting cyber-attacks. Pre-processing, characteristic extraction, feature selection, and classification are all used to detect intrusions. The typing phase effectively determines whether the data are normal or malicious. The information transmission procedure commences if the records are normal. The encryption and decryption methods are implemented using the SHP-ECC set of rules to ensure security. The experimentation assessment is then completed, with an overall performance evaluation and comparative analysis of the offered methods in terms of some overall performance indicators to validate the effectiveness of the given set of rules. The improved method can deal with a wide range of uncertainty and produce even more promising results. The analysis is based on the UNSW-NB 15 dataset, which shows that the proposed approach achieves an excessive security level of 93.75 percent. The suggested cyber-attack detection methodology surpasses current state-of-the-art methodologies and remains more dependable and robust. In the future, the study will be expanded to include more advanced neural networks as well as different types of realistic attacks.

REFERENCES :

- [1] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176. [Google Scholar↗](#)
- [2] Aamir, M., & Zaidi, S. M. A. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, 33(4), 436-446. [Google Scholar↗](#)
- [3] Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, 8(1), 83965-83973. [Google Scholar↗](#)
- [4] Akyazi, U., & Force, T. A. (2014). Possible scenarios and maneuvers for cyber operational area. *European Conference on Cyber Warfare and Security*, 1(10), 1-7. [Google Scholar↗](#)
- [5] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. *IEEE Access*, 8(1), 185938-185949. [Google Scholar↗](#)
- [6] Hussain, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics*, 17(2), 860-870. [Google Scholar↗](#)
- [7] Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers & Security*, 40(1), 108-113. [Google Scholar↗](#)
- [8] Baldoni, S., Battisti, F., Carli, M., & Pascucci, F. (2021). On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. *IEEE Access*, 9(1), 41787-41798. [Google Scholar↗](#)

- [9] Sui, T., Mo, Y., Marelli, D., Sun, X., & Fu, M. (2020). The vulnerability of cyber-physical system under stealthy attacks. *IEEE Transactions on Automatic Control*, 66(2), 637-650.
[Google Scholar](#)
- [10] Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems. *IEEE Internet of Things Journal*, 8(17), 13712-13722.
[Google Scholar](#)
- [11] Lv, Z., Han, Y., Singh, A. K., Manogaran, G., & Lv, H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics*, 17(2), 1496-1504.
[Google Scholar](#)
- [12] Wu, Z., Chen, S., Rincon, D., & Christofides, P. D. (2020). Post cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, 159(1), 248-261.
[Google Scholar](#)
- [13] Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning. *Microprocessors and Microsystems*, 77(1), 103121.
[Google Scholar](#)
- [14] Perez-Diaz, Jesus Arturo, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8(2), 155859-155872.
[Google Scholar](#)
- [15] Karimipour, Hadis, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, and Henry Leung (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* 7, 80778-80788.
[Google Scholar](#)
- [16] Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing DDoS attacks and flash events: Review, research gaps and future directions. *Computer Science Review*, 25(1), 101-114.
[Google Scholar](#)
- [17] Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, 7(3), 366-370.
[Google Scholar](#)
- [18] Ibor, A. E., & Epiphaniou, G. (2015). A hybrid mitigation technique for malicious network traffic based on active response. *International Journal of Security and Its Applications*, 9(4), 63-80.
[Google Scholar](#)
- [19] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, 8(1), 32464-32476.
[Google Scholar](#)
- [20] Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications*, 10(1), 1-22.
[Google Scholar](#)

Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation

SANGEETHA PRABHU, P.S. NETHRAVATHI, CRISTI SPULBAR, AND RAMONA BIRAU

ABSTRACT. The recent exponential rise in the number of cyber-attacks has demanded intensive study into community intrusion detection, prediction, and mitigation systems. Even though there are a variety of intrusion detection technologies available, predicting future community intrusions is still a work in progress. Existing approaches rely on statistical and/or superficial device mastery techniques to solve the problem, and as a result, feature selection and engineering are required. The truth is that no single classifier can provide the highest level of accuracy for all five types of training data set. Cyber-attack detection is a technique for detecting cyber-attacks as they emerge on a laptop or network device, intending to compromise the gadget's security. As a result, using a novel type and encryption mechanism, this paper offered a unique architecture for attack node mitigation. The input UNSW-NB15 dataset is first acquired and divided into training and testing statistics. First and foremost, the information is pre-processed and capabilities are retrieved in the training section. The Taxicab Woodpecker Mating Algorithm (TWMA) is then used to select the critical characteristics. The attacked and non-attacked information are then classified using the BRELU-ResNet (Bernoulli's Leaky Rectified Linear Unit - Residual Neural Community) classifier. The encrypted at Ease Hash Probability-Based Elliptic-Curve Cryptography (ESHP-ECC) technique is used to encrypt the ordinary facts, which are subsequently kept in the security log report. Following that, using Euclidean distance, the shortest course distance is estimated. Finally, the records are decrypted using a set of principles known as Decrypted Relaxed Hash Probability-Based Elliptic-Curve Cryptography (DSHP-ECC). If the input appears in the log file during testing, it is regarded as attacked data and is prevented from being transmitted. If it isn't found, the procedure of detecting cyber-attacks continues.

2020 Mathematics Subject Classification.

Key words and phrases. Cyber-attack detection; BAIT approaches; Cryptosystem; ResNet; Feature extraction; Woodpecker Mating Algorithm (WMA); Elliptic Curve Cryptography (ECC).

1. Introduction

The digital revolution of large-scale manufacturing environments promotes the use of big data analytic in fixing plant outages, equipment breakdowns, fault prediction, and ensuring cybersecurity through the extension of computer networks and interconnectivity of computers in cyber-physical systems [16, 18]. In recent decades, the topic of cyber-defense has piqued researchers' attention, particularly as cyber-physical networks have become extremely malicious cyber-attacks that could threaten any part of the unexploited cyber surface [14]. This emphasizes the significance of putting in place efficient identification algorithms and robust solution mechanisms that protect both

the cyber and physical facets of the infrastructure ? a crucial prerequisite for improving operational technologies [14, 22]. Many contributions have been made throughout this field of operational technologies by the process automation and control group in particular.

CPS (Cyber-Physical Systems) is a term used to describe the mixture of computational, communication, and physical components [9, 12]. Cyber-Physical Systems CPS is a modeling tool that can be used to simulate a wide range of applications, including sophisticated critical infrastructures. Indeed, the widespread integration of Cyber-Physical Systems in vital infrastructures has increased their significance in sustaining economic growth, and their stability and durability have become essential in all facets of modern life [17, 5]. Security incidents and component faults are two of the biggest abnormalities that can disrupt CPS's daily function. Since CPS are so essential to contemporary society's day-to-day activities, they've become a tempting choice for cybercriminals. Because of their extensive use, their attack surface has grown significantly [6]. Various components of the CPS, like every other physical control device, will malfunction at the same time. Both faults and attacks can cause the machine to behave abnormally, but the consequences can be somewhat different. CPS operators may select the appropriate rehabilitation actions that mitigate the detrimental consequences of irregular behavior as they can differentiate [1]. Defining the criteria that could lead to such distinction is a difficult challenge that necessitates a thorough examination of individual components in a CPS structure before arriving at a holistic solution [2, 15].

A malfunction that influences any of CPS's components will cause it to behave abnormally (nodes). Fault detection in CPS has proven to be a difficult challenge due to the system's complexity and large size, as well as the fact that flawed activity is a complex and diverse problem [13]. Traditional CPS fault detection methods focus on the operator's knowledge, while more recent approaches, which characterize the modern IoT age, rely on sensor and alarm data. Machine learning methods and human expertise are combined in certain IoT solutions for fault diagnosis [7, 5]. For example, Artificial Neural Networks, which are adaptive structures inspired by biological systems, are used in fault detection in power and smart grid systems. RBF and SVM are two popular methods in artificial neural networks. Other methods [3] make use of logic to avoid latent faults that can occur when a stable environment is caused by a control system for a failure condition. Existing CPS security procedures are usually classified according to the security triad of secrecy, transparency, and availability [20, 10]. A security purpose is often linked to the appropriated mitigating measures that seek to defend a CPS system defined by a particular system model from an adversary.

The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or from Ransomware. When tested, we use trained information or data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of input. When the model identifies the attacker node, it is removed via the BAIT technique from the network. The rest of the paper could be written as follows: the second segment examines the related studies that are relevant to the proposed technique. The recommended strategy, known as a unique way of BRELU-ResNet based completely cyber-assault detection machine

with BAIT-based approach for mitigation, is explained in section three. Section 4 depicts the findings and discussion for the suggested strategy, which is entirely based on performance indicators. Finally, step five brings the paper to a close with destiny work.

2. Literature review

Wang et al. [20] published a scenario-based two-stage sparse cyber-attack model for smart grids with complete and partial network details in 2018. The proven cyber-attacks were successfully detected, and a security mechanism based on interval state estimation (ISE) was implemented in a novel way. The upper and lower limits of each state variable were modeled as a dual optimization problem in this process, to maximize the function variable's variance cycles. Furthermore, a popular deep learning algorithm, the stacked auto-encoder (SAE), was utilized to collect nonlinear and non-stationary features in electric load results. Such features were then used to increase predictive performance for electric loads, resulting in state variables with a narrow width. A parametric Gaussian distribution was used to represent the variance of forecasting errors. Comprehensive studies on numerous IEEE benchmarks have been used to show the validity of the current cyber-attack models and security mechanisms.

In 2019, Defu et al. [19] presented a machine learning-based attack detection model for power systems that were trained using data and logs obtained by phasor measurement units (PMUs). The findings demonstrate that the data processing method could increase the model's precision, and the AWV model could efficiently identify 37 different types of power grid behaviors. The feature development engineering was completed, and the data was then sent to various machine learning models, with the random forest being selected as AdaBoost's simple classifier. Finally, various comparison criteria were used to equate the proposed model to other ones. The experimental findings show that this model can reach a 93.91 percent accuracy rate and a 93.6 percent identification rate, which is better than eight recently established techniques.

In 2020 Mariam et al. [11] established a recovery strategy for the optimal re-closure of the trickled transmission lines. In specific, a framework for deep strengthening learning (RL) has been created to enable the strategy to adapt the unpredictable cyber-attack scenarios and to take decision-making capabilities in real-time. In this context, an environment has been set up for simulating power system dynamics and generating training data during the attack-recovery process. The profound RL strategy to determine the optimal lock-up time was trained with this information. Numerical outcomes demonstrate that the approach utilized would minimize cyber-attack effects in different circumstances.

Integrity attacks on CPSs were studied by means of Mo and Sinopoli [8] in 2012 the usage of discrete linear time-invariant structures. The researchers were able to characterise the available additives of the system kingdom and estimate the error underneath attack a good way to verify the gadget's resilience to integrity attacks. Additionally they used an ellipsoidal approach to find the on hand set's outer approximations. But, in a few cases where the accessible set is unbounded, the attacker can be capable of undermine the system.

3. Methodology

3.1. Proposed model for Cyber-Attack Detection and Mitigation System.

Over the last few years, the increasing incidence of Cyber-Physical Systems (CPS) attacks has increased concerns regarding industrial control machine cybersecurity. ICS cybersecurity efforts today rely heavily on firewalls, statistics valves, and other intrusion detection and prevention systems, which may not be enough to combat escalating cyber threats from persistent attackers. Previous research has developed a framework for identifying assaults using a deep learning technique. Even though the attack node in the network was detected, it was no longer deactivated. As a solution to this challenge, an upgraded and effective adversary model will be presented. As a result, this work presents a novel architecture for assault node mitigation based on a unique class and encryption approach. Initially, the input data is divided into two categories: training data (80 percentage) and testing data (20 percentage). The total training data is initially pre-processed. The next step is to extract features from the training dataset as input. The feature is tailored for determining the critical capabilities utilizing TWMA in the 0.33 stage. The suggested BReLU-ResNet classifier is then used to train the characteristic. The classifier divides the data into attack and non-attack categories. If the data is attack data, use the BAIT technique to record the Source IP Address into a secure log file. Following that, if the information is updated regularly, the data are prepared for transmission. The records are first encrypted using the ESHP-ECC method before being sent. Following that, using Euclidean distance, the shortest route distance is estimated. The records are decrypted using the DSHP-ECC method at the destination. During testing, the checking facts are first checked in the Security Log File (SLF). If the source IP address of the data is already known, the records are blocked or an assault is identified. The proposed structure is depicted as a block diagram in Figure 1.

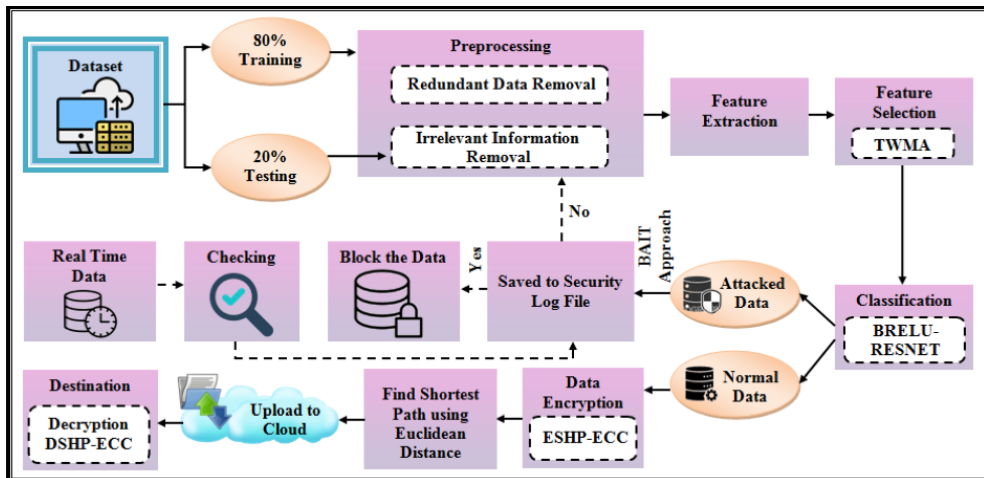


FIGURE 1. The framework for the proposed cyber-attack detection and mitigation system (Jiang, Wang, Wang, and Wu, 2020) [8].

3.2. Data Encryption Using ESHP-ECC. Elliptic-curve cryptography (ECC) is a public-key cryptosystem based on the elliptic curve hypothesis, which is a secure asymmetric encryption scheme used for data security. It generates public and private keys for each user through the elliptic curve properties. These keys are then used to encrypt and decrypt the data. In a conventional ECC technique, the keys are generated randomly. So, the attackers may easily hack the key information. To address the problem, the probability of ones and zeros are generated based on the randomly generated key value. Also, the key values are converted into a hash value using the secure hash method. Due to the alterations in the general ECC, the proposed technique is called as Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC) algorithm. The encryption process of ESHP-ECC is detailed below,

- At first, the elliptic curve equation used for key generation is given by,

$$Y^2 = X^3 + aX + b, \quad (1)$$

where in (1), a, b denotes the integers.

- Then, a random number (η) is generated from $([1, n - 1])$ and the probability of ones and zeros of this random number is calculated, defined as the private key. After that, the public key (ρ) is calculated as,

$$\rho = \eta * B. \quad (2)$$

Here, B describes the point on the elliptic curve.

- Thereafter, these public and private keys are converted into a hash value using a secure hashing method. Secure Hashing Algorithm (SHA) is a cryptographic hash function that takes the keys as the input and produces a 160-bit (20-byte) hash value. The private and public keys after hashing are represented as η and ρ accordingly.

- Consider, M be the message to be transmitted and it has the point Q on the elliptic curve. Randomly select σ from $[1, n - 1]$. Two cyphertexts ($C^{(1)}, C^{(2)}$) are calculated using equations (3), (4),

$$C^{(1)} = \sigma * B \quad (3)$$

$$C^{(2)} = Q + \sigma * \rho \quad (4)$$

where, ($C^{(1)}, C^{(2)}$) defines the encrypted message that is transmitted to the cloud server through the shortest path.

3.3. Decryption through DSHP-ECC. The encrypted message in equation 4 is decrypted using the below equation,

$$Q = C^{(2)} - \eta * C^{(1)}, \quad (5)$$

where, Q specifies the original message.

4. Results

This section focuses on the specific findings of the suggested structure's final consequence. The exhibition inspection, such as the relative inquiry, is performed to demonstrate the feasibility of the work. The suggested concept is carried out with the use of MATLAB, and the open source UNSW- NB15 dataset is utilized for this

work. These results focuses on the specific examination of the suggested structure's final consequence. The exhibition inspection, such as the relative inquiry, is performed to demonstrate the feasibility of the work.

4.1. Performance analysis of the proposed BRELU-RESNET. The suggested BRELU-ResNet is compared with existing methodologies such as CNN, ANN, Adaptive Network-based Fuzzy Inference System in terms of sensitivity, False positive rate (FPR), accuracy, False negative rate (FNR), precision, recall, specificity, F-Measure, and Matthews correlation coefficient (MCC) (ANFIS). The comparative analysis is also done with the existing techniques to state the effectiveness of the model.

Table 1: Performance analysis of proposed BRELU-ResNet with respect to FPR, FNR, and MCC.

Techniques	FPR	FNR	MCC
Proposed BRELU-ResNet	22.46	1.66	77.38
CNN	36.38	2.19	66.24
ANN	41.16	4.22	51.12
ANFIS	55.58	2.83	50.6

Table 1 depicts the performance evaluation of the proposed BRELU-ResNet and other existing techniques concerning FPR, FNR, and MCC. The lower value of FPR and FNR efficiently discards the misclassification or miss-prediction error.

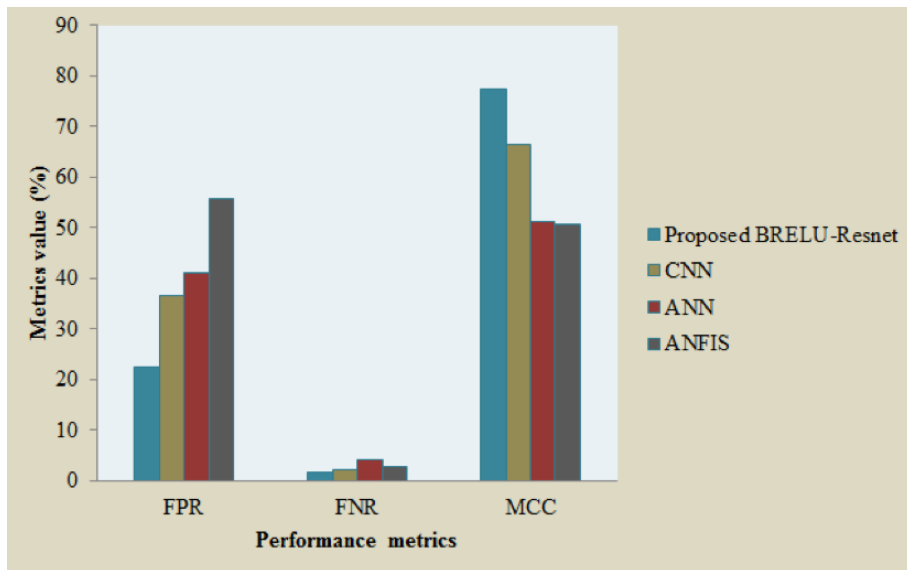


FIGURE 2. Comparative analysis of proposed BRELU-ResNet in terms of FNR, FPR, and MCC

Figure 2 compares the evaluation metrics such as FNR, FPR, and MCC of the proposed work with the existing works. The consequence of the model is determined by the low value of FPR and FNR rates and the high value of MCC.

5. Discussion

According to the results obtained in the previous section, the proposed method achieves 22.46 percentage of FPR and 1.66 percentage of FNR values. But the average FPR and FNR values of the existing techniques are 44.37 percentage and 3.0 percentage respectively. Conversely, the higher MCC value denotes the robustness of the model; here, the proposed method obtains 77.38 percentage of MCC, while the existing techniques obtain the average MCC value of 55.98 percentage.

Hence, it is revealed that the proposed work is more reliable and outperforms the existing approaches. In accordance with the significance of the model is resolute by the FNR and FPR rates of the proposed work are low and the MCC rate achieved by the proposed work is higher than the existing approaches. Hence, the proposed method outperforms the other state-of-art methods and delivers better outcomes in the cyber-attack detection process.

6. Conclusion

The research proposes a novel strategy for detecting and mitigating cyber-attacks using a BRELU- ResNet -based system with aBAIT-based mechanism. This method applied to a number of tasks involving the green detection of cyber-attacks. The work goes through pre-processing, function extraction, function choosing, and categorization for intrusion detection. The categorization step effectively determines if the facts are routine or malicious. The facts transfer operation begins if the records are normal. The encryption and decryption techniques are carried out in accordance with the SHP-ECC set of principles to ensure security. After that, the experimental assessment is completed, in which the overall performance evaluation and comparison analysis of the offered strategies are carried out in terms of a few overall performance metrics with the goal of validating the proposed algorithm's efficacy. The new approach can deal with a variety of uncertainty and produce more promising outcomes. The suggested technique achieves 22.46 percent of FPR, 1.66 percent of FNR, and 77.38 percent of MCC using publicly available datasets named the UNSW-NB 15 dataset. On average, the suggested cyber-assault detection system surpasses current state-of-the-art technologies and remains more reliable and robust. The study will be expanded in the future with a few sophisticated neural networks, as well as a focus on unique sorts of practical assaults.

References

- [1] M. Aamir and S.M.A. Zaidi, Clustering-based semi-supervised machine learning for DDoS attack classification, *Journal of King Saud University - Computer and Information Sciences* **7** (2019), no. 2, 1–11. DOI: [10.1016/j.jksuci.2019.02.003](https://doi.org/10.1016/j.jksuci.2019.02.003)
- [2] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, An ensemble deep learning-based cyber-attack detection in the industrial control system, *IEEE Access* **8** (2020), no. 5, 83965–83973. DOI: [10.1109/ACCESS.2020.2992249](https://doi.org/10.1109/ACCESS.2020.2992249)
- [3] M. Marsaline Beno, I.R. Valarmathi, S.M. Swamy, and B. R. Rajakumar, Threshold prediction for segmenting tumors from brain MRI scans, *International Journal of Imaging Systems and Technology* **24** (2014), no. 2, 129–137. DOI: [10.1002/ima.22087](https://doi.org/10.1002/ima.22087)

- [4] X. Fang, M. Xu, S. Xu, and P. Zhao, A deep learning framework for predicting cyberattacks rates, *Eurasip Journal on Information Security* **2019** (2019), no. 1, 1–11. DOI: [10.1186/s13635-019-0090-6](https://doi.org/10.1186/s13635-019-0090-6)
- [5] T. Gopalakrishnan, D. Ruby, F. Al-Turjman, D. Gupta, I.V. Pustokhina, D.A. Pustokhin, and K. Shankar, Deep learning enabled data offloading with a cyber-attack detection model in mobile edge computing systems, *IEEE Access* **8** (2020), no. 1, 185938–185949. DOI: [10.1109/ACCESS.2020.3030726](https://doi.org/10.1109/ACCESS.2020.3030726)
- [6] B. Hussain, Q. Du, B. Sun, and Z. Han,, Deep Learning-Based DDoS-Attack Detection for Cyber- Physical System over 5G Network, *IEEE Transactions on Industrial Informatics* **17** (2021), no. 2, 860–870. DOI: [10.1109/TII.2020.2974520](https://doi.org/10.1109/TII.2020.2974520)
- [7] A.E. Ibor, F.A. Oladeji, O.B. Okunoye, and O.O. Ekabua, The conceptualization of Cyberattack prediction with deep learning, *Cybersecurity* **3** (2020), no. 1, 1–13. DOI: [10.1186/s42400-020-00053-7](https://doi.org/10.1186/s42400-020-00053-7)
- [8] K. Jiang, W. Wang, A. Wang, and H. Wu, Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network, *IEEE Access* **8** (2020), no. 3, 32464–32476. DOI: [10.1109/ACCESS.2020.2973730](https://doi.org/10.1109/ACCESS.2020.2973730)
- [9] V. Kanimozhi and T.P. Jacob, Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS 2018 using cloud computing, *ICT Express* **8** (2020), no. 1, 1–8. DOI: [10.1016/j.ict.2020.12.004](https://doi.org/10.1016/j.ict.2020.12.004)
- [10] N.M. Karie, V.R. Kebande, and H.S. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, *Forensic Science International: Synergy* **17** (2019), no. 1, 61–67. DOI: [10.1016/j.fsisy.2019.03.006](https://doi.org/10.1016/j.fsisy.2019.03.006)
- [11] M. Elnour, N. Meskin, K. Khan, and R. Jain, A dual-isolation-forests-based attack detection framework for industrial control systems, *IEEE Access* **8** (2020), no. 3, 36639–36651. DOI: [10.1109/ACCESS.2020.2975066](https://doi.org/10.1109/ACCESS.2020.2975066)
- [12] U. Noor, Z. Anwar, T. Amjad, and K.K.R. Choo, A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise, *Future Generation Computer Systems* **9** (2019), no. 6, 227–242. DOI: [10.1016/j.future.2019.02.013](https://doi.org/10.1016/j.future.2019.02.013)
- [13] Y. Pan, F. Sun, Z. Teng, J. White, D.C. Schmidt, J. Staples, and L. Krause, Detecting web attacks with end-to-end deep learning, *Journal of Internet Services and Applications* **10** (2019), no. 1, 2–22. DOI: [10.1186/s13174-019-0115-x](https://doi.org/10.1186/s13174-019-0115-x)
- [14] D.T. Ramotsoela, G.P. Hancke, and A.M. Abu-Mahfouz, Attack detection in water distribution systems using machine learning, *Human-Centric Computing and Information Science* **9** (2019), no. 1, 1–26. DOI: [10.1186/s13673-019-0175-8](https://doi.org/10.1186/s13673-019-0175-8)
- [15] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.K.R. Choo, and R.M. Parizi, An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic, *IEEE Internet of Things Journal* **7** (2020), no. 9, 8852–8859. DOI: [10.1109/JIOT.2020.2996425](https://doi.org/10.1109/JIOT.2020.2996425)
- [16] A. Samy, H. Yu, and H. Zhang, Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning., *IEEE Access* **8** (2020), no. D1, 74571–74585. DOI: [10.1109/ACCESS.2020.2988854](https://doi.org/10.1109/ACCESS.2020.2988854)
- [17] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for the internet of things in a smart city, *Future Generation Computer Systems* **10** (2020), no. 7, 443–442. DOI: [10.1016/j.future.2020.02.017](https://doi.org/10.1016/j.future.2020.02.017)
- [18] A. Subroto and A. Apriyana, Cyber risk prediction through social media big data analytics and statistical machine learning, *Journal of Big Data* **6** (2019), no. 1, 1–19. DOI: [10.1186/s40537-019-0216-1](https://doi.org/10.1186/s40537-019-0216-1)
- [19] D. Wang, X. Wang, Y. Zhang, and L. Jin, Detection of power grid disturbances and cyber-attacks based on machine learning, *Journal of Information Security and Applications* **46** (2019), no. 1, 42–52. DOI: [10.1016/j.jisa.2019.02.008](https://doi.org/10.1016/j.jisa.2019.02.008)
- [20] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, Deep learning aided interval state prediction for improving cybersecurity in the energy internet, *Energy* **17** (2019), no. 4, 1292–1304. DOI: [10.1016/j.energy.2019.03.009](https://doi.org/10.1016/j.energy.2019.03.009)
- [21] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks, *IEEE Transactions on Industrial Informatics* **14** (2018), no. 11, 4766–4778. DOI: [10.1109/TII.2018.2804669](https://doi.org/10.1109/TII.2018.2804669)

- [22] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, Machine Learning and Deep Learning Methods for Cybersecurity, *IEEE Access* **6** (2018), no. 1, 35365–35381. DOI: [10.1109/ACCESS.2018.2836950](https://doi.org/10.1109/ACCESS.2018.2836950)

(Sangeetha Prabhu) COLLEGE OF COMPUTER SCIENCE AND INFORMATION SCIENCE, SRINIVAS UNIVERSITY, MANGALORE, INDIA. ORCID ID 0000-0002-8026-1133
E-mail address: sangeethaprabhu96@gmail.com

(P.S. Nethravathi) COLLEGE OF COMPUTER SCIENCE AND INFORMATION SCIENCE, SRINIVAS UNIVERSITY, MANGALORE, INDIA. ORCID ID 0000-0002-0088-3355
E-mail address: nethrakumar590@gmail.com

(Cristi Spulbar) FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION, UNIVERSITY OF CRAIOVA, ROMANIA. ORCID ID 0000-0002-3909-9496
E-mail address: cristi_spulbar@yahoo.com

(Ramona Birau) C-TIN BRANCUSI UNIVERSITY OF TARGU JIU, FACULTY OF EDUCATION SCIENCE, LAW AND PUBLIC ADMINISTRATION, ROMANIA. ORCID ID 0000-0003-1638-4291
E-mail address: ramona.f.birau@gmail.com

ABCD Analysis of Cyber Attack Detection and Mitigation Model

Sangeetha Prabhu*
Dr. Nethravaathi P. S**

Abstract

A cybersecurity framework is a structured set of guidelines, best practices, and standards that organizations use to manage and improve their cybersecurity posture. These frameworks provide a comprehensive approach to safeguarding digital assets, sensitive data, and information systems. By applying this ABCD analysis to a cybersecurity framework, organizations can systematically identify, assess, and address security risks, ensuring that resources are allocated to protect the most critical assets and defend against the most significant threats. This approach enhances overall cybersecurity posture and resilience.

Keywords:

ABCD Analysis;
Cyber attack;
Attack detection;
Attack Mitigation;
ABCD Framework.

Copyright © 2023 International Journals of Multidisciplinary Research Academy. All rights reserved.

Author correspondence:

Sangeetha Prabhu,
Research Scholar, Institute of Computer Science & Information Sciences
Srinivas University, Mangalore
Email: sangeethaprabhu96@gmail.com

1. Introduction

Complex decision-making procedures are frequently a part of strategic management. Businesses and organizations use a variety of tools and frameworks to negotiate this complexity. The Advantages, Benefits, Constraints, and Disadvantages (ABCD) framework is one such tool that facilitates the evaluation of methods, procedures, or initiatives [1]. The ABCD framework is a flexible analytical tool for analyzing and appraising several facets of a choice, a course of action, or a circumstance. It provides as a methodical way to thoroughly assess all the different aspects of a subject.

Company and industry analysis are regarded as the first steps in academic research. To identify the difficulties or problems or to analyze the past, present, and future performance of the system, data collected from businesses and industries utilizing primary and secondary sources must be analyzed in a systematic format. SWOT (strengths, weaknesses, opportunities, and threats), balanced scorecard, and quality function deployment are some of the various frameworks used for a corporate study. Other frameworks, like Porter's Value Chain Analysis (VCA), make it easier to analyze internal corporate processes, but they don't offer a simple way to connect those analyses to overarching business goals [2]. Relationships and an organization's overarching economic theory. Prior to implementing innovative changes within a specific environment, a consistent method for analyzing the structure, behavior, and dynamics of a company business should enable the identification of potential optimizations governing the business models, the assessment of the impact of innovative changes, and the identification of critical success factors. SWOC analysis, PESTLE analysis, McKinsey 7S framework, ICDT model, Portor's five force model, and other frameworks are used to examine individual traits or organizational effectiveness & tactics in a specific context.

When examining the business value in society, the ABCD framework can be used to examine individual qualities, system characteristics, the effectiveness of a concept or idea, and the effectiveness of a plan [3].

* Research Scholar, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore

** Professor, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore

The SWOT analysis, SWOC analysis, PEST analysis, McKinsey 7S framework, ICDT model, Portor's five force model, etc. can all be used to examine individual traits or organizational effectiveness & tactics in a particular context. In 2015, the ABCD analysis framework for business analysis was introduced [3]. It is suitable for analyzing business concepts, business systems, technology, business models, or business ideas in terms of determining various factors for selected determinant issues under four constructs known as advantages, benefits, constraints, and disadvantages. A specific resource (material, machine, information, or human resource) can be examined using the ABCD analysis framework based on how it is used in the society. The concept, system, strategy, technology, model, idea, and resource are further investigated in the qualitative analysis utilizing the ABCD framework by finding constitutional important factors [2]. The concept, idea, system, technology, or strategy can be accepted or rejected by evaluating the scores in the quantitative analysis using the ABCD framework [1]. The appropriate score or weight can be given to each constituent critical element under each construct through empirical research. As a result, the ABCD analysis framework, which takes into account a company's business models, systems, concepts, ideas, technology, strategy, and material analysis, can be used as a study tool in various fields.

2. Objectives

1. To identify the determinant concerns that can be taken into account while analyzing the study model.
2. To list the different essential characteristics for each determining factor.
3. To incorporate each essential component of each determining issue into the study model and evaluate it in light of the ABCD constraints (Advantages, Benefits, Constraints, and Drawbacks)

3. Dimension of the ABCD Framework

The four dimensions of ABCD Framework are explained as below:

1. **Advantages:** The "Advantages" dimension focuses on identifying the positive aspects or strengths associated with a decision, strategy, or situation [4]. It involves recognizing the inherent benefits that can be derived from a particular course of action. Advantages encompass both quantitative and qualitative factors, including cost savings, revenue generation, enhanced efficiency, improved customer satisfaction, competitive advantage, and more.
2. **Benefits:** The "Benefits" dimension delves deeper into the outcomes or gains that can be realized as a result of implementing the decision or strategy. Benefits are often measurable and specific, and they directly contribute to achieving organizational objectives [5]. They may include increased market share, expanded customer base, higher profitability, reduced operational risks, improved employee morale, and other tangible results.
3. **Constraints:** The "Constraints" dimension highlights the limitations, barriers, or challenges that may impede the successful execution of the decision or strategy. Constraints can manifest in various forms, such as budgetary constraints, resource limitations, regulatory hurdles, technological constraints, and time constraints [6]. Identifying constraints is crucial for devising effective mitigation strategies.
4. **Disadvantages:** The "Disadvantages" dimension focuses on the potential drawbacks, risks, or negative consequences associated with the decision, strategy, or situation. It is essential to anticipate and assess these disadvantages to make informed decisions. Disadvantages can encompass financial risks, reputational damage, legal liabilities, customer dissatisfaction, and other adverse effects.

4. Applications of the ABCD Framework

The ABCD framework finds applications across a wide range of domains and industries. It is a versatile tool that can be employed in decision-making, project management, risk assessment, and strategic planning [7]. Here are some key areas where the ABCD framework proves valuable:

1. **Strategic Planning:** In the realm of strategic management, the ABCD framework aids in evaluating and prioritizing strategic initiatives. It allows organizations to assess the advantages and benefits of proposed strategies, identify potential constraints, and anticipate any disadvantages that may arise during implementation.
2. **Project Management:** Project managers utilize the ABCD framework to conduct comprehensive project assessments. By analyzing the advantages, benefits, constraints, and disadvantages of a project, they can make informed decisions regarding resource allocation, risk management, and project prioritization.
3. **Risk Assessment:** When assessing risks associated with a particular course of action, the ABCD framework serves as a structured approach. It helps organizations identify potential constraints and disadvantages, enabling them to develop risk mitigation strategies and contingency plans.
4. **Investment Analysis:** In finance and investment, the ABCD framework assists investors and financial analysts in evaluating investment opportunities. By examining the advantages, benefits, constraints, and disadvantages of an investment, stakeholders can make well-informed investment decisions.

5. **Product Development:** In the context of product development, businesses use the ABCD framework to assess new product ideas. This evaluation considers the advantages and benefits of bringing a new product to market, along with any potential constraints or disadvantages, such as development costs and market competition

5. Advantages and Benefits of the ABCD Framework

The ABCD framework offers numerous advantages and benefits to organizations and decision-makers.

1. **Comprehensive Evaluation:** One of the primary strengths of the ABCD framework is its ability to provide a comprehensive evaluation of a subject matter. By considering advantages, benefits, constraints, and disadvantages, decision-makers gain a 360-degree view of the situation [8].
2. **Informed Decision-Making:** Incorporating the ABCD framework into decision-making processes promotes informed decision-making. Decision-makers can weigh the pros and cons, assess risks, and align their choices with organizational goals and objectives.
3. **Risk Mitigation:** Identifying constraints and disadvantages through the ABCD framework allows organizations to proactively address risks. This risk mitigation approach helps minimize the negative impacts of unforeseen challenges.
4. **Resource Allocation:** The ABCD framework aids in optimizing resource allocation. By prioritizing initiatives based on their advantages and benefits, organizations can allocate resources more effectively to projects or strategies with the greatest potential for success.
5. **Enhanced Communication:** When stakeholders use the ABCD framework to evaluate and communicate strategies or decisions, it fosters clear and transparent communication. All parties involved can understand the rationale behind a particular choice.
6. **Alignment with Goals:** The framework ensures that decisions align with organizational goals and objectives. By emphasizing benefits, organizations can ensure that initiatives contribute directly to desired outcomes.
7. **Flexibility:** The ABCD framework is adaptable and can be tailored to suit the specific needs of different industries and organizations. It accommodates both quantitative and qualitative assessments.
8. **Improved Accountability:** By systematically documenting the advantages, benefits, constraints, and disadvantages of a decision or strategy, organizations enhance accountability. They can track progress and measure outcomes against initial assessments.

6. Constraints and Disadvantages of the ABCD Framework

While the ABCD framework offers significant advantages, it is not without its constraints and disadvantages [9]. Understanding these limitations is crucial for using the framework effectively:

1. **Subjectivity:** The assessment of advantages, benefits, constraints, and disadvantages may involve subjective judgments. Different individuals or teams may perceive the same factors differently, leading to potential biases in the evaluation.
2. **Complexity:** In some cases, the ABCD framework may not fully capture the complexity of a situation. Decision-makers must be cautious not to oversimplify intricate issues by relying solely on this framework.
3. **Time-Consuming:** Conducting a thorough ABCD analysis can be time-consuming, particularly for complex decisions or projects. This may not be practical when quick decisions are required.
4. **Lack of Predictive Power:** While the framework helps identify potential disadvantages and risks, it may not always predict the exact outcomes of a decision. Unforeseen events and external factors can influence results.
5. **Overemphasis on Quantitative Factors:** The ABCD framework may tend to emphasize quantitative factors over qualitative ones. This could result in a bias toward easily measurable metrics while overlooking less tangible but equally important aspects.
6. **Dynamic Nature:** The framework does not inherently account for changes over time. Advantages, benefits, constraints, and disadvantages may evolve as circumstances change, requiring ongoing assessment and adjustment.
7. **Not a Standalone Solution:** The ABCD framework should not

6. The Methodology of ABCD Framework

The methodology includes the identification of the determinant issues in the beginning. Later the key attributes are determined for every determinant issue. The ABCD analysis is done on every key attribute of the determinant issue [10]. Here the determinant issues and the corresponding key attributes are chosen based on various parameters related to the research model considering the factors like technology, the contribution of the product to society, environmental benefits of the product, production, profitability, and the various stock holders of the research model.

The ABCD analysis methodology involves a structured and systematic approach to evaluating a subject matter comprehensively [10]. The detailed steps to conduct an ABCD analysis is:

Step 1: Define the Subject of Analysis: Clearly define the subject or decision that you intend to analyze using the ABCD framework. This step is critical as it sets the scope and boundaries of the analysis. The subject could be a strategic initiative, a project, a proposed business decision, or any other situation that requires evaluation.

Key Considerations:

- Clearly articulate the purpose and objectives of the analysis.
- Define the boundaries and timeframe for the analysis.

Step 2: Identify Advantages:

- a. **List the Positive Aspects:** Begin the analysis by identifying and listing all the positive aspects or strengths associated with the subject of analysis. These could be tangible and intangible benefits that might result from the decision or strategy.
- b. **Quantify if Possible:** If possible, quantify the advantages. For instance, if you're evaluating a marketing campaign, you might consider increased revenue, customer acquisition, or brand visibility as quantifiable advantages.

Key Considerations:

- Engage relevant stakeholders to gather insights into potential advantages.
- Prioritize advantages based on their significance and relevance to organizational goals.

Step 3: Identify Benefits:

- a. **Define Measurable Outcomes:** Determine the specific, measurable outcomes or benefits that can be expected from implementing the decision or strategy. These should directly contribute to organizational goals.
- b. **Set Clear Metrics:** Establish clear metrics and key performance indicators (KPIs) that will be used to measure the benefits. This ensures that you can track and evaluate the success of the initiative.

Key Considerations:

- Align identified benefits with strategic objectives.
- Ensure that benefits are quantifiable and time-bound for effective measurement.

Step 4: Identify Constraints

- a. **Identify Potential Barriers:** Identify the potential constraints or limitations that may hinder the successful execution of the decision or strategy. Constraints can take various forms, such as budgetary limitations, resource shortages, regulatory hurdles, or time constraints.
- b. **Prioritize Constraints:** Prioritize constraints based on their potential impact and likelihood of occurrence. Focus on those constraints that could have the most significant negative effects.

Key Considerations:

- Involve subject matter experts and relevant teams to identify constraints.
- Assess the severity of each constraint and its potential to derail the initiative.

Step 5: Identify Disadvantages:

- a. **Anticipate Negative Consequences:** Consider the potential negative consequences, risks, or disadvantages associated with the decision or strategy. This involves thinking critically about the potential pitfalls.
- b. **Assess Severity and Likelihood:** Assess the severity and likelihood of each identified disadvantage. Some disadvantages may have minor impacts, while others could be more significant and pose higher risks.

Key Considerations:

- Conduct a thorough risk assessment to identify potential disadvantages.
- Consider both short-term and long-term consequences.

Step 6: Analyze and Weigh Factors:

- a. **Consider the Interplay:** Analyze how the advantages, benefits, constraints, and disadvantages interact with each other. For example, a high potential benefit might be worth pursuing despite some constraints, but the severity of disadvantages might change that assessment.
- b. **Weigh Significance:** Assign relative significance or importance to each factor. This involves determining which factors have the most substantial influence on the decision-making process.

Key Considerations:

- Use a scoring or weighting system to objectively assess the significance of each factor.
- Engage decision-makers and stakeholders in discussions to reach a consensus on factor importance.

Step 7: Develop Mitigation Strategies:

- a. **Address Constraints:** For identified constraints, develop strategies to mitigate their impact. This might involve finding alternative resources, adjusting timelines, or seeking regulatory approvals.

- b. **Mitigate Disadvantages:** Similarly, develop strategies to mitigate or manage the potential disadvantages. Risk mitigation plans can help address negative consequences if they occur.

Key Considerations:

- Ensure that mitigation strategies are practical and aligned with organizational capabilities.
- Monitor the progress of mitigation efforts and adjust strategies as needed.

Step 8: Make Informed Decisions: Based on the comprehensive analysis of advantages, benefits, constraints, and disadvantages, make an informed decision regarding the subject of analysis. Consider the balance between positive and negative factors, as well as the alignment with organizational goals and objectives.

Key Considerations:

- Clearly document the decision and the rationale behind it.
- Ensure that all relevant stakeholders are informed

7. Determinant Issues and Key Attributes Involved in the ABCD Analysis

The ABCD (Advantages, Benefits, Constraints, and Disadvantages) analysis is a structured framework used to evaluate a subject or decision comprehensively. To conduct an effective ABCD analysis, it's important to understand the determinant issues and key attributes involved in each dimension of the analysis. The below table explains issues and attributes of ABCD analysis for each dimension:

Advantages

Advantages encompass the positive aspects or strengths associated with the subject of analysis. To identify these, the following determinant issues and key attributes are considered as shown in below table:

Table 1. The summary of determinant issues and key attributes of various factors interms of advantages.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Positive Impact	Determine how the subject positively impacts the organization, project, or decision.	Consider factors such as increased revenue, cost savings, improved efficiency, enhanced customer satisfaction, and competitive advantage.
2	Strategic Alignment	Assess how the subject aligns with the organization's strategic goals and objectives.	Evaluate whether the subject contributes to achieving long-term strategic targets and whether it aligns with the organization's mission and vision.
3	Quantifiability	Determine if the advantages can be quantified or measured.	Identify specific metrics and key performance indicators (KPIs) that can be used to measure the advantages. This enables objective evaluation.
4	Stakeholder Perspectives	Consider the perspectives and feedback of relevant stakeholders.	Engage with stakeholders to understand their views on the advantages. Ensure that a diverse range of perspectives is considered.
5	Comparative Analysis	Compare the advantages of the subject with alternative options or scenarios.	Assess how the advantages of the subject stack up against the advantages of other potential courses of action. This provides context for decision-making.

Benefits

Benefits delve deeper into the specific, measurable outcomes or gains that result from the implementation of the subject[11]. To identify these, the following determinant issues and key attributes are considered as shown in below table:

Table 2. The summary of determinant issues and key attributes of various factors interms f benefits.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Measurable Outcomes	Define the tangible and quantifiable outcomes that can be expected.	Identify specific benefits such as increased market share, revenue growth, cost reduction, improved product quality, or enhanced brand reputation.

2	Time Frame	Determine the timeframe within which the benefits are expected to materialize.	Assess whether the benefits are short-term or long-term. This helps in setting realistic expectations and planning
3	Alignment with Goals	Evaluate how well the benefits align with organizational goals and objectives.	Ensure that the benefits directly contribute to achieving strategic objectives and are consistent with the organization's mission.
4	Attribution	Understand which aspects of the subject are responsible for generating specific benefits.	Attribute benefits to specific features or actions related to the subject. This helps in optimizing and replicating successful strategies.
5	Risk Mitigation	Consider how the benefits contribute to risk mitigation and resilience.	Analyze whether the benefits help in reducing risks, enhancing resilience to external factors, or improving the organization's ability to respond to challenges.

Constraints

Constraints encompass the limitations, barriers, or challenges that may impede the successful execution of the subject of analysis [12]. To identify these, the following determinant issues and key attributes are considered as shown in below table.

Table 3. The summary of determinant issues and key attributes of various factors interms of constraints.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Resource Limitations	Assess the availability of resources, including budget, personnel, and technology.	Identify resource constraints that may affect the subject's implementation. Consider whether resource allocation is adequate.
2	Regulatory Compliance	Examine regulatory requirements and compliance issues.	Identify any legal or regulatory constraints that may impact the subject's implementation. Ensure that the subject complies with applicable laws and regulations.
3	Technological Challenges	Evaluate the technological feasibility and readiness for implementation.	Consider whether technological constraints, such as compatibility issues or infrastructure limitations, need to be addressed
4	Time Constraints	Assess the time frame available for implementation.	Determine whether time constraints, such as tight deadlines, could hinder the subject's successful execution. Develop strategies to manage time effectively.
5	Stakeholder Resistance	Anticipate potential resistance from stakeholders.	Identify stakeholders who may resist the subject's implementation and understand their concerns. Develop strategies for stakeholder engagement and communication.

Disadvantages

Disadvantages involve the potential drawbacks, risks, or negative consequences associated with the subject of analysis [13]. To identify these, the following determinant issues and key attributes are considered as shown in below table.

Table 4. The summary of determinant issues and key attributes of various factors interms of advantages.

Sl. No.	Factor	Determinant Issue	Key Attributes
1	Risk Identification	Conduct a comprehensive risk assessment.	Identify potential risks and negative consequences associated with the subject. Consider both the likelihood and severity of these risks.
2	Reputational Impact	Evaluate how the subject may impact the organization's reputation.	Consider whether the subject poses reputational risks, such as negative public perception or damage to the brand image.

3	Financial Implications	Assess the financial implications of potential disadvantages.	Analyze the financial risks, including potential losses, increased costs, and budget overruns, that may arise from the subject's implementation.
4	Contingency Planning	Develop contingency plans for managing disadvantages.	Create strategies and action plans to mitigate or address potential disadvantages if they materialize. This ensures preparedness.
5	Monitoring and Evaluation	Plan for ongoing monitoring and evaluation.	Establish mechanisms for continuously assessing the subject's impact and identifying disadvantages as they emerge. This allows for timely interventions.

Effective ABCD analysis involves a holistic approach that integrates all four dimensions. Consider how the advantages align with the benefits, how constraints may impact disadvantages, and vice versa. A well-rounded analysis provides a comprehensive view of the subject, enabling more informed decision-making. The ABCD analysis is a valuable tool for systematically evaluating decisions, strategies, projects, or situations. Understanding the determinant issues and key attributes within each dimension (Advantages, Benefits, Constraints, and Disadvantages) is essential for conducting a thorough and insightful analysis. By considering these factors, organizations can make informed choices that optimize positive outcomes, mitigate risks, and align with their strategic goals.

8. Framework of Systematic Review of its Usage

The ABCD analysis framework, which stands for Advantages, Benefits, Constraints, and Disadvantages, is a structured approach used to evaluate a subject or decision comprehensively. It provides a systematic method for considering both positive and negative aspects to make well-informed decisions. In this systematic review, we will explore the usage of the ABCD analysis framework in various contexts and industries [14].

Table 5. The summary of Systematic Review of ABCD Analysis Usage.

Sl. No.	Factor	Application	Benefits	Constraints
1	Strategic Planning	The ABCD framework is widely used in strategic planning. Organizations evaluate proposed strategies by considering their advantages and benefits against constraints and disadvantages. This aids in selecting strategies aligned with long-term objectives.	Improved alignment with organizational goals, better resource allocation, and reduced risks associated with strategic decisions.	Subjectivity in assessing advantages and disadvantages, and the need for thorough data collection.
2	Project Management	Project managers employ the ABCD analysis to assess project feasibility, resource allocation, and risk mitigation. It helps in understanding the potential benefits and constraints involved.	Enhanced project planning, effective resource allocation, and better risk management.	Time-consuming process, and the need for detailed analysis for complex projects.
3	Risk Assessment	In risk assessment, the ABCD framework helps in identifying potential disadvantages and constraints that could lead to adverse events. It assists in devising mitigation strategies.	Enhanced risk management, proactive identification of potential issues, and improved decision-making.	Subjectivity in risk assessment and the challenge of predicting all possible risks.
4	Investment Analysis	Investors and financial analysts use ABCD analysis to evaluate investment opportunities. They assess	Informed investment decisions, reduced financial risks, and improved portfolio	The complexity of financial markets and the need for robust data analysis.

		potential advantages and benefits against constraints and disadvantages to make investment decisions.	management.	
5	Product Development	Businesses apply the ABCD framework to assess new product ideas. It helps in evaluating potential benefits and advantages against constraints and disadvantages.	Enhanced product development decisions, improved product quality, and increased market competitiveness.	Subjectivity in product assessment and the need for comprehensive market research.
6	Supply Chain Management	In supply chain and inventory management, ABCD analysis helps optimize stock levels. It categorizes items based on their importance and value, enabling organizations to allocate resources effectively.	Reduced carrying costs, improved inventory turnover, and better supply chain efficiency.	Continuous monitoring and updating of item categorization.
7	Strategic Resource Allocation	Organizations employ the ABCD framework to allocate resources such as budgets, personnel, and technology. It helps prioritize resource allocation based on potential advantages and benefits.	Efficient resource allocation, cost optimization, and improved strategic decision-making.	Resource constraints may limit the implementation of strategies with high potential benefits.
8	Operational Efficiency Improvement	Companies use ABCD analysis to identify areas for operational improvement. By assessing advantages and benefits against constraints and disadvantages, they prioritize process enhancements.	Enhanced efficiency, cost savings, and streamlined operations.	Resistance to change and the need for continuous process monitoring.
9	Marketing Campaign Evaluation	In marketing, the ABCD framework is employed to evaluate the effectiveness of advertising campaigns. It helps assess advantages and benefits against constraints and disadvantages.	Improved marketing ROI, better targeting, and data-driven campaign optimization.	The complexity of tracking campaign metrics and the need for real-time data analysis.

9. Conclusion

The ABCD analysis framework is a systematic approach that helps individuals and organizations make informed decisions and solve complex problems. It encourages a structured process of assessment, creative idea generation, careful evaluation, and effective execution. This framework can be applied to a wide range of scenarios, from business strategy development to personal decision-making, to ensure that decisions are well-informed and actions are purposeful. A cyber-attack detection and mitigation framework offer several benefits, including improved security, proactive defense, risk reduction, regulatory compliance, and efficient resource allocation. However, these advantages must be weighed against the potential constraints and drawbacks, such as complexity, false positives, resource demands, and adaptability challenges. To maximize the benefits and mitigate the drawbacks, organizations should carefully choose and tailor a framework to their specific needs while staying agile in responding to evolving cyber threats.

References

- [1]. D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, "MTHAEL: cross-architecture IoT malware detection based on neural network advanced ensemble learning," *Institute of Electrical and Electronics Engineers Transactions on Computers*, vol. 69, no. 11, pp. 1654–1667, 2020.

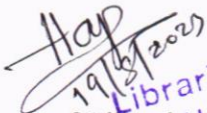

- [2]. Aithal, P. S., Shailashree, V., & Kumar, P. M. (2015). A new ABCD technique to analyze business models & concepts. *International Journal of Management, IT and Engineering*, 5(4), 409-423.
- [3]. Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems. *International Journal in Management and Social Science*, 4(1), 95-115.
- [4]. Shenoy, V., & Aithal, P. S. (2017). Quantitative ABCD Analysis of IEDRA Model of Placement Determination. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 103-113.
- [5]. Mendon, S., & Aithal, P. S. (2022). Quantitative ABCD Analysis of Organic Food Product and its Impact on Purchase Intention. *International Journal of Management, Technology, and Social Sciences (IJMITS)*, 7(1), 254-278.
- [6]. Kumari, P., & Aithal, P. S. (2022). Stress Coping Mechanisms: A Quantitative ABCD Analysis. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 6(2), 268-291.
- [7]. Prabhu, N., & Aithal, P. S. (2023). Quantitative ABCD Analysis of Green Banking Practices and its Impact on Using Green Banking Products. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 7(1), 28-66.
- [8]. Raj, K., & Aithal, P. S. (2022). Assessing the Attractiveness & Feasibility of doing Business in the BoP Market—A Mixed Method Approach using ABCD Analysis Technique. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 6(2), 117-145.
- [9]. Frederick, D. P., & Salins, M. (2022). Quantitative ABCD Analysis of Online Shopping. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 6(1), 313-329.
- [10]. Nayak, P., & Kayarkatte, N. (2022). Education for Corporate Sustainability Disclosures by Higher Educational Institutions—A Quantitative ABCD Analysis. *International Journal of Management, Technology, and Social Sciences (IJMITS)*, 7(1), 465-483.
- [11]. Nandini Prabhu, G., (2023). Quantitative ABCD Analysis of Integrating Corporate Social Responsibilities with Green Banking Practices by Banks from Customers' Attraction and Retention Perspectives in Selected Indian Banks. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(2), 1-37.
- [12]. Madhura, K., & Panakaje, N., (2023). The Power of Social Media on Online Buying Behaviour of the Fashion Products: A Quantitative ABCD Analysis. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(3), 90-118.
- [13]. Namreen Asif, V. A., & Ramesh Pai (2023). A Quantitative ABCD Analysis of Coffee Industry Stakeholders. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 7(3), 287-313.
- [14]. Aithal P. S, Shailashree V. T., Suresh Kumar P. M., (2015a) "A New ABCD Technique to Analyze Business Models & Concepts", *International Journal of Management, IT and Engineering*, 5 (4), pp 409 - 423.



SRINIVAS UNIVERSITY

Srinivas Nagar, Mukka- 574 146, Mangalore, Phone: 0824-2477456
(Private University Established by Karnataka Govt. ACT No.42 of 2013, Recognized
by UGC, New Delhi & Member of Association of Indian Universities, New Delhi)
Web: www.srinivasuniversity.ac.in, Email: info@srinivasuniversity.edu.in
Administrative Office : GHS Road, Mangalore-01, Phone 0824-2425966

Date: 19.08.2023

CERTIFICATE OF PLAGIARISM CHECK FOR THESIS/ DISSERTATION	
Author Name	SANGEETHA PRABHU
USN Number	19SUPHDF38
Name of Course	DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE
Title of the Thesis	A NOVEL DEEP LEARNING BASED CYBER ATTACK DETECTION SYSTEM WITH BAIT BASED APPROACH FOR MITIGATION
Name of the Guide	DR. NETHRAVATHI P. S.
Name of the College	Institute Of Computer Science & Information Science SRINIVAS UNIVERSITY, MANGALURU - 575001
Director of Research/ Chief Librarian	librarian@srinivasuniversity.edu.in
Acceptable Limit	25 %
Similarity Index	09 %
Status	Accepted
Submission Date	19.08.2023
* The Report is Generated by Drillbit Plagiarism Detection Software	
 Signature of Librarian Srinivas University Library, Mangalore	 Signature of Director of Research

Registered Office: Srinivas Campus, Srinivas Nagar, Mukka, Surathkal, Mangaluru - 574 146.
Karnataka State, INDIA. Website: www.srinivasuniversity.edu.in Email: info@srinivasuniversity.edu.in