e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

EMERGENCE OF AI IN CYBER SECURITY

Ribence Kadel[*1], Himesh Shrestha[*2], Animesh Shrestha[*3], Pramish Sharma[*4], Nishant Shrestha[*5], Jeeban Bashyal[*6], Sakshyam Shrestha[*7]

[*1]Budhanilkantha School, Nepal.

[*2]Kathmandu Model Secondary School, Nepal.

[*3]Little Angels College, Nepal.

[*4]Budhanilkantha School, Nepal.

[*5]Xavier International College, Nepal.

[*6]Kathmandu Model Secondary School, Nepal.

[*7]Khwopa Secondary School, Nepal.

DOI : https://www.doi.org/10.56726/IRJMETS32643

ABSTRACT

Individuals can only manage the complexity of activities and the volume of information needed to secure cyberspace with significant automation. But to adequately defend against security risks, technology and software with conventional fixed implementations are challenging to design (hardwired decision-making logic). AI machine learning techniques and machine simplicity can be used to treat this issue. The discipline that could most benefit from adopting artificial intelligence is undoubtedly cybersecurity. Artificial intelligence approaches can enhance the performance of conventional security systems where they may be slow and insufficient and offer better defense against an expanding variety of complex cyber threats. The application of AI in cybersecurity entails legitimate risks in addition to the enormous opportunities it provides. Neither people nor AI has demonstrated effectiveness in this field; a holistic picture of firms' cyber environments combining human understanding and AI is necessary to advance cybersecurity maturity further. In order to further reduce the risks and problems associated with this, socially responsible usage of AI technology will be crucial.

Keywords: Artificial Intelligence (AI), Phishing, Malware, Cyber Defense Tools, Machine Learning, Deep Learning.

I. INTRODUCTION

According to many security analysts, security incidents reached the highest number ever recorded in 2019. From phishing to ransomware, from the dark web as a service economy to attacks on civil infrastructure, the cybersecurity landscape involved attacks that grew increasingly sophisticated during the year. This upwards trend continued in 2020. The volume of malware threats observed averaged 419 threats per minute, an increase of 44 threats per minute (12%) in the second quarter of 2020. Cybercriminals managed to exploit the Covid-19 pandemic and the growing online dependency of individuals and corporations, leveraging potential vulnerabilities of remote devices and bandwidth security. According to Interpol, 907,000 spam messages related to Covid-19 were detected between June and April 2020. Similarly, the 2020 Remote Workforce Cybersecurity Report showed that nearly two-thirds of respondents saw an increase in breach attempts, with 34% of those surveyed having experienced a breach during the shift to telework. Exploiting the potential for high impact and financial benefit, threat actors deployed themed phishing emails impersonating government and health authorities to steal personal data and deployed malware against critical infrastructure and healthcare institutions.

The day-to-day rising and progressing cyber security threat facing global businesses can be reduced by integrating Artificial Intelligence into cyber security systems. Machine learning and Artificial Intelligence (AI) are being connected more extensively crosswise over industries and applications than at any other time in recent memory as computing power, storage capacities and data collection increase. Some people can only deal with this vast measure of information. With machine learning and AI, that peak of data could be carved down in a fraction of the time, which helps the enterprise to identify and recover from the security threat.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

Traditional cybersecurity approaches focus on static control of security equipment and work in reaction to an attack. For example, in the event of a network intrusion assault, security systems monitor nodes based on a predefined set of criteria. These approaches await notification that an assault has happened. The old strategy, however, is no longer effective in light of the rising number of cyberattacks. The Equifax attack in 2017, which exposed private information for up to 143 million consumers, illustrates the inadequacies of typical cybersecurity approaches. Furthermore, with new threat techniques such as advanced persistent threats (APTs) and zero-day attacks, attackers typically conceal their activities, and attacks occur before software developers discover the vulnerabilities; as a result, it takes a significant amount of time to repair the vulnerable systems.

AI in cybersecurity offers tremendous benefits but poses significant hurdles, as does any sophisticated general-purpose, dual-use technology. AI can help with cybersecurity and defense. ML and deep learning AI will intensify sophisticated assaults, allowing for quicker, more focused, and more damaging attacks. The use of AI in cybersecurity raises security and ethical problems. Among other things, it is still being determined how duties for autonomous response systems should be assigned, how to ensure that systems behave as expected, or what the security threats posed by the rising anthropomorphizing of AI systems are.

II. CYBER SECURITY

Protecting systems, networks, applications, programs, data, and all kinds of information from cyberattacks refers to cyber security. Human dependence on technology is increasing daily and becoming integral to our lives. Thus, technological enhancement has changed our world into a digital world. The more the world moves towards digital, the more vulnerable it is to digital threats. Therefore, to mitigate the threats, cyber security is introduced.

Cyber security is the need and essence of the digital world. Not only our daily activities from shopping, business, banking and other financial transactions but also official documentation, information and programs are done and stored in the computers and systems. Single small attacks and leakage of data in those systems can lead to the loss of millions and billions of dollars. For example, the I LOVE YOU computer virus launched on 11 May 2000 caused an estimated $10 billion in damages. Twenty years on, the I LOVE YOU virus remains one of the farthest-reaching ever, causing millions of computers worldwide to be affected. Many programmers are developing computer viruses intentionally for the sole purpose of earning money. Hence, cyber security is needed for every small site in every industry for its sustainable existence and success.

2.1 Types of Cyber Threats

Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Some of the Cyberattacks are listed below:

a. Computer Virus: It is a self-replicating program that can link itself to another program to reproduce. It is a malware program that hides in unknown locations in the memory of computer systems. It is very complicated to track down as it can change its digital locations anytime.

b. Adware: Adware is a malware program known for producing pop-up messages. Hackers make an attractive advertisement, and when a user downloads the advertisement, they excessed the user's computer and can delete or use their data.

c. Trojan Horse: Trojan Horse is a type of malware program that presents itself as helpful software and controls our system. Though Trojan Horse cannot reproduce itself, it can install the virus in the system. It can delete important files and data from the user's computer and send information to the hacker's system. It can also lock the user's system.

d. Ransomware: This is a computer virus where the user's computer is attacked and blackmailed to earn money. After demanding and gaining money, they left those viruses and moved away.

e. Phishing Emails: Phishing Emails are mainly used to steal the user's personal information. It is a type of fraud where fraudulent emails are sent to the user, manipulating them as if they are from officials. This virus gives hackers information on login details of different social media accounts and other credit card information.

Moreover, Man-in-the-middle attacks (MITM), Denial of Service (DoS), SQL injection and Botnets are other types of cyber threats.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

Hence, cyber security is fundamental because we can live our lifestyles and enjoy different services. The main job of those cyber experts is to:

- Find, test, and repair weaknesses within a company's infrastructure
- Monitor systems for malicious content
- Identify network breaches
- Install regular software updates, firewalls, and antivirus protection
- Strengthen areas where attacks may have occurred

They use different methods to defend the systems and networks from cyber-attacks. Some of the best practices include:

- Using two-way authentication
- Installing regular updates
- Using firewalls to disable unwanted services
- Employing cryptography, or encryption
- Securing domain name servers or DNS
- Avoiding phishing scams
- Running antivirus software
- Securing passwords

Cyber security discipline plays a vital role in keeping the peace and order in this dynamic digital world. According to Cybercrime Magazine, cybercrime will cost the world $10.5 trillion annually by 2025! Furthermore, global cybercrime costs are predicted to rise by almost 15 per cent yearly over the next four years. Concepts such as the pandemic, cryptocurrency, and the rise in remote working are coming together to create a target-rich environment for criminals to take advantage of. Therefore, the role of cyber security experts is in high demand.

III. ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI)refers to an intelligence of perceiving, synthesizing, and inferring information by machines without any guidance from human beings. The word AI was first coined in 1955 by American Computer Scientist John McCarthy also known as the Father of Artificial Intelligence. Along with the development of technology, the application of AI has increased significantly. The present and future of technology depend upon the advancement of AI.

The application of AI has dominated every sector of human lives. Here are five examples of that:

3.1 AI in healthcare

Modern health system has progressed enough to use AI in healthcare. IBM Watson can understand natural languages and can respond to the question of it. AI helps online virtual health assistants and chatbots to help patients and healthcare customers find medical information, schedule appointments, understand the billing process and complete other administrative processes.

3.2 AI in business

Machine learning algorithms have contributed a lot to the business. Customer Relationship Management (CRM) platforms and chatbots solve almost every problem of customers. AI virtual assistants cut the costs of an extra payment and also helped in decision-making for loans, and to set credit limits and identify investment opportunities.

3.3 AI in education

The one and only way to change the traditional way of teaching into a modern one is only possible if we can introduce AI in the educational field. Nowadays, AI has replaced some teachers as AI tutors can efficiently teach with additional information and supportive ideas for the students. It can even replace school with our own house.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

3.4 AI in manufacturing

AI and machine learning collaboratively enhanced the manufacturing world. ROBOTS have developed enough to perform the tasks themselves. We can see the use of robots in hotels, motels, and big and small industries. Making self-driving vehicles in automobiles, use of AI in the aerospace industry, and different big companies working on the development of their own AI systems ultimately bloomed the manufacturing world.

3.5 AI in transportation and security

Not only in manufacturing automobiles but AI also helps in operating transportation too. Managing traffic, predicting flight delays, and making ocean shipping safer and more efficient are some applications. Similarly, AI helps in security by providing alerts to new and emerging attacks faster than human employees. AI has played an indispensable role to protect against cyberattacks.

Moreover, AI's role in law and finance is also remarkable.

Though it consists of pros, we cannot ignore the cons too. Generating unemployment, being emotionless, having no ethics, no creativity and high costs to operate are its significant challenges. Misleading information, using it in illegal activities, and miscoding can cause big losses in economic as well as human casualties. So, we must be careful enough to utilize it.

3.6 AI in Cyber security

Cyber security itself is a complicated and broad subject. The use of AI in cyber security is more advanced. AI can easily detect misleading information in the systems and programs than human beings by risk prioritizing. But cybercriminals also have the same technology to use for their benefit. Thus, it has become a more sophisticated subject.

The rise in cyberattacks is helping to fuel growth in the market for AI-based security products. A July 2022 report by Acumen Research and Consulting says the global market was $14.9 billion in 2021 and is estimated to reach $133.8 billion by 2030.

Currently, the use of AI in cybersecurity has increased largely. Because of the Covid-19 pandemic, many services and works have been changed to remote, therefore, to protect their data and systems AI has been used widely. Similarly, growing trends in the use of the Internet of Things (IoT) and cloud-based security services increased the application of AI in cyber sectors.

3.7 Security in AI

The security in AI ranges from the use of antivirus/antimalware, data loss prevention, fraud detection/anti-fraud, identity and access management, intrusion detection/prevention system, and risk and compliance management. Big companies like Google, Meta, Microsoft, Amazon, SpaceX, etc. are more concerned about the threats of cybercriminals. According to Finch, "AI can be used to identify patterns in computer systems that reveal weaknesses in software or security programs, thus allowing hackers to exploit those newly discovered weaknesses." Thus, if cyber experts can think a step far than those cybercriminals then only AI in cyber security will enhance and progress. Otherwise, cybercriminals will rule the world.

IV. EMERGENCE OF AI IN CYBER SECURITY

One of the earliest examples of an attack on a computer network was the computer worm creeper written by Bob Thomas at BBN, which propagated through the ARPANET in 1971. The program was purely experimental in nature and carried no malicious payload. A later program, Reaper, was created by Ray Tomlinson in 1972 and used to destroy Creeper.

Between September 1986 and June 1987, a group of German hackers performed the first documented case of cyber espionage. The group hacked into American defense contractors, universities, and military base networks and sold gathered information to the Soviet KGB. The group was led by Markus Hess, who was arrested on 29 June 1987. He was convicted of espionage (along with two co-conspirators) on 15 Feb 1990.

In 1988, Robert Tappan Morris, a Cornell graduate student in computer science distributed program from internet. The program was not designed to cause damage but to gauze size of internet. A critical error, however, transformed program causing it to launch first denial of service attack (DoS) also known as Morris Worm.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

Since the first denial of service altar, the cyberattacks have increased rapidly increased along with advancements in cyber security. Traditional cybersecurity methods work based on response to an attack and rely on the static control of security devices. For instance, in case of network intrusion attacks, security systems monitor nodes according to a pre-defined set of rules. These methods wait to be notified that an attacked has occurred. However, with the increasing number of cyberattacks, the traditional approach is no longer useful.

4.1 Brief overview on AI

The concept of AI was proposed in the year 1956 by John McCarthy as the science and engineering of producing intelligent automata, particularly intelligent computer applications. It is concerned with how to make computers think, work, learn and behave intelligently like humans. Cybercrime is now more common, and it threatens the progress of governments, banks, and multinational companies on a daily basis through online hacking. AI systems adopt techniques that can help overcome short comings of traditional cyber security tools through their flexibility and adaptability.

Machines must be trained by learning algorithms. AI methods rely on algorithms. However, even if there is not too much improvement on algorithms, AI can use big data and massive computing to learn through brute force. AI works in three ways:

- Assisted intelligence, which improves what people are already doing
- Augmented intelligence, which empowers people to do things that they could not do
- Autonomous intelligence, which are features of machines that act on their own.

4.2 AI and Cyberattack

Several AI techniques and methods have developed over the time for cyberattacks. These methods have been divided into: Artificial Neural Network, Expert system, intelligent agents, Machine Language.

4.2.1 ANN

ANN is a statistical learning model mimicking the structural and functional behavior of the human brain, first created as a perception in 1957 by Frank Rosenblatt. ANN has the ability to learn and solve problems in different complex domains. It can learn from data in any domain and address absorbing concerns by merging with disparate nerves. In cyber security, ANNs have been used within all four stages of integrated security approach (a holistic categorization of cyber defense framework), consisting of early warning phase, prevention phase, detection phase and reactive/response phase. Intrusion detection techniques avoidance is also applicable to neural networks. Plans were created in DoS detection, software worm identification, spam filtering, zombie identification, analysis of malware, and forensic science.

4.2.2 Expert system

The most commonly deployed AI methods are specialist programs. An expert program is a technology to seek solutions to problems raised either by a customer or a certain technology in a certain technology area. This may be used specifically in decision-making assistance, for example, with medical care, banking, or virtual worlds. There are various optimization techniques for solving complicated problems size from tiny analytical medical diagnoses to highly advanced hybrid systems. A scheme of expertise comprises a knowledge base that contains the specialist analysis of a specific application area. In advisement to the knowledge base, this contains a deduction engine that offers solutions based on that understanding.

According to the reasoning method, expert systems can solve two types of problems:

- Case-based reasoning: This recalls previous similar problem cases, assumes solutions for the past problem case can be used to solve a new problem case. Subsequently, the new solution will be evaluated and might be revised as needed and then added to the knowledge base. This approach continually helps to improve the accuracy of the system and learns new problems gradually.
- Rule-based reasoning: This uses rules, which are defined by experts to solve problems. Rules consist of two parts: a condition and an action. Problems are analyzed in two steps: first, the condition is evaluated and then the proper action will be taken. Unlike case-based systems, rule-based systems cannot learn new rules or modify existing rules automatically.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

4.2.3 Intelligent agent

Intelligent agent (IA) is a self-controlled entity with separate internal decision-making mechanism and a personal objective. It observes via sensors and monitors the domain using actuators and controls its actions towards the achievement of the objectives. Intelligent agents may also learn or use information to achieve their objectives. They may have responsive characteristics, and when communicating with other autonomous agents they may understand and respond to changes in their domain. This enables them to adopt themselves as they attain experience over time through learning and communicating with their environment. IA is created to avoid Distributed Denial of Service (DDoS) attacks.

4.2.4 Machine Language

ML provides systems the ability to discover and formalize the principles that underlies that data, learn through the data, and improve from experience without being explicitly programmed. The process of learning begins with observing data through examples to look for patterns in data and make a better decision in future based on the given examples. With this knowledge, the algorithm can reason the properties of previously unseen examples. ML uses statistics to extract information, discover patterns, and draws conclusions even while using massive amount of data. There are different types of ML algorithms. In general, they can also be classified into three main categories:

- Supervised learning: This type has a training process with a large labeled data set. After the training process, the system must be checked with test data set. These learning algorithms are usually used as a classification mechanism or regression mechanism. Regression algorithm generates outputs or prediction values, which are one or more continuous-valued numbers according to the input. Classification algorithms categorize data into classes and in contrast to regression, classification algorithms generate discrete outputs.
- Unsupervised learning: In contrast to supervised learning, unsupervised learning uses unlabeled training data set. Unsupervised learnings are usually used to cluster data, reduce dimensionality, or estimate density.
- Reinforcement learning: This type of learning algorithm learns the best actions based on the rewards or punishments. Reinforcement can be considered as a combination of supervised learning and unsupervised learning. Reinforcement learning is useful for situations where data is limited or not given.

4.2.5 Bio-inspired computing

Bio-inspired computing is a sub-field of Artificial Intelligence more studied in recent times. It consists of smart algorithms and techniques that mimic the bio-inspired behaviors and attributes to address a broad range of sophisticated academic, as well as real environment problems. Techniques like Ant Colony Optimization (ACO), Evolution Strategies (ES), Artificial Immune System (AIS), Particle Swamp Optimization (PSO), and Genetic Algorithms (GA) are biologically inspired techniques commonly employed in the field of cyber security.

4.2.6 Search

A broad variety of search techniques is created that takes detailed focus on specific search problems into consideration. Although numerous search techniques in AI were established and are commonly used in many applications, they are rarely used as using AI. Of one, the search is embedded in the application stack and is not seen as an AI function. In this sense, dynamic analysis programming is used primarily to address optimal security concerns. Check on besides- or trees, αβ-index, minimal check-in addition stochastic index is commonly used in the applications of gamers and is useful in network security decision-making.

V. MALICIOUS USE OF AI IN CYBER SECURITY

5.1 Social Engineering:

The term"social engineering" is used to describe a wide variety of malevolent behaviors carried out through interactions with other people. Users are duped into divulging critical information or committing security blunders via psychological manipulation.

Attacks by social engineers may involve one or more phases. To prepare for an assault, a perpetrator first looks into the target in order to learn background details like probable avenues of entry and lax security measures. The attacker next makes an effort to win over the victim's confidence and offer incentives for later security-breaking activities, such as disclosing confidential information or allowing access to vital resources.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

The fact that social engineering depends on human mistakes rather than flaws in software and operating systems makes it even more dangerous. Legitimate user errors are significantly less likely to be predicted, making them more difficult to spot and stop than malware-based intrusions.

5.1.1 Phishing

Phishing scams, one of the most common forms of social engineering attacks, are email and text message campaigns designed to make victims feel intimidated, curious, or afraid. Then it prompts people to divulge private information, click on links to nefarious websites, or open attachments that are infected with malware.

Hackers can create a "social bot" that they can use to trick and control a person into doing what they want by using AI methods. These "social bots" are algorithms made to act like people online by creating content and engaging with other users. For instance, social bots can seek access to a website that gives the criminal access to the victim's computer. The romantic chatbot "Cyberlover" was one of the first reported hacks to incorporate AI technology. It was introduced in 2007 to trick chat room members into disclosing private information or clicking on phony links. The bot delivered a tailored dialogue using natural language processing (NLP), raising worries about the skills employed in cybercrime.

Similarly, attackers might pose as trustworthy persons or businesses in order to persuade the victim to open an email or click on a link in order to steal data. The tactic, known as phishing, may potentially be boosted by AI to increase thieves' reach and profits. This was proved by, who carried out an experiment in which a model based on machine learning techniques was used to produce text for posting on Twitter. Because of the character restriction of each tweet, the writers picked this social media site, which allows postings with broken English and abbreviated links to be regarded as acceptable and regular. The findings suggest that the dynamics of such platforms may make machine-generated content more suitable for phishing. Because postings on social media are made in a casual tone, with occasional spelling and grammar errors, and with shorter links, AI may enable an increase in these sorts of assaults.

5.1.2 Manipulation:

In addition to the potential targeted action outlined in the previous sections, a huge number of bots may be created to assist malevolent intent activities. Bots have the capacity to affect public perception and election outcomes. Social bots, for example, can be used to give the appearance that a politician or political movement is more popular by retweeting certain information or repeating hashtags, fooling people on social media sites. A comparable tactic is astroturfing, which is a method that replicates a bottom-up activity in order to give the appearance that a program or someone has extensive grassroots support when there is little or no support. An example of this is when a certain group is in charge of tweeting thousands of tweets from several accounts in order to influence public opinion against or in favor of a candidate in an election see. Astroturfing may be seen in tweets, blogs, news portals, and other online venues, and it can be used to spread misinformation.

Bots may also be employed in public consultations to generate the impression of support for a subject and to tamper with polling. Concerns about this potential grew following the United States Federal Communications Commission's (FCC) consultation on net neutrality. Because the FCC intended to repeal net neutrality safeguards, the agency launched a public consultation including a comment form to solicit public feedback. Gravwell, a data analytics business, discovered that more than 80% of the nearly 22 million comments received by the FCC were generated by bots. Natural language creation was employed in this case to artificially raise opposition to net neutrality protection.

Online profiling and targeting are another application of AI in this context. The Cambridge Analytica controversy is one example of this. According to claims and whistleblowers, the app GSRApp was used to falsely capture their users' personal data, including personality characteristics, which were then used to train an algorithm. This algorithm created personality scores for app users and their Facebook connections, which were then compared to voter data in the United States. The collected data was utilized by Cambridge Analytica to create voter profiles and targeted advertising services. Politicians might use this knowledge to target certain groups of individuals by altering messaging customized to their psychological profile, as well as deception and provocative content. Using these technologies to manipulate people's behavior can have an influence on democratic processes and election outcomes.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

5.2 Falsity and fake news:

"Fake news" is defined as "fabricated material that resembles news media content in form but not in organizational method or aim. The Internet's rapid pace also allows people to create and quickly share material that can reach a large number of people. This circumstance has created an environment conducive to the fabrication and dissemination of misinformation and fake news.

Deep Fakes are computer-generated artificial videos in which images are blended to create new footage depicting events, comments, or actions that never actually occurred. Deep fakes differ from other types of fraudulent information in that they are extremely difficult to detect as false. Fake videos can be created using a machine learning technique called a “generative adversarial network” or GAN. Deep fakes can be used to spread unsubstantiated rumors, conjecture, and purposefully incorrect information, which can have fatal implications, especially during times of uncertainty and societal upheaval. The real risk of false information and deepfake technologies is instilling cynicism or apathy in individuals about what they see or hear online. Does the fact that anything can be phony imply that nothing is real anymore?

Besides this, manipulating content has been made easier through language models such as “GPT-3”. OpenAI's GPT-3 (Generative Pretrained Transformer 3) is a cutting-edge language processing AI model. It can generate human-like text and offers a wide range of applications, including language translation, language modeling, and text generation for chatbots. In less corporate terms, GPT-3 gives a user the ability to give a trained AI a wide range of worded prompts. Texts generated automatically with the program may appear to be authored by a human due to format, word choice, and consistency, fooling the reader due to apparent trustworthiness. Furthermore, as technology advances, messages can be personalized to the audience's preferences, increasing the prevalence of "filter bubbles" and polarization.

The difficulty in recognizing, tracking, and controlling untrustworthy content makes Fake News an exceedingly tough challenge to handle. A successful solution would necessitate advanced digital technology and processes for content assessment. There is also difficulty in dealing with likely Fake Stories: even when there is early proof that a Fake Story is being distributed online, there is little that can be done until it is proven. Another component of the problem is the large number of online users who behave primarily as content distributors/re-sharers without the essential expertise or even real interest in what they share. Users of this class may consume and spread fake news, unknowingly contributing to the spread of fake news. With so much information available, technological advancements, and the speed with which news and information circulate online, it is becoming increasingly difficult to verify anything online. When it comes to verifying online content, critical thinking abilities are required.

Some measures may help to mitigate the harmful impact of AI systems used to generate and disseminate fake news and misinformation. Companies could use special APIs to cross-check information at share time and tell their users if it has previously been flagged or if there are indicators of reduced reliability. It is critical to educate people on how to use digital resources properly- the greater citizens' ability to critically analyze information of the online worlds, the less untrue tales will affect them and their community. Furthermore, information systems and providers play critical roles. As many users access news based on algorithm decisions and search engines, the providers can modify and upgrade their algorithms in order to arrange content differently and to limit the amount of bogus news appearing in their feeds. At the same time, more human monitoring is required, because only this type of control can grasp information in context.

5.3 Hacking

Hackers develop software that employs artificial intelligence to attack a target. They first determine the type of machinery it is, and then, based on the machine, they determine the vulnerability and type of exploit they will send them so they can be extremely accurate in their use. It's a lot more efficient than, say, letting a person make the decision. The AI enabled algorithm is able to elucidate all that attack and send the best to exploit in order to attack that very specific machine or software.

5.4 Deep Fakes

Images can be manipulated with deep fakes. Deepfakes are the most recent advancement in computer images, produced when artificial intelligence (AI) is trained to swap out one person's likeness for another in a recorded

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

video. The most popular method is face-swapping auto encoders with deep neural networks as the auto encoders. A deep learning AI algorithm called the auto encoder is tasked with watching the video clips to learn how the person appears from various perspectives and in various environments, and then mapping that person onto the person in the target video by identifying shared traits.

Here are the few examples about the impacts of uses of deep fakes:

Pornography made approximately 96% of the deep fake videos that Deep Trace discovered online in 2019. This frequently hit the headlines, severely harming the reputations of famous people.

In 2018, a Belgian political party made public a video showing Donald Trump urging Belgium to leave the Paris climate accord in a speech. Although the video may appear to be phony at first glance, with the development of deepfake technology these images and videos could pose severe problems in our rapidly evolving world.

5.5 Fake Accounts

We have observed that if you create a false account and fail to maintain it, the social platform will simply delete the account. This account is likely being used by a bot. So, the hackers use Artificial Intelligence to make the accounts look like it is actually alive and there is a human behind it. For example, Hackers create a Spotify account. Then they create an AI that moves the cursor on the page and plays music that makes sense. They go to one heavy metal music, then another heavy metal music then they go to another rock music. They do modify it to act human-like with the intention that Spotify never deletes their accounts. AI behavior is used to keep those fraudulent accounts open for longer while hiding their automated administration from Spotify. Such social media accounts are created by hackers so that they may sell them later or do insane things with them, such as mass data theft, the development of fake news feeds, the disruption of social marketing, and many other things.

5.6 Online Game Cheating

The most recent generation of gaming cheats can be seen in games that employ shooting at enemies. Hackers have the ability to develop software that uses AI to see what the target is, locate it automatically, aim at it, and fire. This is significant since the esports industry is immensely wealthy reaching a whole $60 billion gaming industry. It transfers a lot of money, so if an esports player can cheat really well, that may result in $100,000 moving in their direction.

It is possible to master some artificial intelligence techniques in order to dominate games. This type of cheating heavily depends on two factors: 1) whether the game's characteristics allow it to be modeled as a computable problem; and 2) whether artificial intelligence research on such a game is available. A violation of fairness may occur if a single participant takes advantage of an operational error.

VI. AI SYSTEMS TO SUPPORT CYBER SECURITY

Enterprises have begun to use AI to handle a widening spectrum of cybersecurity threats, technological obstacles, and resource restrictions by improving the robustness, resilience, and reaction of their systems. Police dogs are a good model for why businesses are utilizing AI to improve cybersecurity. Police personnel employ the specialized talents of police dogs to seek dangers; similarly, AI systems collaborate with security analysts to modify the pace at which operations may be completed. In this sense, the interaction between AI systems and security operators should be viewed as a synergistic integration in which both people and AI systems' distinctive added value are retained and increased, rather than as a competition between the two. The market for AI in cybersecurity is expected to expand from $3.92 billion in 2017 to $34.81 billion by 2025, at a compound annual growth rate (CAGR) of 31.38% during the forecast period. According to a recent Capgemini report, the adoption rate of AI solutions for cybersecurity is rapidly increasing. From one-fifth of the general sample in 2019, to two-thirds of firms planned to deploy them in 2020, the number of organizations using these systems has increased. In cybersecurity, 73% of the sample tried AI applications. Network security is the most common application, followed by data security and endpoint security. There are three major categories of AI use in cybersecurity: detection (51%), prediction (34%), and response (18%).

6.1 System robustness

Robustness is defined as a system's ability to withstand perturbations that fundamentally alter its configuration. To put it another way, a system is robust when it can continue to function in the face of internal

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

or external challenges without changing its original configuration. System resilience requires that AI can discover and profile anomalies in anything that is generally distinct. It should be emphasized, however, that when sophisticated attackers hide by blending in with regular observed behaviors, this strategy might generate a lot of noise from benign detections and false negatives. As a result, more robust and accurate approaches concentrate on detecting specific and immutable attacker behaviors.

By automating the process using AI technologies, you may save time while also discovering more faults than you could manually. Several AI algorithms are being developed to aid with code review. For example, in June 2020, Amazon Web Services' AI-powered code reviewer from Code Guru became publicly available.

The use of AI to improve system robustness has both tactical and strategic implications (i.e., enhancing system security and lowering susceptibility). It does, in fact, mitigate the impact of zero-day attacks. Zero-day attacks take advantage of vulnerabilities that are exploitable by attackers as long as system providers are unaware of them or there is no patch to address them. AI reduces the impact of zero-day attacks on the black market, lowering their value.

6.2 System resilience

Resilience is defined as a system's capacity to withstand and endure an assault by facilitating threat and anomaly detection. In other words, a system is resilient if it can respond to internal and external obstacles by modifying its operational procedures while remaining operational. Unlike system robustness, system resilience entails a fundamental shift in the essential processes of the system that must adapt to the new environment. TAD (threat and anomaly detection) is the most prevalent use of AI systems nowadays. Every day, about 592,145 new unique malware files are created, with the possibility of even more.

AI cybersecurity solutions enable a fundamental change away from signature-based detection and toward more flexible and continuous monitoring of the network when it deviates from its typical behavior. "AI systems can detect any changes that seem abnormal - without the necessity for a predefined definition of abnormal." Deep packet traces performed by internal or external sensors or monitoring software can give information into prospective assaults.

AI is used by businesses to automate cyber defenses against spam and phishing, as well as to identify malware, fraudulent payments, and compromised computers and network systems.

AI is also applied in key forensics and investigation procedures. AI is utilized in particular to provide real-time, customer-specific analysis, increasing the total percentage of malware found and decreasing false positives. As a result, AI data processing aids in the improvement of cybersecurity threat intelligence. Finally, organizations are employing AI-based predictive analytics to evaluate the likelihood of attacks, hence improving network defense through near real-time data provision. Predictive analytics may assist in processing real-time data from many sources and detecting attack vectors by assisting in large data management; filtering and parsing data before analysis; and automatically filtering out duplicates.

6.3 System response

System resilience and response are inextricably linked and logically interdependent, because in order to respond to a cyberattack, you must first detect what is happening and then develop and deploy an appropriate response by deciding which vulnerability to attack and when, or by launching counterattacks. Seven AI systems competed in the 2014 Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge, detecting and repairing their own vulnerabilities while exploiting their opponents' faults without human intervention. Since then, cyberattack prevention has shifted toward systems that can deploy real-time fixes to security problems. AI can assist in reducing the workloads of cybersecurity specialists by prioritizing areas that require more attention and automating parts of the experts' activities. This is especially important when one considers the current shortage of cybersecurity professionals, which is estimated to be four million workers.

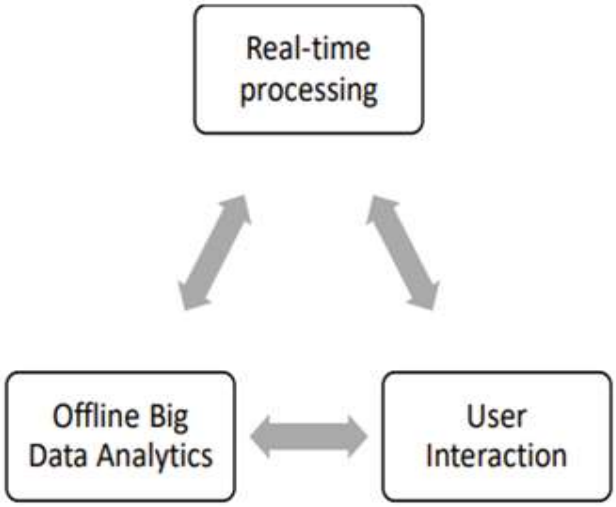
AI can aid in assault response by, for example, deploying semi-autonomous lures that generate a replica of the environment that the attackers plan to enter. These fool them and aid in understanding the payloads (the attack components in charge of carrying out an action to hurt the target). AI systems may also dynamically divide networks to isolate assets in restricted network zones or redirect an attack away from vital data. Furthermore, AI systems may develop adaptive honeypots (computer systems designed to resemble plausible targets of

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

assaults) and honeytokens (data chunks that appear appealing to potential attackers). Adaptive honeypots are more complicated than regular honeypots in that they adapt their behavior in response to attacker interactions. It is possible to deduce the attacker's skills and tools based on its reaction to the defenses. The AI solution learns the attacker's behavior using this tool so that it may be recognized and countered in future attempts.

6.4 Major techniques in the use of AI for system robustness, resilience, and response

Whenever AI is applied to cyber-incident detection and response the problem solving can be roughly divided into three parts, as shown below. Data is collected from customer environments and processed by a system that is managed by a security vendor. The detection system flags malicious activity and can be used to activate an action in response.

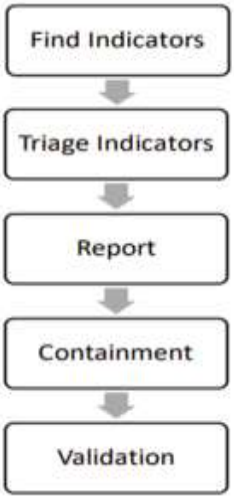


Source: Palo Alto Network contribution to the fourth meeting of the CEPS Task Force.

Companies today recognize that the attack surface is growing massively because of the adoption of the Internet of Things (IoT) and the diffusion of mobile devices, compounded by a diverse and ever-changing threat landscape. Against this backdrop, there are two measures that can be implemented: speed up defenders, slow down attackers.

Companies use AI solutions to automate the detection and response to threats that are already active within the organization's defenses in order to speed up defenders. Traditionally, security teams have spent a significant amount of time dealing with alerts, determining if they are benign or malicious, reporting on them, containing them, and confirming the containment steps. Some of the activities that security operations teams spend the majority of their time on can be assisted by AI.

Notably, this is also one of the keys and most widespread applications of AI in general.



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

The questions the security team can use are the maturity, scale, method of exploit, actions and behavior manifestation of the attack.

VII. CHALLENGES IN CYBER SECURITY

· Large number of input samples is required to build an Artificial Intelligence system. It is highly time consuming to obtain and process the samples and require a lot of resources. Skillful resources essential to execute this technology are costly.

· Four elements of an integrated AI system: perception, learning, decisions and actions run in a sophisticated environment. The elements need to interact and be mutually dependent (e.g., misperception may lead to inconsistent decision). Also, each element has a unique vulnerability that can lead to a successful attack.

· Founded in 2000, the Singularity Institute for Artificial Intelligence (SIAI) alerts investigators that there could be the risk of increasingly accelerated intelligence growth on machines. This can progress to Singularity, defined as follows: Singularity is the technical advancement of intellect that is smarter than an individual.

· As AI technology has been defending against the cyberattacks, the attacks have been increasing and becoming more advanced. It is because of the reduced cost and easy accessibility to the AI and machine learning tools. With time the cyberattacks are going to be more dangerous and difficult to defend against.

· Algorithms can be used by attackers as a tool to advance their attacks. Machine learning algorithms have vulnerabilities and are often targeted by attackers to gain a significant benefit by exploiting them. Incidents reported against spam filters, antivirus engines, and autonomous bots have been increasing in this time.

· Selecting the appropriate machine learning technique for cybersecurity is a major problem. While techniques to analyze big data can be used to enhance security, there is a need to enhance their performance and security. Thus, the varying nature of the problems faced by the asset defenders, makes machine learning tasks used for the security of the cyber system challenging.

· It is hard to avoid missing data in large data because of many reasons including randomness, or missing observations, or corrupt entries. Reliable imputation techniques are needed to resolve it and maintain the completeness of the data set.

· Frequent false alarms are a challenge for the end client. It disrupts businesses by procrastinating essential responses which entirely affects the business efficiency. The process of fine-tuning is a trade-off between minimizing false alarms and sustaining the level of security.

VIII. ADVANTAGES OF AI IN CYBER SECURITY

· By using AI in cybersecurity, businesses can understand and modify threat patterns to identify new dangers and breaches to their system. Finding incidents, investigating them, and removing hazards thereby requires less time and effort overall. Because AI allows for the transition from manual reaction, detection, and remediation to automated remediation, AI offers tremendous opportunities for cybersecurity. AI reportedly lowers the cost of breach detection and response, according to almost two-thirds of Executives (64%) Cost savings for most businesses vary from 1% to 15% (with an average of 12%).

· AI replicates the best human attributes while excluding the worst, taking care of repetitious cybersecurity procedures that might tire your cybersecurity professional. It regularly assists in the detection and management of basic security concerns. It also does a full examination of your network to look for any security breaches that may be hazardous to it.

· Using the available signature codes, also known as the signature-based approach, AI is capable of identifying malware and cyberattacks. Using an AI system, certain codes in malware or cyberattacks are found. The cyber security team might thus have an edge in preventing the assault by matching the signature from recent attacks or a database. To identify the assault, the signature codes must be compared immediately. Thus, the time and resources needed to stop the attack are determined by the type of attack. Prior to the influence of AI technology on cybersecurity, these detections would take a long time to complete, resulting in significant failures and losses.

· Machine learning, a part of AI, analyzes data that already exists to improve its methods and practices over time. It recognizes and grasps typical user behavior and can detect even the slightest change from that pattern. AI may apply this information to improve its own strategies and operations. If you asked a person to sift

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:12/December-2022 Impact Factor- 6.752 www.irjmets.com

through massive amounts of computer usage, logins, and system data, they would never be able to keep up with all the information. But AI can manage all of this data quickly, simply, and continually at any time.

IX. DRAWBACKS OF AI IN CYBER SECURITY

·An imminent risk of the usage of AI in cybersecurity is commonly called adversarial AI, which is a terminology used for the application and utilization of AI for sinister purposes. According to Accenture, a professional IT service company, adversarial AI is something that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder." This takes place when an AI system's neural networks are deceived into misidentifying or falsely representing objects because of intentionally changed inputs by hackers.

So, what is the end goal of doing this? Imagine a hacker making an adversarial picture that can go through the facial recognition software undetected. Most smartphones today have a "FaceId" access feature that uses neural networks to recognize the device owner's face, allowing hackers to simply encroach on this security feature and steal one's personal information without drawing attention.

· Since AI can only be programmed to carry out a specific activity, it is limited and cannot completely replace humans. When it fails to recognize threats that are practically impossible to identify, it might cause problems because they appear to be the original message. Due to the dynamic nature of cyber risks, AI may potentially have trouble detecting dangers. Malware and viruses can improve and change at any time, and the AI system should too in order to remain effective. Additionally, there are more people who practice cybersecurity than cybercriminals, who typically know more about hacking than their counterparts. Cybercriminals can therefore develop a more potent danger that artificial intelligence would find more difficult to identify.

· The fact that AI is basically computer code designed to make sure that it has followed protocols and developed itself in case of anything is one of the most important limits of it. This situation could seem fine because they can grow on their own if necessary. But because the system is completely programmed, anyone may take control of them, manipulate them, and use them as a weapon. Only a few lines of code need to be changed, and after that, the extensive work hours might be exploited as a weapon by the program itself. Therefore, AI technology can be used as a weapon to harm what it was designed to safeguard if the necessary skills and knowledge are gathered.

X. CONCLUSION

One of the most rising advances in information technology is artificial intelligence (AI), and cybersecurity is arguably the field that stands to gain the most from it. New techniques and algorithms are constantly being discovered on the global market. We concentrated on categorizing the ways that AI systems can be utilized or misused by bad actors based on the literature, reports, and prior occurrences that were available. This encompasses injury to one's bodily, psychological, political, and economic well-being, among other things. We looked at the weaknesses of AI models, like unintended consequences, and AI-enabled and -enhanced assaults, like forging.

Understanding the dangers posed by the misuse of AI systems is necessary to develop defenses against attacks on society and vital infrastructure. Additionally, DDoS avoidance experience has shown that if clever ways are applied, security against significant attacks can be achieved with relatively little resource investment. Reviews of publications show that research on artificial neural networks provides the insights of AI that are most directly applicable to cybersecurit. When enough data is available, techniques like statistical analysis could also be used to provide a more thorough picture of the threat scenario. The capacity to prevent attacks and respond appropriately to them is increased by continuously mapping the dangers related to the malicious use and misuse of AI. It is impossible to estimate how quickly general artificial intelligence has developed, but there is still a chance that criminals will take use of new forms of artificial intelligence as long as they are available. In order to achieve the highest level of security, it is vital to incorporate all technical solutions, pertinent procedures, and relevant people into an ISA framework. However, in the end, it is the human element that matters, not just the tools.

XI. REFERENCES

[1] M.Drolet (2020), "The Evolving Threat Landscape: Five Trends to Expect in 2020 and Beyond", Forbes Technology Council; Orange Business Service (2020), "2020 Security Landscape".

[2] McAfee (2020), "McAfee Labs Threats Report", November. 28 Fortinet (2020), Enterprises Must Adapt to Address Telework Security Challenges: 2020 Remote Workforce Cybersecurity Report", August.

[3] INTERPOL (2020), "INTERPOL report shows alarming rate of cyberattacks during COVID-19", August (www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-duringCOVID-19).

[4] Arockia Panimalar.S, GiriPai.U, Salman Khan.K, "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03 | Mar-2018, e-ISSN: 2395-0056, p-ISSN: 2395- 0072.

[5] Ribence Kadel, Riya Kadel, "Impact of AI on Cyber Security", International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 6, Nov- Dec 2022, ISSN: 2581-7175.

[6] KatanoshMorovat, Brajendra Panda, "A SURVEY OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY,". 2020 International Conference on Computational Science and Computational Intelligence (CSCI).

[7] https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

[8] https://en.wikipedia.org/wiki/Cyberattack#:~:text

[9] https://www.simplilearn.com/tutorials/cyber-security-tutorial

[10] https://www.imperva.com/learn/application-security/social-engineering-attack/

[11] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9831441

[12] Fake News - Misinformation, Disinformation, and Propaganda - LibGuides at Cornell University

[13] Is artificial intelligence the antidote to disinformation? | World Economic Forum (weforum.org)

[14] Can artificial intelligence help end fake news? | Research and Innovation (europa.eu)

[15] ChatGPT: Everything you need to know about OpenAI's GPT-3 tool | BBC Science Focus Magazine

[16] Explained: What Are Deepfakes? - (webwise.ie)

[17] Infographic: Spot Fake News - Misinformation, Disinformation, and Propaganda - LibGuides at Cornell University

[18] How to stop Fake News and misinformation using digital technologies | Innovation Mode (theinnovationmode.com)

[19] Atiku, Shidawa.B., Aaron, Achi.U., Job, Goteng.K., Shittu, Fatima, Yakubu, Ismail.Z. (2020). Survey On The Applications Of Artificial Intelligence In Cyber Security, International Journal of Scientific & Technology Research, 9,10, 165-170

[20] AitMaalem Lahcen, Rachid & Mohapatra, Ram. (2022). Challenges in Cybersecurity and Machine Learning. Panamerican Mathematical Journal. 32. 14-33.

[21] Das, Rammanohar & Sandhane, Raghav. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series. 1964. 042072. 10.1088/1742-6596/1964/4/042072

[22] WhoisXML API (2019), "The importance of Predictive Analytics and Machine Learning in Cybersecurity", CircleID, September (2019), "Cybersecurity Workforce Study Strategies for Building and Growing Strong Cybersecurity Teams"
(www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-WorkforceStudy-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482).

[23] [LjubomirLazic (2019). BENEFIT FROM AI IN CYBERSECURITY. The 11th International Conference on Business Information Security (BISEC-2019).
https://www.researchgate.net/publication/336826190_BENEFIT_FROM_AI_IN_CYBERSECURITY

[24] [Trappe, W., & Straub, J. (2018). Cybersecurity: A New Open Access Journal. Cybersecurity, 1(1), 1.https://doi.org/10.3390/cybersecurity1010001]

[25] [Chung, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations.]

[26] [LjubomirLazic (2019). BENEFIT FROM AI IN CYBERSECURITY. The 11th International Conference on Business Information Security (BISEC-2019).]

[27] [Ansari, Dash, Sharma, &Yathiraju. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.
https://www.researchgate.net/publication/364122631_The_Impact_and_Limitations_of_Artificial_Intelligence_in_Cybersecurity_A_Literature_Review]

[28] K. Morovat and B. Panda, "A Survey of Artificial Intelligence in Cybersecurity," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 109-115, doi: 10.1109/CSCI51800.2020.00026.

[29] Das, Rammanohar & Sandhane, Raghav. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series. 1964. 042072. 10.1088/1742-6596/1964/4/042072.

[30] Atiku, Shidawa.B., Aaron, Achi.U., Job, Goteng.K., Shittu, Fatima, Yakubu, Ismail.Z. (2020). Survey On The Applications Of Artificial Intelligence In Cyber Security, International Journal of Scientific & Technology Research, 9,10, 165-170

[31] Wikipedia contributors. (2022, December 23). Computer security. In Wikipedia, The Free Encyclopedia. Retrieved 09:25, December 26, 2022, from:
https://en.wikipedia.org/w/index.php?title=Computer_security&oldid=1129036301

[32] https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

[33] https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html