Prediction of DDoS Attacksusing Machine Learning and Deep Learning Algorithms

Saritha, B. RamaSubba Reddy, A Suresh Babu

Abstract: ***With the emergence of network-based computing technologies like Cloud Computing, Fog Computing and IoT (Internet of Things), the context of digitizing the confidential data over the network is being adopted by various organizations where the security of that sensitive data is considered as a major concern. Over a decade there is a massive growth in the usage of internet along with the technological advancements that demand the need for the development of efficient security algorithms that could withstand various patterns of the security breaches. The DDoS attack is the most significant network-based attack in the domain of computer security that disrupts the internet traffic of the target server. This study mainly focuses to identify the advancements and research gaps in the development of efficient security algorithms addressing DDoS attacks in various ubiquitous network environments.***

Keywords: DDoS attack, machine learning, Deep learning, Volumetric attacks, protocol attacks

I. INTRODUCTION

Now a day'swith the advent of 4G, 5G networks and economic smart devices there is a massive growth in the usage of the internet that has become a part of daily life. A vast range of services provided over the internet in diverse application areas such as business, entertainment, and education, etc. made it a vital component in framing various business models. This context made security over wireless networks as the most important factor while using the internet from unsecured connections[1]. Different security algorithms and frameworks are developed to enable protection from Internet-based attacks while devising high-performance IDS (Intrusion detection systems) which act as a defensive wall while confronting the attacks over internet-based devices. Distributed architecture based computing environments like cloud computing and IoT are more prone towards DDoS attacks in which multiple devices are coordinated to launch attacks over distributed targets.

DDOS attacks are primarily launched in the context of exhausting the connectivity and the processing of the target server resources in which it enables the access constraints to the legitimate users to utilize the services provided by the target server that leads towards the partial unavailability or total unavailability of the services. The phenomenon of distributed computing is based on the one-to-many dimension in which these types of attacks may cause a possible amount of damage to the server resources [3]. It is observed from the previous research studies that the damage capacity, as well as the disrupting nature of the DDoS attacks, is gradually increased with the rate of internet usage.

Revised Manuscript Received on November 15, 2019

Saritha, Research Scholar, Department of Computer Science Engineering, JNTUA College of Engineering, Anantapuramu, Andhra Pradesh, India

B. RamaSubba Reddy, Professor, Department of Computer Science Engineering, SV College of Engineering, Tirupati, Andhra Pradesh, India

A Suresh Babu, Professor and HOD, Department of Computer Science Engineering, JNTUA College of Engineering, Anantapuramu, Andhra Pradesh, India

As an outcome of several research studies, there are several statistical mechanisms to detect the intrusions in the network traffic on analyzing the source and destination IP address, detection based on the port degeneration values, destination decay and wavelet-based analysis, etc [4]. With the massive usage of cloud computing and IoT technologies, the model for DDoS attack has been changing frequently with the frameworks of computing. Design and development of the novel statistical models are time-consuming as it will not be able to sustain rapid and dynamic changes within the network. The major drawback observed while constructing the statistical model is that it is bounded towards a single application scenario and the range of complexity in building and maintain the model. In the context of resolving the problems of the statistical models in detecting and predicting DDoS attacks, the researchers have focused on the deep and machine learning algorithms to develop context-aware prediction models that are bounded to be less complex and high performance-centric. It is evident from various research studies that Machine learning algorithms have demonstrated high performance while adopting towards the dynamic changes within the network and predicting the network traffic along with the intrusions within the network.

Machine learning and deep learning algorithms have the ability to identify unconstrained information within massive amounts of data which draws the attention of various researchers to study the application of these strategies. Researchers in [2] have utilized the access patterns of various clients, flow size constrained to the network traffic and chronological behavior while devising machine learning models to classify abnormal network from a normal network in the circumstance of controlling the servers. The major advantage of machine learning models is that data is updated dynamically within the prediction model such that the changes within the network could be easily identified. Few studies evident that still there are few deficiencies while adopting machine and deep learning algorithms because of its substantial computational complexity. DDoS attack patterns vary from different network components. Primarily DDoS attacks involved in devastating the target remote server or network traffic towards the server could be categorized into three categories that include application-layer based attacks, Protocol level attacks, and Network traffic attacks.

The contribution of this article is threefold. Firstly, the attack patterns and characteristic features of DDoS attacks are analyzed to identify the common motivational aspects behind the attack. Secondly, a systematic review of various studies involved in the application of machine and deep learning algorithms are detailed. Further, an attempt of identifying research gap is made based on the evidence-based research to analyze the success rate machine and deep learning algorithms in the detection and prediction of DDoS attacks in an

unconstrained network environments.

The rest of the article is organized as follows: Systematic procedure of the review and research framework adopted for the review along with the procedure involved in the selection of the studies is detailed in Section 2. Section 3 provides details about various types of DDoS attacks while Section 4 summarizes the review of the various existing machine and deep learning models for detection and prediction of DDoS attacks Section 5 addresses the research gaps and open challenges based on the review results. Finally, Section 6 concludes the paper along with further research directions.

II. RESEARCH METHODOLOGY

This paper adopts the procedure of conducting a systematic literature review (SLR) from [5]. The main intention of conducting SLR is to execute a well-planned literature study in the context of answering the Research Questions that are framed at the initial stage of the study. SLR enables the researchers to discover, evaluate and amalgamate the research studies conducted by various network security researchers. The development of SLR includes the following process:

- Development of review protocol that includes complete procedure involved in conducting SLR of predicting DDoS attacks using the machine and deep learning applications.
- Enumerate the Research Questions based on the PICO search strategy [6] in the context of DDoS attacks.
- Primary and secondary selection strategy to filter the articles addressing the research questions.
- Synthesize the selected studies to answer the research questions.

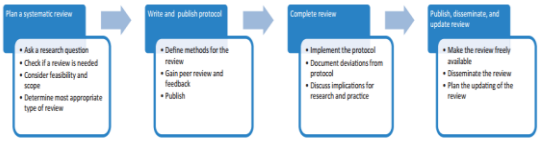

Figure 1: SLR Process [6]

2.1 Research Questions

The most important step in the systematic review protocol is defining Research Questions (RQ's). The streamline of the study is initially maintained by RQ's. In the context of defining RQ's, this article adopts a PICO strategy that involves various components that elevate the quality of the study. The research questions framed on addressing a DDoS attack are as follows:

RQ1	What are the various types of DDoS attacks that could be referred to as a major concern in the context of distributed networks?
RQ2	What are various existing machine learning algorithms devised to address DDoS attack prediction?
RQ3	What are the various tools and data sets utilized?
RQ4	How machine learning and deep learning techniques influence the research in the prediction of DDoS attacks

2.2 Search strategy

The intention of the systematic study is to discover, compare and classify the existing research studies within the class imbalance problems using a systematic procedure. Popular scientific databases like IEEE, SPRINGER, ACM, SCIENCE DIRECT and Google scholar libraries are utilized for the searching process using the following search strings in different combinations.

DDoS Attacks**OR** Intrusion detection Systems **OR** Network Security

AND

Application layer attacks **OR** Network Traffic based attacks **OR**Protocol Attacks

AND

Distributed Computing**OR** Cloud Computing**OR** Internet of Things (IoT)

AND

Machine learning Algorithms**OR**Deep learning Algorithms **OR** Hybrid Mechanisms

AND

Systematic Study **OR** SLR **OR** Mapping Study **OR** Review

In the initial cases during the study using the above search string we have identified around 220 research papers in specific to the class imbalanced problems that are published in the past decade. Table 2 indicated different online mechanisms utilized for the process of searching relevant studies.

Table. 2 Various Scientific databases considered for SLR

S.No	Database	No. Of Papers
1	IEEE	108
2	ACM	10
3	SPRINGER	42
4	SCIENCE DIRECT	35
5	GOOGLE SCHOLAR	25
Total		220

2.2.1 Preliminary selection

In the preliminary phase, of the selection, 300 related articles are extracted from the scientific databases using the search strings in which articles are scrutinized based on the relevancy of the title towards the problem statement and further the remaining are ignored. Additionally, the articles from the thesis, book chapters, short papers and papers communicated in non-English language are ignored from the study. The inclusion and exclusion criterion of the articles is made by analyzing the title, abstract and conclusion of the articles. Such that filteringof the appropriate articles is accomplished with relevance to the class imbalance problem.

Title: **(DDoS attacks**OR **Intrusion detection systems**OR **Machine learning model**OR **Algorithm Centric techniques** OR **Application layer attack**OR**Deep Learning Model**OR **Network Attack**OR**Hybrid Mechanisms** OR**Network Traffic**OR**Software-defined networking** OR **Cloud Computing)**

AND

Abstract: (Machine learning mechanisms OR **Techniques and approaches of network security** OR **Deep Learning mechanisms)**

2.2.2 Selecting the articles based on the Implementation details and Data sets Utilized

In this phase, we further analyze the quality of the articles based on the implementation details furnished in the article, such that the article is thoroughly examined to identify the algorithm utilized to resolve the DDoS attacks in classification along with its implantation with real-world dataset are considered for the review process. Further, the articles with a detailed description of the algorithm are considered based on the novelty of the technique. Based on the opinions and suggestions of the experts with experience in the process of conducting a systematic review in various domains, search strings are modified to be more focused on the topic and furnished above. Feedback from a team of research experts is considered to enhance the process of SLR. The detailed discussion of various algorithms, techniques, and approaches regarding the prediction of DDoS attacks is provided in section 3. The inclusion and exclusion criteria framed for the study selection as shown in table 3. Finally, 34 articles are considered for the review related to DDoS prediction and detection based on the inclusion and exclusion criteria.

Table 3. Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Articles that include prediction and detection techniques associated with the machine and deep learning algorithms	Articles with an ambiguity in the context of the implementation of the proposed mechanisms
Articles prepared in the context ofevidence-based research in predicting DDoS attacks with a clear representation of implementation details that includes datasets, tools, and mechanisms	White papers and Lecture notes regarding the prediction of DDoS attacks using the machine and deep learning techniques
Articles that are primarily implemented in the computer science domain	Articles are written in other than the English language
Articles that are written in the English language	

III. CHARACTERISTICS AND CLASSIFICATION OF VARIOUS DDOS ATTACKS

The primary characteristic of the DDoS attack is gaining control over the network of remote servers in the context of launching an attack. Initially, malware is injected to the computer machines over the network which in turn transform each machine as an intruder through which the targeted server accessed using its IP address or Network traffic and various components of the network connection. This context may cause a situation in which the authenticated users will not be able to utilize the premium services enabled by the server. There are various types of DDoS attacks based on the network layer on which the attack was being launched. Classification of DDoS attacks is as follows:

a) Application Layer Attacks*:* The primary objective of the application layer attacks is to wear out the resources of the targeted server. This kind of attacks mainly focuses on the dynamic web pages that are generated by the server and in turn delivered to the client upon an HTTP request. Serving an HTTP request from the server side is considered as a complex process as it is involved in loading multiple sets of files based on the database transactions in the process of generating access to the web page.

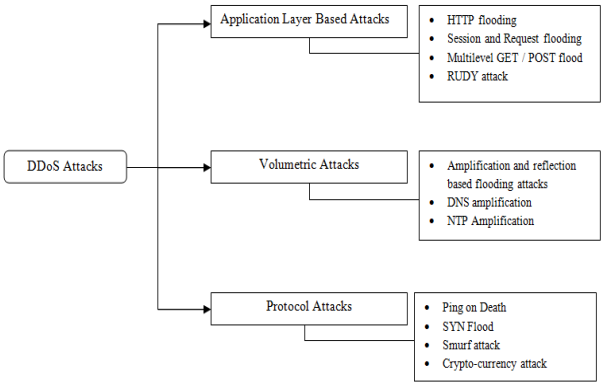

Figure 2: Classification of DDoS attacks

b) Volumetric Attacks: This kind of attacks mainly concentrate on the congestion levels of the network in the context of the target server. The objective of this attack is to create and unnecessary congestion over the target servers network by means of disposing large amounts of data to the server over the network using various amplification techniques. The amount of traffic generated using volumetric attack will be able to create disruption over the server's network.

c)Protocol Attacks:These attacks mainly concentrate on exhausting the server resources interms of the processing speed. These attacks mainly concentrate on the network and transport layers through which it tries to exhaust the processing capacity of the servers as well as the middleware network resources that include firewall, load balancers, and networks switches. This attacks always try to make use of TCP handshake mechanism and IP protocol with a spoofed IP address to gain access to the target machine.

IV. REVIEW OF MACHINE LEARNING AND DEEP LEARNING APPROACHES IN PREDICTING DDOS ATTACKS

Detection and prediction techniques of DDoS attacks are broadly classified into four major areas that include soft computing, knowledge-based mechanisms, Statistical methods and Machine learning methods based on the research studies conducted by Prasad et al [8].Further few research studies have categorized the detection methods based on DoS-misuse detection as well as anomaly detection.Table 4 Synthesises the information based on the different classes of DDoS attack prediction and detection mechanisms. IDS (Intrusion Detection System) that works based on the attack signatures require an individual administrator that concentrates on the pattern of the attack to predict and identify the attacks, in this scenario huge manpower is required for creating, deploying and testing the attack signatures over the network. Addressing this problems usage of machine learning algorithms [9] will automate the process of

predicting DDoS by learning attack signatures with improved accuracy.

Table 5. Categories of various techniques to detect DDoS attacks

Category	Description
Knowledge-based Mechanisms	These methods intend to identify the attacks whose signatures are already aware and the same are used to track the patterns of the new attack
Machine Learning(ML) based Mechanisms	ML and advanced learning mechanisms like deep learning (DL) effectively predict the hidden patterns of network information to predict and classify various attacks
Statistical Methods	Modelling the statistical patterns of the normal attacks and use these inferences to classify the dynamically generated network traffic to predict network traffic based attacks
Soft Computing Mechanisms	Derive learning patterns based on the optimization techniques to optimize network traffic for predicting attacks

The recent studies presented by Gil and Poletto [10] Details about the statistical technique derived based on a multi-level tree that analyses the online packet statistics in this context the researcher had was you made that the bracket rates in between the hosts are constrained to be proportional to each other.

4.1 Machine Learning and Deep Learning Mechanisms to predict Application layer DDoS Attacks.

Application layer DDoS attacks generally deal with the concept of botnets. Most of the DDoS attacks were launched based on the open-source tools which in turn different organizations will not be able to identify the traces of attacks.The researchers in [11] have analyzed the context of coding that lies behind various popular DDoS attacks that include agobots, SpyBot, SDbot, and Rbot.The main objective here is to gain knowledge with respect to the patterns of various DDoS attacks that would be utilized to mitigate the effect of future DDoS attacks.

Botnet based DDoS attacks and its effect was studied by Almariet.al[12] which mainly focused on the application layer that may cause the security damage to their business through which it is identified to be a major concern in the context of the business.Possible solutions and further research directions have been summarised in this research. Most widely used method to defend DDoS attack is Pushback method as this method utilizes the concept of congestion control. This method mainly comprised of selective drop as well as detection stages through which it could efficiently defend application-layer attacks. Further, the researchers in [13] have extended the pushback technique based on the puzzle-solving method in which the target server will send a puzzle over the network to the client to authenticate whether the reliable client has been connected to the serve.The attack patterns and principles are evaluated and presented in [14] Through the study of existing DoS attacks and their patterns that label is the distributed and wireless network systems.

The analysis of the botnet based attack similarity in gaining access to the web application was discussed in detail in [15]. SVM (Support Vector Machine) based mechanism was proposed to detect these attacks based on the pattern of requests generated by the clients and analyzed the context thoroughly based on the request rhythm matching algorithm. Addressing the problem of the similarity of information flow over the network by similar bots Xiao et al in[16] have proposed a KNN based algorithm that identifies the network traffic generated by similar bots. An artificial neural network-based Radial Basis Function (RBF) is utilized to detect the features of the patterns through which the router will be able to classify the network traffic as into the category of normal or attack. In this context, if the input network traffic is analyzed as an attack based pattern then it is filtered and triggers the alarm based on the source IP address.

Further, in [17], the authors have utilized a data mining based mechanism in which a prior association and FCM clustering algorithms are used to define a threshold value to detect an attack based on the extraction of the network traffic as well as the network packet protocol. Authors in [18] have proposed a mechanism based on the grey relational analysis and decision tree system in which they have utilized at most 15 diverse attributes that inturn monitor and compile the input and output traffic using TCP ACK and SYN flag rate to analyze the pattern.The main context of using decision tree here is to identify the abnormal flow of the traffic.

4.2 Detection and Prediction of Volumetric attacks

DRDoS attacks are a category of DDoS attack that is prone to protocol layer attack. DRDoS(distributed and reflective denial of service attack) mainly concentrates on exhausting the resources of the target server based on deploying continuous requests to the server and spoofing the IP address of the remote server. In the context of DRDoS attacks, two factors play a vital role in detecting the impact of the attack such that initially, attackers will try to amplify the network bandwidth by misusing the network protocol on generating unnecessary traffic.As the IP address spoofing mechanism is constrained to TCP handshake policy review of different TCP protocols has been excluded. It is observed from the research studies that the following protocols shown in table 6 are prone to DRDoS attacks.

Table 6. Protocols that are more prone to the DRDoS attacks

Protocol	Description
NTP	This protocol mainly related to the tyme synchronization with 123 ports
NetBios	It acts as a Name Service Protocol for API that represents NetBios
DNS	Domain name resolution protocol with 53 ports
SSDP	UPnP- enabled hosts are discovered using this protocol with 1900 ports
SNMP2	It usually monitors the devices that are attached to the network with around 161 ports
Sality	It is considered as malware dropper protocol that works on P2P mechanism
ZAv2	It enables rootkit for P2P based computing

Aangnostopoulos et.al [19] in his research study have developed a mechanism that amplifies DNSand demonstrated the scenario of the real attack. The demonstration of the work include two groups of packets that includes 3539 packets with the size around 5MB and 3110 packets with size around 3.5 MB that are recorded on the target server with the range of amplification in between 37 to 44 such that the individual attacking node will have the capability of releasing 3 to 4 Mbps of unnecessary traffic to victim. Further, the research

work in [20] utilizes DNS query in the context of analyzing DNS based DDoS attack amplification that eventually targets the remote server.

Kumbourakis et.al in his article [21] have devised a mechanism that operates on individual-centric mapping phenomenon that mainly works on the request-response scenario of the DNS query wherein the context of the DNS amplification there be an absence of such kind of querying procedure. Weizhang et.al [22] in the context of detecting the anomaly has made use of the data mining based approaches that classify the traffic of the DNS query. UzmaSattar et.al [23] have developed a modified bloom filter based mechanism such that his research study that demonstrates the process in which the filter stores the request generated to the server such that if the response from the server is delivered in specific time period then it allows that particular IP address else the IP address is blocked. Further, the studies in [24] addressed the context of the trivial file transfer protocol through which the amplification factor is elevated. Prediction and monitoring of the DNS traffic caused by the botnet will gradually increase as synthesized in the literature[25][26]. Addressing the usage of the artificial neural network in the context of detecting and predicting on classifying normal data packet and DDoS attack intruder packets within the realtime environments on blocking the forged data packets before these packets arrive the target server.

TejmaniSinam et.al [27] in the context of detecting VOIP over the network have devised amachine learning technique. In this research study, the main objective is to classify the application traffics of VOIP based on the usage of the application The role of the proposed machine learning algorithm is to classify the VOIP traffic from forged data packets.

4.3 Detection and prediction of Protocol attacks using Machine learning Mechanisms

A research study conducted in [28] addressing the context of smurf attack in which a large number of ICMP data packets are transported towards the target remote server in such a way that it is flooded over with ping messages that include five different steps in the process of executing the smurf attack without any inconsistencies. The most common effect of a smurf attack is that it will cripple the target server with unlimited ping such that it may cause huge revenue loss. In a few cases, certain smurf attacks are launched along with rockets that allow accessing the system to shutdown the server. Further in [29], the research study focus on the context of designing a packet marking algorithm that was based on the ICMP trackback phenomenon to predict a DDoS attack. In this scenario, the work is evaluated based on two different mechanisms in the initial context a virtual machine is utilized to trackback the system further in the next step the algorithm evaluates the data packets launched by the attacker.

Data transmission is initially established between the client and server using TCP handshake protocol and usually, this phenomenon is known as three-way handshake mechanism of TCP where the client and the server are initially communicated with the message as n SYN message and acknowledgment as SYN-ACK to establish the connection. In this scenario, if the attacker floods SYN messages continuously to the server irrespective of the ACK then it is called a TCP-SYN flooding attack.This attack is usually launched by spoofing the IP address[30].

The research studies in [31] indicate that the size of the IP packets as 65535 bytes that includes the size of the headers. The server will not be able to handle the requested ping packet that is larger than the indicated maximum size that breaches the IP regulations. In general, the attackers will flood the forged data packets in the form of fragments to the servers that are reassembled by the target servers if an oversized packet fragment occurs it is prone to be a ping of death packet that crashes the target server.

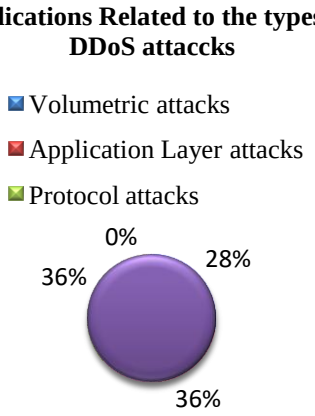

Figure 3 Quantitative analysis of publications related to Different types of DDoS attacks

V. ANALYSIS AND QUALITY ASSESMENT OF THE REVIEW

The systematic literature review presented in this article made an attempt to identify the role of machine learning and deep learning approaches in the context of detection and prediction of DDoS attacks that could be executed in various distributed computing environments and software-defined networking environments.The quality assessment of the review is conductedbased on mapping the research questions (RQ's) framed in section 2.1. Initially, the fundamentals of DDoS attacks are detailed in section 3 that will map to RQ1. The detailed review of the existing techniques that specify RQ2 is demonstrated in section 4. Figure 3 demonstrates various existing techniques that briefly explain the range of publications over the years addressing different types of DDoS attacks.Table 7 provides the synthesis of various popular works along with their implementation details.

Table 7 Analysis of countermeasures for different types of DDoS attacks

Author Names	Parameters	Prediction and Detection level of DDoS	Dataset	Performance analysis
S. Hameed et al [32]	Packet header and packet protocol, Source, and destination IP along with Timestamps	Quantifiably high-frequency levels of detection	Case study based experimental data	Processing power, memory and measure utility
S. Behal et al [33]	Packet header and time size window	Fluctuated levels depending on the flash crowd	CAIDA and FIFA	Precision and recall, classification rate and F measure
S. Y. Nam et al [34]	Black and white lists of the threshold values	DDoS attacks constituted too high rates	Case study based experimental data	Accuracy of prediction and speed of detection
S. N. Shiaeles et al[35]	Hop Count, Source MAC address and agent-based on the web browser	DDoS attacks constituted to high rates	LLDOS and DARPA	Rate of detecting DDoS attack
J. Wang et al[36]	Weigh moving algorithm and probability analysis	DDoS attacks constituted to high rates	Case study based experimental data and Clark net	False-positive
Q. Liao et al[37]	Frequency of the request interval and request sequence analysis	DDoS attacks constituted to high rates	Weblogs based on university data	Accuracy of prediction and Rate of detecting DDoS attack
K. Johnson Singh et al[38]	Genetic algorithm-based multi-layer perceptron	DDoS attacks constituted to high rates	Dataset generated based on BONSI	Sensitivity analysis and accuracy
N. Hoque et al[39]	IP indexing of source server	DDoS attacks constituted to high rates	TUIDS and DARPA	Accuracy of prediction and Rate of detecting DDoS attack
A. Aborujilah et al [40]	TCP based covariance matrix	DDoS attacks constituted to low rates	Case study based experimental data and KDD cup 99	False-positive and negative

5.1 Research Gap

Based on the detailed analysisof the various existing techniques selected in the literature it is identified that most of the existing solutions that provide countermeasures for DDoS attacks are based on the knowledge-based and statistical analysis methods. Adoption of Machine and deep learning mechanisms for predicting DDoS attacks was in the infant stage of the research. Figure 3 depicts that the countermeasures for detection and prediction of DDoS attacks in different layers are given importance but these techniques are developed only on the basis of traditional techniques and it is observed that each time detection of DDoS attacks is given a higher priority.

Further, the research on the behaviour of various DDoS attacks and their countermeasure execution in the context of distributed computing environments like cloud computing, grid computing, and IoT are given the least priority. Utilization of deep learning algorithms for the classification and prediction of DDoS attacks is considered a challenging aspect of research. Design and development of various deep learning and machine learning-based solutions for different types of DDoS attacks in various layer and analyzing their behaviour when deployed in distributed computing environments will be fruitful research for future consideration.

VI. CONCLUSION

This article includes the systematic study of literature in the context of detecting and predicting DDoS attacks on utilizing machine learning and deep learning algorithms. In this study, after the thorough filtering process, 34 articles are considered for the study through which it is observed that most of the existing research includes solutions and algorithmic patterns that are framed based on the statistical algorithms such that most this algorithms suffer from computational complexity. Additionally, there are very few publications addressing the scope of predicting the DDoS. This study outlines the synthesis of various DDoS attacks and their countermeasure algorithms that enables the researchers of the next generation to easily identify the research gap in the context of applying machine learning algorithms to automate the process of predicting DDoS attacks in various distributed networks.

REFERENCES

1. Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM ComputerCommunication Review 34.2 2004, 39-53.
2. Dietrich, Sven, Neil Long, and David Dittrich. "Analyzing Distributed Denial of Service Tools: The Shaft Case." LISA. 2000, pp. 329-339.
3. Arbor Networks, "Worldwide ISP Security Report", Sept. 2005, pp. 1-23.
   Lee, Wenke, and Salvatore J. Stolfo. "Data mining approaches for intrusion detection." Usenix Security. 1998, pp. 1-10.
4. Barbara Kitchenham and Pearl Brereton. A systematic review of systematic review process research in software engineering. Info. Softw. Technol. 55, 12 (2013), 2049–2075
5. Adrian Sayers, "Tips and tricks in performing a systematic review" British Journal of General Practice 2008; 58 (547): 136. DOI: https://doi.org/10.3399/bjgp08X277168
6. Santos CMC, Pimenta CAM, Nobre MRC. The PICO strategy for the research question construction and evidence search. Rev Latino-am Enfermagem 2007 maio-junho; 15(3):508-11
7. K. Prasad, A. R. M. Reddy and K. V. Rao, "DoS and DDoS attacks: defense, detection and traceback mechanisms - a survey," Global J. of Computer Science and Technology: E Network, Web & Security, vol. 14, no. 7, pp. 15-32
8. Ahmad Riza'ainYusof* and NurIzuraUdzir, Systematic literature review and taxonomy for DDoS attack detection and prediction Int. J. Digital Enterprise Technology, Vol. 1, No. 3, 2019
9. T. M. Gil, M. Poletto, "MULTOPS: A datastructure for bandwidth attack detection". In USENIX, editor, Proceedings of the 10th USENIX Security Symposium, August1317, Washington, vc DC, USA, 2001
10. Kumarasamy, S., &Asokan, R. (2012). Distributed Denial of Service (DDoS) Attacks Detection Mechanism. arXiv preprint arXiv:1201.2007, pp. 41-49
11. Alomari, Esraa, et al. "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art." arXiv preprint arXiv:1208.0403 2012, pp. 24-32 .
12. J. Li Yong, L. Lin Gu, "DDoS Attack Detection Based On Neural Network", Aware Computing (ISAC), 2010 2nd International Symposium 196 – 199, IEEE 2010.
13. F. Gumus, C. OkanSakar, Z. Erdem, O. Kursun, "Online Naive Bayes classification for Network Intrusion Detection", 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2014
14. P.Arun Raj Kumar, S.Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems", Elsevier, Computer Communications 36(2013), pp. 303-319, 2012.
15. Zhu, Xiaojin, and Andrew B. Goldberg. "Introduction to semisupervised learning." Synthesis lectures on artificial intelligence and machine learning 3.1, 2009, pp. 1-130.
16. Fu, Z., Papatriantafilou, M., &Tsigas, P. (2008, October). Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. In Reliable Distributed Systems, 2008. SRDS'08 pp. 63-72
17. Yau, David KY, et al. "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles." IEEE/ACM Transactions on Networking (TON) 13.1 2005, pp. 29-42.
18. MariosAnagnostopoulos, 2013. *DNS Amplification AttackRevisited*. Computer & Security, Vol. 39,Part B, November 2013, pp. 475-485
19. A. Buscher and T. Holz. Tracking DDoS Attacks: Insights ¨ into the Business of Disrupting the Web. In *Proceedingsof the 5th USENIX Workshop on Large-Scale Exploitsand Emergent Threats (LEET)*, San Jose, CA, USA, April 2012
20. GeorgiosKambourakis, 2007. *A Fair Solution to DNSAmplification Attacks*. Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 2007
21. WeizhangRuan, 2013. *Pattern Discovery in DNS QueryTraffic*. Procedia Computer ScienceVol. 17, 2013, pp. 80-87
22. UzmaSattar, 2013. *Secure DNS from amplification attack byusing Modified Bloom Filters*. Eighth International Conference on Digital Information Management (ICDIM), 2013, pp. 20-23
23. Richard Sharp, Ed Warnicke, .Wireshark User's Guide.https://www.wireshark.org/docs/wsug_html_chunked/.
24. SergiosTheodoridis, KonstantinosKautroumbas. Pattern Recognition. Second Edition.
25. Decision Tree Learining, http://www.ke.tudarmstadt.de/lehre/archiv/ws0809/mldm/dt.pdf. Accessed date 15 December 2015.
26. TejmaniSinam, NandaraniNgasham, Pradeep Lamabam, IrengbamTilokchan Singh, Sukumar Nandi, 2014. *EarlyDetection of VoIP Network Flows based on Sub-FlowStatistical Characteristics of Flows using Machine LearningTechniques*. 2014 IEEE International Conference on Advanced Networks and Telecommunications Systems (ATNS), 2014, pp. 1– 6
27. Alan Saied, Richard E. Overill, Tomasz Radzik, 2016.*Detection of known and unknown DDoS attacks usingArtificial Neural Networks*. Neurocomputing, Vol. 172, January 2016, pp. 385-393.
28. US-CERT, DNS Amplification attack, https://www.uscert.gov/ncas/alerts/TA13-088A. Accessed date 23 September 2015.
29. Xi YE, Yiru YE, 2013. *A Practical Mechanism toCounteract DNS Amplification DDoS Attacks*. Journal of Computational Information Systems, Vol. 9(1), 2013, pp. 265-272.
30. Richard Sharp, Ed Warnicke, .Wireshark User's Guide. https://www.wireshark.org/docs/wsug_html_chunked/.
31. S. Hameed and U. Ali, "HADEC: hadoop-based live DDoS detection framework," *EURASIP Journal on Information Security*, vol. 2018, no. 1, p. 11, 2018.
32. S. Behal, K. Kumar, and M. Sachdeva, "D-FACE: an anomaly based distributed approach for early detection of DDoS attacks and flash events," *Journal of Network and ComputerApplications*, vol. 111, pp. 49–63, 2018
33. S. Y. Nam and S. Djuraev, "Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 7, pp. 2512–2531, 2014
34. S. N. Shiaeles and M. Papadaki, "FHSD: an improved IP spoof detection method for web DDoS attacks," *Computer Journal*, vol. 58, no. 4, pp. 892–903, 2014
35. T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer DDoS attack using time series analysis,"*Journal of Control Science and Engineering*, vol. 2013, pp. 1–6, 2013
36. Q. Liao, H. Li, S. Kang, and C. Liu, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," *Security and Communication Networks*, vol. 8, no. 17, pp. 3111–3120, 2015.
37. K. Johnson Singh, K.)ongam, and T. De, "Entropy-based application layer DDoS attack detection using artificial neural networks," *Entropy*, vol. 18, no. 10, p. 350, 2016
38. N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: trends and hallenges," *IEEE CommunicationsSurveys and Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.
39. A. Aborujilah and S. Musa, "Cloud-based DDoS HTTP attack detection using covariance matrix approach," *Journal ofComputer Networks and Communications*, vol. 2017, Article ID 7674594, 8 pages, 2017

AUTHORS PROFILE

Ms. Saritha Anchuri, Research scholar in JNTU college of Engineering received M.Tech from Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal. At present she is working as assistant professor in the Department of CSE at Sri Venkateswara Engineering College, Tirupathi. She is having 10 years of teaching experience. She has guided 10 B.Tech Projects and 6 M.Tech projects. She has worked in various Engineering colleges in Andhra Pradesh.

Dr. B. RamaSubbaReddy, Professor and Vice principal of Sri Venkateswara College of Engineering, Tirupathi has received PhD from Sri Venkateswara University, Tirupathi. He worked in various prestigious institutions both in Telangana and Andhra Pradesh as Head of the Department and is having more than 20 years of teaching experience. His areas of interest include Data mining, Computer Networks, Network security and cryptography, Machine Learning. He has guided more than 50 B.Tech projects and 15 M.Tech projects.

He is guiding 4 PhD scholars. He has published many papers in reputed journals.

Dr. A.Suresh Babu, Professor and Head of the Department, JNTUACEA has received PhD from JNTU, Hyderabad, India. Since then he Served as Head of the Department , Computer Science & Engineering, JNTUACE, Pulivendula ,Chairman of UG & PG Board Of Studies, CSE, JNTUACE(Autonomous), Pulivendula, worked as Addl. Controller of Examinations, JNTUA from Feb 2009 to March 2011,Worked as Deputy Warden for I YEAR Boys Hostel, JNTUACEA. Currently he is working as Professor and Head of the Department of Computer Science and Engineering in JNTU college of Engineering, Anantapuramu. His research areas include Data mining, Cloud Computing, Big Data Analytics. He has guided more than 60 B.Tech projects, 50 MCA projects, 40 M.Tech Projects and 8 Ph.D. Scholars. He has published more than 50 papers in reputed journals.