Leveraging Machine Learning and Deep Learning Technologies for Predicting Distributed Denial of Service Attacks: A Systematic Review Analysis

Jean Paul NDAYIZIGIYE
Student at UDOM, Master in IT
Department of Information and Systems Technology,
University of Dodoma(UDOM), Tanzania

Dr. Mohamedi Mjahidi, Dr. Gilbert Gilbert
Lecturer, College of Information and Virtual Education (CIVE), UDOM

Abstract:- Technologies, especially Fourth Industrial Revolution Technologies (4thIRTs) like Big Data Analytics (BDA), Artificial Intelligence (AI), and Cloud Computing (CC), among others, have led to exponential growth in intrusions and assaults across Internet-based technologies. One of the fatal dangers rising is the distributed denial of service (DDoS) assault that may shut down Internet-based systems and applications in no time. The attackers are changing their skills frequently and consequently avoiding the existing detection mechanisms. Since the number of files created and stored has expanded manifolds, the standard detection systems are not suited for identifying modern DDoS attacks. With the emergence of network-based computing technologies like cloud computing, fog computing, and IoT (Internet of Things), the context of digitizing confidential data over the network is being adopted by various organizations where the security of that sensitive data is considered a major concern. Over the past decade, there has been massive growth in the usage of the internet, along with technological advancements that demand the development of efficient security algorithms that can withstand various patterns of security breaches. The work systematically evaluates the prominent literature, specifically in deep learning, to identify DDoS using machine learning techniques.

Keywords:- *DDoS Attack, Machine Learning, Deep Learning,VolumetricAttacks, Network Intrusion Detection System, PICO, PRISMA, SLRA.*

I. INTRODUCTION

A distributed denial of service (DDoS) assault sends floods of attack packets to the target resources, rendering them inaccessible to normal users on the network and the victim host (Vishwakarma & Jain, 2020). A DoS attack radiates from a single source and floods resources that serve genuine traffic (Vishwakarma & Jain, 2020; Mirkovic & Reiher, 2004). Currently, one of the most prevalent network assaults is distributed denial-of-service. The damage caused by a DDoS assault is getting worse as computer and communication technology advance so quickly. Therefore, it is more crucial than ever to research DDoS attack detection (Umarani & Sharmila, 2015). DDOS is a server attack where the main goal is to deny authorized users access to the source. In this case, it completely disables one user source. Multiple digital devices which are connected are more vulnerable Hackers may also aim for personal information and data that protects them from unauthorized additions (Kitchenham & Brereton, 2013). Nowadays some related research has been conducted and certain advancements have been made. However, there is yet no detection system with a detection accuracy that is sufficient, due to the diversity of DDoS attack tactics and the fluctuating amount of attack traffic.

Now a days with the advent of 4G, and 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, education, etc. made it a vital component in framing various business models. This context made security over wireless networks the most important factor while using the internet from unsecured connections (Siddiqui et al., 2021; Umarani & Sharmila, 2015). 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 to 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 which enables access constraints for legitimate users to utilize the services provided by the target server which leads to 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 (Lam et al., 2006). 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. As an outcome of several research studies, there are several statistical mechanisms to detect intrusions in the network traffic by analyzing the source and destination IP address, detection based on the port degeneration values, destination decay, and wavelet-based analysis among others (Kitchenham & Brereton, 2013). With the massive usage of cloud computing and IoT technologies, the model for DDoS attacks has been changing frequently with the frameworks of computing. Design and development of novel statistical models are time-consuming as they will not be able to sustain rapid and dynamic changes within the network. The major drawbacks observed while constructing the statistical model are that it is bounded towards a single application scenario and the range of complexity in building and maintaining 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 (SaiSindhuTheja & Shyam, 2021). It is evident from various research studies that Machine learning algorithms have demonstrated high performance while adopting the dynamic changes within the network and predicting the network traffic along with the intrusions within the network.

Machine learning and deep learning algorithms can identify unconstrained information within massive amounts of data which draws the attention of various researchers to study the application of these strategies. Researchers 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 networks from a normal network in the circumstance of controlling the servers (Ali et al., 2022; Dietrich, Long & Dittrich, 2000). 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 a few deficiencies while adopting machine and deep learning algorithms because of their substantial computational complexity. DDoS attack patterns vary from different network components (Jaafar, Abdullah & Ismail, 2019). Primarily DDoS attacks involved in devastating the target remote server or network traffic toward the server could be categorized into three categories that include application- layer based attacks, Protocol level attacks, and Network traffic attacks (Singh, Tanwar & Sharma, 2020).

The contribution of this article is threefold; a systematic literature review of various studies involved in the application of machine and deep learning algorithms is detailed (Singh et al., 2020). Further, an attempt of identifying the research gap is made based on evidence-based research to analyze the success rate of machine and deep learning algorithms in the detection and prediction of DDoS attacks in an unconstrained network environment (Singh et al., 2020).The rest of this review paper is organized as follows: brief literature review background in section two (2), the 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 two (3). Section three (4) provides details of the findings and discussion of the paper, while Section five (5) gives a summary of various existing machine and deep learning models for the detection and prediction of DDoS attacks. Finally, Sectionsix (6) and seven (7) addresses the research gaps and conclusions respectively on the review results.

The most important step in the systematic review protocol is defining Research thematic areas. The streamlining of the study is initially maintained by thematic areas. In the context of defining thematic areas, this review paper adopts a population, (2) the Intervention, (3) the Comparison (if there is one), and (4) the Outcome(s) (PICO) strategy that involves various components that elevate the quality of the study. The research thematic areas framed on addressing DDoS attacks, detection, and prevention using machine learning were: 1) types of DDoS attacks that could be referred to as a major concern in the context of distributed networks, 2) existing machine learning algorithms devised to address DDoS attack prediction, 3) tools and data sets utilized and finally 4) machine learning and deep learning techniques influence the research in the prediction of DDoS attacks.

II. RESEARCH METHODOLOGY

A systematic literature review based on the blend of Search, Appraisal, Synthesis, And Analysis (SASA) framework and Preferred Reporting Items for the Systematic Review and Meta-Analysis (PRISMA) statement and PICO framework was chosen as the methodology to achieve the study purpose (Figure 2). Compared to a traditional literature review, the advantage of this methodology is the rigorous filtering of relevant literature according to a predefined set of criteria (Mohamed et al., 2021;Rother, 2007). The literature chosen is therefore strictly relevant to the thematic are a being investigated. Systematic literature review (SLR) was complemented by preferred reporting items for the systematic review and meta-analysis (PRISMA) statement for the richness and validity of the review results (Sarkis-Onofre et al., 2021; Khan et al., 2003). Moreover, PRISMA also acts as a guide to guide for authors, reviewers, and editors (Selçuk, 2019). This review paper adapts the procedure of conducting a systematic literature review (SLR) (Sayers, 2008). The main intention of conducting SLR is to execute a well-planned literature study in the context of addressing research thematic areas for the study. SLR enables the researchers to discover, evaluate and amalgamate the research studies conducted by various network security researchers. The development of SLR included the following process(Figure 1:

- **Protocol development:** This included the Development of a review protocol that includes the complete procedure involved in conducting SLR of predicting DDoS attacks using the machine and deep learning applications.
- **Research Question Determination:** Enumerate the Research Questions based on the PICO search strategy (Santos et al., 2007) in the context of DDoS attacks.
- **Article Filtration:** Primary and secondary selection strategy to filter the articles addressing the research questions.

- **Article Synthesis:** Synthesize the selected studies to answer the research questions.

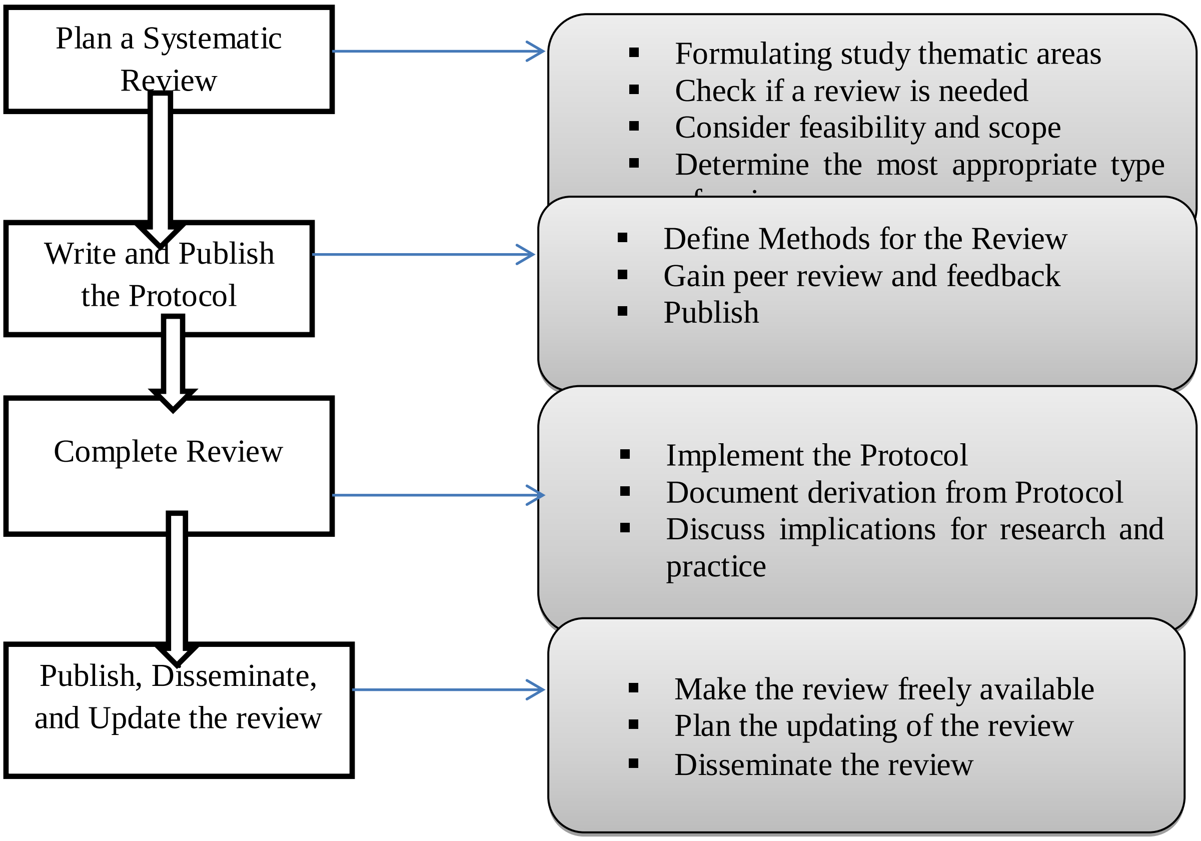
Plan a Systematic Review
Write and Publish the Protocol
Complete Review
Publish, Disseminate, and Update the review
Formulating study thematic areas
Check if a review is needed
Consider feasibility and scope
Determine the most appropriate type
Define Methods for the Review
Gain peer review and feedback
Publish
Implement the Protocol
Document derivation from Protocol
Discuss implications for research and practice
Make the review freely available
Plan the updating of the review
Disseminate the review

Fig. 1: The development Process of Systematic Literature Review Analysis as applied in this Study

This study exploits existing relevant literature from the following different scholarly databases; ACM Digital Library, IEEE Explore, Google Scholar, Scopus, Springer, EBSCO Host, Science Direct, E brary, and Web of Science to understand the facets regarding the Prediction of DDoS Attacks using Machine Learning and Deep Learning Algorithms. The articles were perused following defined inclusion and exclusion conditions as a way to achieve the utmost appropriate articles for the study independent of any part of the world. To perform the widest evaluation of the literature as viable and to consist of as many viable studies similar to the subject, the look for papers was accomplished in the numerous reputable databases as listed in the first paragraph of this section. The systematic literature review process was performed following the four (4) steps below:

- **Step 1: Identifying Articles for Review:** This step involved running the searches designed through the abstract and citation databases selected. Here, the research questions were framed, with the relevant literature subsequently being identified. This involved defining keywords and databases with logical justifications. Keywords/combination DDoS Attacks + Intrusion detection Systems+ Network Securitywere identified.
- **Step 2: Screening the Articles:** The reading of the title and abstract of each record happened here. This reading is intended to determine whether the article contains content that would be relevant to the study. The inclusion and exclusion criteria were established, according to which the references retrieved from online and manual searches were scanned and the relevant articles were marked.
- **Step 3: Eligibility:** This involved taking the articles that remained after the title and abstract screening and were read in full. The intention was to determine whether these articles would help you to answer the research question. The quality of the literature retrieved was assessed and its relevance or not to the study was evaluated.
- **Step 4: Inclusion**: After excluding irrelevant, the number of studies to be included in the review for content analysis was determined.

The keywords/combination of keywords and chosen databases were determined through the conduction of brainstorming sessions and discussions between authors and further the findings were relayed before the experts to have final results of which databases to consider as well as which keywords/combination of keywords that should be considered for the search. The keywords were taken in combination as a way to keep the scope of the study.

A total of one hundred and sixty (160) articles were discovered for the content analysis by employing the quest combination of the considered keywords.

One hundred(100) articles were removed based on defined exclusion criteria as shown in figure 2 below and five (5) were removed at the content analysis level. According to the publication information of the fifty-five (55) publications nominated, forty (40) articles were found in journals and only ten (10) came from various published books.

- **The exclusion standards were as follows:** Summaries of Conferences, Convention lawsuits, Book reviews, Field of agriculture science, Interviews, Technical as well as health science, Summaries of meetings, Editorial letters; Non-academic texts, and Non-English papers. These papers were excluded from the evaluation, Articles with ambiguity in the context of the implementation of the proposed mechanisms, White papers and Lecture notes regarding the prediction of DDoS attacks using machine and deep learning techniques, Articles written in other than the English language
- **The inclusion criteria included the following:** Books, Empirical studies, Editorials, Articles in academic journals,Case studies, Articles that include prediction and detection techniques associated with the machine and deep learning algorithms, Articles prepared in the context of evidence-based research in predicting DDoS attacks with a clear representation of implementation details that includes datasets, tools, andmechanisms, Articles that are primarily implemented in the computerscience domain, Articles that are written in theEnglish language.

The quality of the articles based on the implementation details furnished in the article, such as identifying the algorithm utilized to resolve the DDoS attacks in classification along with its implantation with real-world datasets was 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 furnished above. Feedback from a team of research experts is considered to enhance the process of SLR. A 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, fifty-five (55) articles were considered for the review related to DDoS prediction and detection based on the inclusion and exclusion criteria.

Even though the inclusion and exclusion conditions were strictly adhered to, certain additional references that were mentioned in the chosen articles were added throughout the review process.

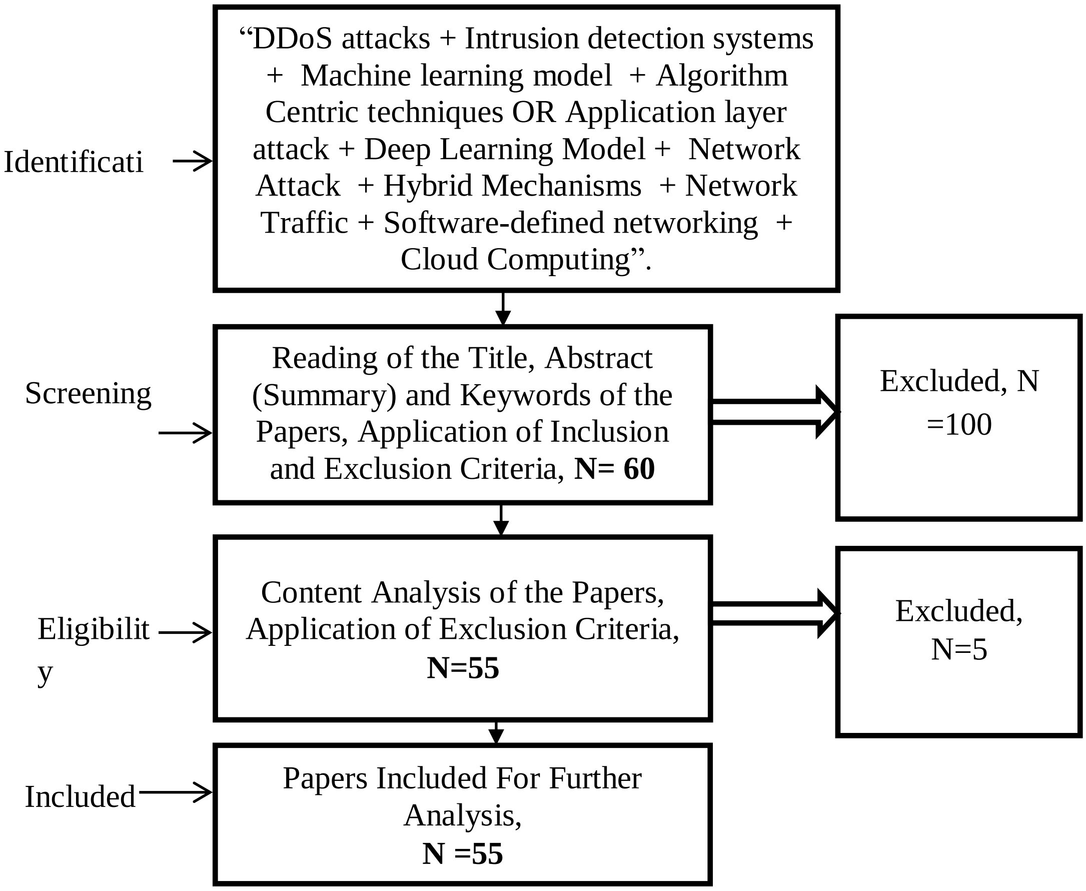
Identificati
"DDoS attacks + Intrusion detection systems + Machine learning model + Algorithm Centric techniques OR Application layer attack + Deep Learning Model + Network Attack + Hybrid Mechanisms + Network Traffic + Software-defined networking + Cloud Computing".
Screening
Reading of the Title, Abstract (Summary) and Keywords of the Papers, Application of Inclusion and Exclusion Criteria, N= 60
Excluded, N =100
Eligibilit y
Content Analysis of the Papers, Application of Exclusion Criteria, N=55
Excluded, N=5
Included
Papers Included For Further Analysis, N =55

Fig. 2: Process Flow of Inclusion and Exclusion According to PRISMA Assertion

III. DISCUSSION AND RESULTS

A. 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 into the computer machines over the network which in turn transforms each machine into 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:

B. Application Layer Attacks:

The primary objective of the application layer attacks is to wear out the resources of the targeted server. This kind of attack 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 a complex process as it is involved loading multiple sets of files based on the database transactions in the process of generating access to the web page.

C. Volumetric Attacks:

These kinds 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 unnecessary congestion over the target server's network by disposing of large amounts of data to the server over the network using various amplification techniques. The amount of traffic generated using a volumetric attack will be able to disrupt the server's network.

D. Protocol Attacks:

These attacks mainly concentrate on exhausting the server resources in terms of 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 network switches. These attacks always try to make use of the TCP handshake mechanism and IP protocol with a spoofed IP address to gain access to the target machine.

Table 1: Classification of DDoS attacks Reviewed

Application Layer-Based Attacks	HTTP Flooding
	Session and Request Flooding
	Multi-level GET/POST Flooding
	Rudy Attack
Volumetric Attacks	Amplification and Reflection based flooding Attacks
	DNS Amplification
	NTP Amplification
Protocol Attacks	Ping on Death
	SYN Flood
	Smurf Attack
	Crypto-Currency Attack

E. General Machine Learning and Deep Learning Approaches in PredictingDDoS 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 (Peraković, et al., 2-2017; Kumar & Kumar, 2016; Prasad, 2014).

Further few research studies have categorized the detection methods based on DoS-misuse detection as well as anomaly detection. Table 4 Synthesizes 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 requires 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 problem usage of machine learning algorithms (Islam et al., 2022; Muhammad & Saleem, 2022) will automate the process of predicting DDoS by learning attack signatures with improved accuracy.

Table 2: Categories of variousMachine Learning and Deep Learning techniques to detect DDoSattacks

S/N	Category	Description
001	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
002	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
003	Statistical Methods	Modeling the statistical patterns of the normal attacks and using these inferences to classify the dynamically generated network traffic to predict network traffic-based attacks The recent studies presented by (Khalafet al., 2019; Gil & Poletto, 2001) Detail the statistical technique derived based on a multi-level tree that analyses the online packet statistics in this context the researcher had were you made that the bracket rates between the hosts are constrained to be proportional to each other.
004	Soft Computing Mechanisms	Derive learning patterns based on the optimization techniques to optimize network traffic for predicting attacks

F. *Specific Machine Learning and Deep Learning Mechanisms to predict Specific DDoS Attacks*

Application layer DDoS Attacks.

- Application layer DDoS attacks generally deal with the concept of botnets (Yuan, Li, & Li, 2017). Most of the DDoS attacks were launched based on open-source tools which in turn different organizations will not be able to identify the traces of attacks. The researchers (Alomari et al., 2021) have analyzed the context of coding that lies behind various popular DDoS attacks that include agobots, SpyBot, SDbot, and Robot. The main objective here is to gain knowledge concerning 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 were studied by Li, Liu & Gu, (2010) who mainly focused on the application layer that may cause security damage to their business which is identified to be a major concern in the context of the business (Yuan, Li, & Li, 2017). Possible solutions and further research directions have been summarized in this research. The most widely used method to defend against DDoS attacks is the Pushback method as this method utilizes the concept of congestion control. This method mainly comprised selective drop as well as detection stages through which it could efficiently defend against application-layer attacks (Revathi, Ramalingam, & Amutha, 2021). Further, the technique is 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 by (Yuan, Li, & Li, 2017; Kumar & Selvakumar, 2013) through the study of existing DoS attacks and their patterns that are labeled as distributed and wireless network systems.
- The analysis of the botnet-based attack similarity in gaining access to the web application was discussed in detail (Khan et al., 2019; Lu & Wang, 2016; Zhu & Goldberg, 2009). 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 have proposed a KNN-based algorithm that identifies the network traffic generated by similar bots (Fu, Papatriantafilou & Tsigas, 2012). 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 into the category of normal or attack.

G. *Detection and Prediction of Volumetric DDoS attacks*

- Distributed and reflective denial of service attacks DDoS attacks are a category of DDoS attack that is prone to protocol layer attacks (Prasad & Chandra, S2022). DRDoS 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 (Nuiaa, Manickam & Alsaeedi, 2021). 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 (Nuiaa et al., 2021; Liu et al., 2015). As the IP address spoofing mechanism is constrained to the 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.
- Some research studies have developed a mechanism that amplifies DNS and demonstrated the scenario of a real attack (Meitei, Singh & De, 2016; Anagnostopoulos et el., 2013; Büscher & Holz, 2012). The demonstration of the work includes two (2) groups of packets that include 3539 packets with a size of around 5MB and 3110 packets with a size of around 3.5 MB that is recorded on

the target server with a range of amplification between 37 to 44 such that the individual attacking node will have the capability of releasing 3 to 4 Mbps of unnecessary traffic to the victim. Further, some research says that DNS query in the context of analyzing DNS-based DDoS attack amplification eventually targets the remote server (Kim et al., 2017; Anagnostopoulos et el., 2013).

- There is also a mechanism that operates on an 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 (Schlackl, Link & Hoehle, 2022; Kolias et al., 2015; Ruan, Liu, & Zhao, 2013; Kambourakis et al., 2008). In the context of detecting the anomaly, there has been made use of data mining-based approaches to classify the traffic of the DNS query (Lombardo et al., 2018; Ruan et al., 2013). Others have developed a modified bloom filter-based mechanism such that his research study 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 a specific period then it allows that particular IP address else the IP address is blocked (Naqash et al., 2021; Sattar et al., 2013; Geneiatakis, Vrakas & Lambrinoudakis, 2009). Further, the studies in [24] addressed the context of the trivial file transfer protocol through which the amplification factor is elevated (Sieklik, Macfarlane & Buchanan, 2016). Prediction and monitoring of the DNS traffic caused by the botnet will gradually increase as synthesized in the literature (Sieklik et al., 2016; Suthaharan & Suthaharan, 2016; Sinam et al., 2014). Addressing the usage of the artificial neural network in the context of detecting and predicting on classifying normal data packets and DDoS attack intruder packets within the real-time environments on blocking the forged data packets before these packets arrive at the target server.
- In the case of detecting VOIP over the network has devised a machine-learning technique has. 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 (Azab et al., 2022; Sinam et al., 2014).

Table 3: Protocols that are more prone to the DRDoS Attacks

S/N	**Protocol**	**Description**
001	NTP	This protocol is mainly related to the time synchronization with 123 ports
002	NetBios	It acts as a Name Service Protocol for API that represents NetBIOS
003	DNS	Domain name resolution protocol with 53 ports
004	SSDP	UPnP- enabled hosts are discovered using this protocol with 1900 ports
005	SNMP2	It usually monitors the devices that are attached to the network with around 161 ports
006	Salty	It is considered a malware dropper protocol that works on the P2P mechanism
007	ZAv2	It enables rootkit for P2P-based computing

H. Detection and prediction of Protocol attacks Using Machine Learning

- As a way to address the context of asmurf attack in which a large number of ICMP data packets are transported toward the target remote server, five (5) different steps in the process of executing the smurf attack without any inconsistencies are recommended (Rabhi, Abbes & Zarai, 2023; Mondal et al., 2022; Yavuz et al., 2018). The most common effectof a smurf attack is that it will cripple the target server with unlimited ping such that it may cause huge revenue loss. Ina few cases, certain smurf attacks are launched along with rockets that allow accessing the system to shut down the server.
- Data transmission is initially established between the client and server using TCP handshake protocol and usually, this phenomenon is known as the 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 (Goldschmidt, 2019). 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 (Goldschmidt, 2019; Hsu et al., 2016).
- From the literature reviewed, it can be indicated that the size of the IP packets is 65535 bytes which include the size of the headers (Guo, et al., 2022; Hameed & Ali, 2018). The server will not be able to handle the requested ping packet that is larger than the indicated maximum size which breaches the IP regulations (Paliwal, Bharti, & Mishra, 2022). In general, the attackers will flood the forged data packets in the form off ragments to the servers that are reassembled by the target servers if anoversized packet fragment occurs it is prone to be a ping of death packet that crashes the target server (Paliwal et al., 2022; Hameed & Ali, 2018).

Table 4: Qualitative analysis of Publications related to different types of DDoS attacks

Type of Attack	Frequency of Publication
Volumetric Attacks	28%
Application Attacks	36%
Protocol Attacks	36%

IV. SUMMARY OF THE REVIEW PAPER FINDINGS

Tables 4 and 5 show the analysis of counter measures for different types of DDoS attacks and the accuracy of DDoS detection using various Machine Learning Algorithms respectively. The systematic literature review presented in this article attempted 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 conducted based on mapping the research thematic areas framed in section 1.

Table 5: Analysis of counter measures for different types of DDoS attacks

Author Name	Parameters	Prediction and The detection level of DDoS	Dataset	Performance analysis
Hameed & Ali (2018)	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 measuring utility
Singh & Behal (2020)	Packet header and time size window	Fluctuated levels depending on the flash crowd	CAIDA and FIFA	Precision and recall, classification rate and F measure
Aborujilah & Musa (2017)	TCP-based covariance matrix	DDoS attacks constituted low rates	Case study-based experimental data and KDD cup 99	False-positive and negative
Hoque, Bhattacharyya, & Kalita (2016)	IP indexing of source server	DDoS attacks constituted high rates	TUIDS and DARPA	Accuracy of prediction and Rate of detecting DDoS attack
Nam & Djuraev, (2014).	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
Singh & De, (2017)	Genetic algorithm-based multi-layer perceptron	DDoS attacks constituted high rates	The dataset generated based on BONSI	Sensitivity analysis and accuracy
Shiaeles, & Papadaki, (2015)	Hop Count, Source MAC address and agent-based on the web browser	DDoS attacks constituted too high rates	LLDOS and DARPA	Rate of detecting DDoS attack
Liao et al., (2015)	Frequency of the request interval and request sequence analysis	DDoS attacks constituted high rates	Weblogs based on university data	Accuracy of prediction and Rate of detecting DDoS attack
Wang, Fleet & Hertzmann. (2007)	Weigh moving algorithm and probability analysis	DDoS attacks constituted high rates	Case study-based experimental data and Clark net	False-positive

Table 6: Accuracy of DDoS detection using various Machine Learning Algorithms

S/N	Topic	Author Name	Algorithm	Accuracy
1	Detecting Flooding DDOS Attacks Over Software-Defined Networks using Machine Learning Techniques	Jose et al, (2021)	Support Vector Machine	99.99%
2	Distributed Denial Of Service Attacks Detection System By Machine Learning Based On Dimensionality Reduction	Abbas & Almhanna (2021	PCA	99.97%
3	A DDoS Attack Detection Method Based on Machine Learning	Pei et al.,(2019)	Random Forest Algorithm	99.49%
4	Feature selection and comparison of classification algorithms for wireless sensor networks	Pande et al., (2021)	SVM, Perceptron, K-nearest neighbor	98.87%
5	Automated DDOS attack detection in software-defined networking.	Ahuja et al., (2021)	Random Forest and Support Vector machine	98.8%

V. RESEARCH GAP

Based on the detailed analysis of 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 knowledge-based and statistical analysis methods. The adaption of Machine and deep learning mechanisms for predicting DDoS attacks was in the infant stage of the research. Table three (3) depicts that the countermeasures for detection and prediction of DDoS attacks in different layers are given importance but these techniques are developed only based on traditional techniques and it is observed that every time detection of DDoS attacks is given a higher priority. Further, the research on the behavior of various DDoS attacks and their countermeasure execution in the context of distributed computing environments like cloud computing, grid computing, and IoT is 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 layers and analyzing their behavior when deployed in distributed computing environments will be fruitful research for future consideration.

VI. CONCLUSION

A DDoS attack happens when numerous hacked computers are utilized to conduct an attack on a single target, overloading it with unwanted traffic and taking it down or drastically degrading its performance. Either situation may also confuse IT, workers, allowing black hat hackers to exploit additional weaknesses, steal data, or infect a network with other types of malware. DDOs attacks will continue to be a major danger to many large and small enterprises since they cause a wide range of harm to internet users. Areas that may rely on human operators, high computing times, and a lack of freely available data still, several areas must be prioritized to identify DDoS attacks. DDoS attacks are detected using a variety of algorithms, including Linear Regression, Random Forest, and selection. The study also discusses the future of analyzing and performing DDoS attacks using a deep learning model, as well as topological attack detection.

This article includes the systematic study of literature in the context of detecting and predicting DDoS attacks by 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 of these algorithms suffer from computational complexity.

REFERENCES

[1.] Abbas, S. A., & Almhanna, M. S. (2021, February). Distributed denial of service attacks detection system by machine learning based on dimensionality reduction. In Journal of Physics: Conference Series (Vol. 1804, No. 1, p. 012136). IOP Publishing.

[2.] Aborujilah, A., & Musa, S. (2017). Cloud-based DDoS HTTP attack detection using covariance matrix approach. Journal of Computer Networks and Communications, 2017.

[3.] Ahuja, N., Singal, G., Mukhopadhyay, D., & Kumar, N. (2021). Automated DDOS attack detection in software-defined networking. Journal of Network and Computer Applications, 187, 103108.

[4.] Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics, 11(3), 494.

[5.] Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403.

[6.] Alzahrani, R. J., & Alzahrani, A. (2021). Security analysis of DDoS attacks using machine learning algorithms in network traffic. Electronics, 10(23), 2919.

[7.] Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., & Gritzalis, S. (2013). DNS amplification attack revisited. Computers & Security, 39, 475-485.

[8.] Azab, A., Khasawneh, M., Alrabaee, S., Choo, K. K. R., & Sarsour, M. (2022). Network traffic classification: Techniques, datasets, and challenges. Digital Communications and Networks.

[9.] Büscher, A., & Holz, T. (2012, April). Tracking DDoS Attacks: Insights into the Business of Disrupting the Web. In LEET.

[10.] Dietrich, S., Long, N., & Dittrich, D. (2000, December). Analyzing distributed denial of service tools: The shaft case. In LISA (pp. 329-339).

[11.] Fu, Z., Papatriantafilou, M., & Tsigas, P. (2012). Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. IEEE Transactions on Dependable and Secure Computing, 9(3), 401-413.

[12.] Geneiatakis, D., Vrakas, N., & Lambrinoudakis, C. (2009). Utilizing bloom filters for detecting flooding attacks against SIP-based services. computers & security, 28(7), 578-591.

[13.] Gil, T. M., & Poletto, M. (2001, August). MULTOPS: A Data Structure for Bandwidth Attack Detection. In USENIX security symposium (pp. 23-38).

[14.] Goldschmidt, P. (2019). TCP Reset Cookies–a heuristic method for TCP SYN Flood mitigation. Excel@ FIT 2019.

[15.] Guo, W., Xu, J., Pei, Y., Yin, L., Jiang, C., & Ge, N. (2022). A distributed collaborative entrance Defense framework against DDoS attacks on satellite internet. IEEE Internet of Things Journal, 9(17), 15497-15510.

[16.] Hameed, S., & Ali, U. (2018). HADEC: Hadoop-based live DDoS detection framework. EURASIP Journal on Information Security, 2018(1), 1-19.

[17.] Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2016). FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. Security and Communication Networks, 9(13), 2032-2041.

[18.] Hsu, F. H., Hwang, Y. L., Tsai, C. Y., Cai, W. T., Lee, C. H., & Chang, K. (2016). TRAP: A three-way handshake server for TCP connection establishment. Applied Sciences, 6(11), 358.

[19.] Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT-based monitoring systems of the banking sector using machine learning models. Sustainability, 14(14), 8374.

[20.] Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attacks. Journal of Computer Networks and Communications, 2019.

[21.] Jose, A. S., Nair, L. R., & Paul, V. (2021). Towards detecting flooding DDoS attacks over software-defined networks using machine learning techniques. REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS, 11(4), 3837-3865.

[22.] Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2008). Detecting DNS amplification attacks. In Critical Information Infrastructures Security: Second International Workshop, CRITIS 2007, Málaga, Spain, October 3-5, 2007. Revised Papers 2 (pp. 185-196). Springer Berlin Heidelberg.

[23.] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abdullah, W. M. (2019). A comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713.

[24.] Khan, R. U., Kumar, R., Alazab, M., & Zhang, X. (2019, May). A hybrid technique to detect botnets, based on P2P traffic similarity. In 2019 Cybersecurity and Cyberforensics Conference (CCC) (pp. 136-142). IEEE.

[25.] Kim, S., Lee, S., Cho, G., Ahmed, M. E., Jeong, J., & Kim, H. (2017). Preventing DNS amplification attacks using the history of DNS queries with SDN. In Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II 22 (pp. 135-152). Springer International Publishing.

[26.] Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. Information and software technology, 55(12), 2049-2075.

[27.] Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. Information and software technology, 55(12), 2049-2075.

[28.] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[29.] Kumar, P. A. R., & Selvakumar, S. (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Computer Communications, 36(3), 303-319.

[30.] Kumar, V., & Kumar, K. (2016, September). Classification of DDoS attack tools and their handling techniques and strategy at the application layer. In 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

[31.] Lam, H. Y., Li, C. P., Chanson, S. T., & Yeung, D. Y. (2006, June). A coordinated detection and response scheme for distributed denial-of-service attacks. In 2006 IEEE International Conference on Communications (Vol. 5, pp. 2165-2170). IEEE.

[32.] Li, J., Liu, Y., & Gu, L. (2010, November). DDoS attack detection based on neural network. In 2010 2nd international symposium on aware computing (pp. 196-199). IEEE.

[33.] Liao, Q., Li, H., Kang, S., & Liu, C. (2015). Application layer DDoS attack detection using a cluster with labels based on sparse vector decomposition and rhythm matching. Security and Communication Networks, 8(17), 3111-3120.

[34.] Liu, B., Li, J., Wei, T., Berg, S., Ye, J., Li, C., ... & Han, X. (2015). SF-DRDoS: The store-and-flood distributed reflective denial of service attack. Computer communications, 69, 107-115.

[35.] Lombardo, P., Saeli, S., Bisio, F., Bernardi, D., & Massa, D. (2018). Fast flux service network detection via data mining on passive DNS traffic. In Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21 (pp. 463-480). Springer International Publishing.

[36.] Lu, Y., & Wang, M. (2016, June). An easy defense mechanism against botnet-based DDoS flooding attacks originated in the SDN environment using sFlow. In Proceedings of the 11th International Conference on Future Internet Technologies (pp. 14-20).

[37.] Meitei, I. L., Singh, K. J., & De, T. (2016, August). Detection of DDoS DNS amplification attack using a classification algorithm. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-6).

[38.] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[39.] Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2021). The ABC of systematic literature review: the basic methodological guidance for beginners. Quality & Quantity, 55, 1319-1346.

[40.] Mondal, B., Koner, C., Chakraborty, M., & Gupta, S. (2022). Detection and investigation of DDoS attacks in network traffic using machine learning algorithms. Int. J. Innov. Technol. Explore. Eng., 11(6), 1-6.

[41.] Muhammad, M. U. U. A. H., & Saleem, A. M. S. F. M. (2022). Intelligent Intrusion Detection System for Apache Web Server Empowered with Machine Learning Approaches. International Journal of Computational and Innovative Sciences, 1(1), 1-8.

[42.] Nam, S. Y., & Djuraev, S. (2014). Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection. KSII Transactions on Internet and Information Systems (TIIS), 8(7), 2512-2531.

[43.] Naqash, T., Zafar, M. R., Razzaq, K., & bin Ubaid, F. (2021) Secure DNS from amplification attack by using modified bloom filters. In Eighth International Conference on Digital Information Management (ICDIM 2013).

[44.] Nuiaa, R. R., Manickam, S., & Alsaeedi, A. H. (2021). Distributed reflection denial of service attack: A critical review. International Journal of Electrical and Computer Engineering, 11(6), 5327.

[45.] Paliwal, S., Bharti, V., & Mishra, A. K. (2022). Machine learning combating DOS and DDOS attacks. International Journal of Business Information Systems, 40(2), 177-191.

[46.] Pande, S., Khamparia, A., Gupta, D., & Thanh, D. N. (2021). DDOS detection using machine learning technique. In *Recent Studies on Computational Intelligence: Doctoral Symposium on Computational Intelligence (DoSCI 2020)* (pp. 59-68). Springer Singapore.

[47.] Pei, J., Chen, Y., & Ji, W. (2019, June). A DDoS attack detection method based on machine learning. In Journal of Physics: Conference Series (Vol. 1237, No. 3, p. 032040). IOP Publishing

[48.] Peraković, D., Periša, M., Cvitić, I., & Husnjak, S. (2017). Model for detection and classification of DDoS traffic based on artificial neural network. Telfor Journal, 9(1), 26-31.

[49.] Prasad, A., & Chandra, S. (2022). VMFCVD: an optimized framework to combat volumetric DDoS attacks using machine learning. Arabian Journal for Science and Engineering, 47(8), 9965-9983.

[50.] Prasad, K. M. (2014). DoS and DDoS attacks: defense, detection, and traceback mechanisms-a survey. Global Journal of Computer Science and Technology, 14(E7), 15-32.

[51.] Rabhi, S., Abbes, T., & Zarai, F. (2023). IoT Routing Attacks Detection Using Machine Learning Algorithms. Wireless Personal Communications, 128(3), 1839-1857.

[52.] Revathi, M., Ramalingam, V. V., & Amutha, B. (2021). A machine learning-based detection and mitigation of the DDOS attack by using SDN controller framework. Wireless Personal Communications, 1-25.

[53.] Rother, E. T. (2007). Systematic literature review X narrative review. Acta paulista de enfermagem, 20, v-vi.

[54.] Ruan, W., Liu, Y., & Zhao, R. (2013). Pattern discovery in DNS query traffic. Procedia Computer Science, 17, 80-87.

[55.] SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm-based feature selection and recurrent neural network for DoS attack detection in the cloud computing environment. Applied Soft Computing, 100, 106997.

[56.] Santos, C. M. D. C., Pimenta, C. A. D. M., & Nobre, M. R. C. (2007). The PICO strategy for the research question construction and evidence search. Revista latino-americana de enfermagem, 15, 508-511.

[57.] Sattar, U., Naqash, T., Zafar, M. R., Razzaq, K., & bin Ubaid, F. (2013, September). Secure DNS from amplification attacks by using modified bloom filters. In Eighth International Conference on Digital Information Management (ICDIM 2013) (pp. 20-23). IEEE.

[58.] Sayers, A. (2008). Tips and tricks in performing a systematic review. British Journal of General Practice, 58(547), 136-136.

[59.] Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. Information & Management, 103638.

[60.] Shiaeles, S. N., & Papadaki, M. (2015). FHSD: an improved IP spoof detection method for web DDoS attacks. The Computer Journal, 58(4), 892-903.

[61.] Siddiqui, F., Beley, J., Zeadally, S., & Braught, G. (2021). Secure and lightweight communication in heterogeneous IoT environments. Internet of Things, 14, 100093.

[62.] Sieklik, B., Macfarlane, R., & Buchanan, W. J. (2016). Evaluation of TFTP DDoS amplification attack. computers & security, 57, 67-92.

[63.] Sinam, T., Ngasham, N., Lamabam, P., Singh, I. T., & Nandi, S. (2014, December). Early detection of VoIP network flows based on sub-flow statistical characteristics of flows using machine learning techniques. In 2014 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.

[64.] Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges, and future directions. Computer Science Review, 37, 100279.

[65.] Singh, K. J., & De, T. (2017). MLP-GA-based algorithm to detect application layer DDoS attacks. Journal of information security and applications, 36, 145-153

[66.] Singh, R., Tanwar, S., & Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy, 3(3), e96.

[67.] Suthaharan, S., & Suthaharan, S. (2016). Decision tree learning. Machine Learning Models and Algorithms for Big Data Classification: Thinking with Examples for Effective Learning, 237-269.

[68.] Ulemale, T. (2021). Review on Detection of DDOS Attack using Machine Learning.

[69.] Umarani, S., & Sharmila, D. (2015). Predicting application layer DDoS attacks using machine learning algorithms. International Journal of Computer and Systems Engineering, 8(10), 1912-1917.

[70.] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defense mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25.

[71.] Wang, J. M., Fleet, D. J., & Hertzmann, A. (2007). Gaussian process dynamical models for human motion. IEEE transactions on pattern analysis and machine intelligence, 30(2), 283-298.

[72.] Yau, D. K., Lui, J. C., Liang, F., & Yam, Y. (2005). Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Transactions on Networking, 13(1), 29-42.

[73.] Yavuz, F. Y., Devrim, Ü. N. A. L., & Ensar, G. Ü. L. (2018). Deep learning for detection of routing attacks in the internet of things. International Journal of Computational Intelligence Systems, 12(1), 39.

[74.] Yuan, X., Li, C., & Li, X. (2017, May). DeepDefense: identifying DDoS attacks via deep learning. In 2017 IEEE international conference on smart computing (SMARTCOMP) (pp. 1-8). IEEE.

[75.] Zhu, X., & Goldberg, A. B. (2009). Introduction to semi-supervised learning. Synthesis lectures on artificial intelligence and machine learning, 3(1), 1-130.