International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Distributed Denial of Service Attacks in Cloud Computing based on Deep Learning: A Study

Mukul Ahirwal
M. Tech. Scholar, Department of Computer Science and Engineering, LNCT, Bhopal, M.P., India

Prof. Puneet Nema
Professor, Department of Computer Science and Engineering, LNCT, Bhopal, M.P., India

Dr. Vivek Richhariya
HOD, Department of Computer Science and Engineering, LNCT, Bhopal, M.P., India

Abstract
Cloud computing has transformed the digital landscape by offering scalable and cost-effective resources. However, its dynamic and shared infrastructure makes it a prime target for cyberattacks, particularly Distributed Denial of Service (DDoS) attacks. These attacks disrupt the availability of services by overwhelming cloud systems with illegitimate traffic from multiple distributed sources. Traditional detection methods often fall short in identifying sophisticated and large-scale DDoS patterns in real time. This study explores the application of deep learning (DL) techniques for detecting and mitigating DDoS attacks in cloud environments. By leveraging models such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and autoencoders, the research aims to accurately classify malicious traffic patterns and distinguish them from legitimate behavior. A deep learning-based Intrusion Detection System (IDS) is proposed, trained on real-world datasets such as CICDDoS2019 and UNSW-NB15. The experimental results demonstrate that DL models significantly outperform traditional machine learning approaches in terms of accuracy, adaptability, and real-time performance. This study contributes to the advancement of intelligent cloud security systems and highlights the potential of deep learning in building resilient and proactive defense mechanisms against evolving cyber threats in cloud computing.

Keywords: - Denial of service (DoS), Neural Network, Attack

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

1. INTRODUCTION

The purpose of computer security is devising ways to prevent the weaknesses from being exploited. In computer security stand point three important aspects of confidentiality, integrity, availability, control and audit have to be addressed. Confidentiality, otherwise termed as secrecy or privacy is required to ensure that computer related assets are accessed only by authorized parties. It can be achieved through physical isolation, cryptography and background checks on people. Integrity means that assets can be modified (writing, changing, changing status, deleting and creating) only by authorized parties or only in authorized ways [1]. In maintaining integrity data integrity takes the top most priority, where redundancy to some extent, preserving backups, having checksums for the purpose of error detection and correction, and including digital signatures to ensure authenticity. Availability means that authorized parties access assets at appropriate times, and such accesses should not be prevented, sometimes known by its opposite, denial of service (1). It can be achieved through hardening, redundancy and having reference checks on people. A service, data item or a system is available if there is timely response to requests, fair allocation of resources, fault tolerance exhibited for hardware and software, easy usage of service of system, and the concurrency is controlled when simultaneous accesses, deadlocks, and exclusive accesses occur [2]. Full implementation of availability is a great challenge for security. Control, otherwise termed as countermeasure attempts to prevent exploiting computer system's vulnerability. There are a variety of controls available, out of which some of easier or cheaper to implement, and some are costlier or difficult to make them feasible. Some of them are encryption, controls in the form of software, controls in the form of hardware, effective policies and procedures and physical controls [3]. Audit is a systematic and measurable technical assessment of deployment of the organization's security policy at a specific site. To perform the audit, auditors require the full knowledge of the organization, and at times with considerable inside information to understand the nature of resources to be audited. The candidates of verification during the audit can be strength of passwords, presence of ACLs and audit logs, security strength of operating systems, elimination of unnecessary applications and services, information on backup media, disaster recovery plan, availability of cryptographic tools, security standpoint of custom built applications, documentation and review of configuration and code changes [4, 5].

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

2. LITERATURE REVIEW

R. P et al. [1], because of its many uses and benefits, cloud computing (CC) continues to be a top research topic for analysts. CC's distributed nature and reliance on internet access present a number of threats and difficulties. DDoS attacks primarily aim to interfere with internet operations. Traditional detection methods, such as firewalls, cannot identify insider threats. To lessen DDoS activity, this paper proposes a DDoS detection technique. The suggested work addresses specific detection process procedures, which contributes from a large data standpoint. The first step is the data generation phase, and the DDoS dataset is regarded as big data from the work's point of view. Mapper manages the data and processes the feature extraction, which comprises the extraction of raw features, packet feature extractor, improved correlation, and statistical feature, because the task is viewed through the lens of big data. The merged feature set is provided by the reducer. Appropriate features are chosen from the extracted feature set using a weighted improved hybrid model that combines models such as Deep Maxout (DMO) and Long Short Term Memory (LSTM) networks. The White Shark-Remora Optimization (WSROA) algorithm is used to select the LSTM and DMO weights in the best possible way. The features for DDoS attack detection are carefully chosen using the Recursive Feature Elimination (RFE) procedure. The results demonstrate that the suggested hybrid bio-inspired algorithm performs better than LSTM, Convolutional Neural Networks (CNN), and Deep Belief Networks (DBN), with an accuracy of 94%.

Bakro et al. [2], Cloud computing use is growing in popularity across a range of industries. However, there are serious hazards to the general safety of cloud computing due to its intrinsic security flaws. Thus, intrusion detection systems (IDS) are essential for spotting harmful activity in cloud systems. Repetitive and irrelevant features may be included in the large amount of network traffic data, which could affect the classifier's classification performance. Additionally, processing such a large amount of data in the cloud intrusion detection process increases complexity and time consumption. This study suggests a hybrid feature selection strategy that combines two bio-inspired algorithms—the genetic algorithm (GA) and the grasshopper optimization algorithm (GOA)—to improve the IDS's performance. A more effective search for the best answers is guaranteed when these two algorithms are combined. These ideal characteristics are used to train a random forest (RF) classifier. Additionally, by applying a hybrid approach—using an adaptive synthetic (ADASYN) algorithm to over-sample the minority classes and random under-sampling (RUS) for the majority class when

necessary—the proposal tackles the problem of imbalanced data. Each category is greatly impacted by this integrated approach, which raises the TPR while lowering the FPR to improve system performance as a whole. Three datasets—UNSW-NB15, CIC-DDoS2019, and CIC Bell DNS EXF 2021—were used to assess the suggested method. For these datasets, the corresponding recorded accuracies were 98%, 99%, and 92%. The hybrid feature selection-based IDS produced excellent results for individual classes in the datasets as well as outstanding performance in multi-class classification.

Kumar, S. et al. [3], with its on-demand services, elasticity, scalability, and flexibility, cloud computing has revolutionized the world by offering end users with affordable resources in a pay-as-you-go model. However, protecting cloud services against threats, vulnerabilities, and contemporary attacks continues to be a top priority. Because malicious traffic might be mistaken for legitimate traffic flows, application layer assaults are especially hazardous because they can result in serious harm and are frequently hard to identify. Furthermore, because Distributed Denial of Service (DDoS) attacks have a significant impact on network bandwidth and physical computer resources, they are difficult to prevent. This study uses artificial intelligence (AI)-based techniques to identify and stop such contemporary attacks and looks at novel DDoS attack variants in the larger framework of cyberthreats. According to the results of the inquiry, the majority of the current detection strategies use single, hybrid, and collective Machine Learning (ML)/Deep Learning (DL) approaches. Furthermore, in order to protect cloud infrastructure from the damaging effects of DDoS attacks, it is essential to analyze various DDoS attacks and the defensive tactics that go along with them. This article provides a thorough categorization of the many kinds of cloud DDoS attacks as well as a detailed examination of the methods used for characterisation, detection, prevention, and mitigation.

Aliar et al. [4], these days, the largest companies in the world are those that provide cloud services. The availability of cloud-based services whenever needed is one of the main issues facing cloud service providers (CSPs) and users (CUs). In recent years, a distributed denial of service (DDoS) attack has posed a serious risk to system security. Academic and commercial research is now focused on DDoS defense and attack detection. Nevertheless, the majority of methods are unable to achieve effective detection results with minimal false alarms. CSPs can therefore provide CUs with high-quality services by reducing the effects of DDoS assaults. To successfully detect DDoS attacks in the cloud industry, a collective deep structured algorithm

is proposed. Data collection, pre-processing, optimal feature detection, and selection are the steps in the suggested approach. The initial stage is gathering information from publically accessible sources. The input data also goes through preparation. As a result, the Hybrid Border Collie and Dragonfly Algorithm (HBCDA) is used to optimize the weighted feature selection procedure on the preprocessed data. Lastly, adaptive deep dilated ensemble (ADDE), a novel technique that combines recurrent neural networks (RNN), bidirectional long short-term memory (Bi-LSTM), deep temporal convolutional neural networks (DTCNN), and one-dimensional convolutional neural networks (1DCNN), is used to detect DDoS attacks.

Uddin et al. [5], by lowering latency and utilizing the capabilities of edge devices, edge computing has become the most popular communication technique bridging the gap between the cloud and the Internet of Things. But like any emerging technology, its broad use has also brought to a number of security flaws. The distributed denial of service (DDoS) assault, which is the main subject of this study, is one prominent danger, along with the denial of service (DoS) attack. By analyzing the vulnerabilities connected to distinct edge peripherals, this article seeks to investigate the effects of various DoS and DDoS attack types on edge computing layers. To solve these shortcomings, current detection and preventive methods are also examined. Additionally, a theoretical architecture to counteract distributed denial of service assaults against edge systems is put forth. This study intends to aid in the creation of reliable and secure edge computing systems by thoroughly examining and resolving security issues associated with DoS and DDoS assaults in edge computing.

Han, D. et al. [6], the considerable increase in network speed and connection density brought forth by 5G technology has made network security more difficult. Specifically, in software-defined network (SDN) systems, distributed denial of service (DDoS) assaults have increased in frequency and complexity. The complexity and diversity of 5G networks lead to a large number of superfluous features, which can impair the model's capacity to generalize and add noise into an intrusion detection system's (IDS) detection process. The goal of this article is to enhance the IDS's performance on 5G networks, particularly with regard to detection accuracy and speed. In order to increase the robustness and detection efficiency of the IDS, it suggests a novel feature selection (FS) technique to remove the most representative and distinctive features from network traffic data. This study evaluates the InSDN, CICIDS2017, and CICIDS2018 datasets using four popular machine learning (ML) models and performs real-time DDoS attack detection on the simulation platform to verify the effectiveness of the

proposed strategy. Experimental results indicate that the proposed FS approach can significantly reduce detection time and maintain or improve DDoS detection accuracy, while simultaneously meeting 5G network requirements for high speed and high reliability of the IDS.

Rao et al. [7], as IoT devices proliferate, the network infrastructures of the Internet of Things (IoT) are more vulnerable to distributed denial of service (DDoS) attacks. Specialized strategies are needed to detect and predict such attacks in this dynamic and complex environment. This paper introduces DDoSNet, a method for identifying and forecasting DDoS assaults from a realistic multidimensional dataset designed especially for IoT network environments. The dataset must be cleaned up, missing values must be addressed, and the data must be converted into an analysis-ready format at the start of the data preprocessing stage. A number of preprocessing techniques are employed to increase the data's accuracy and reliability, such as imputation techniques and data-cleaning algorithms. The African Buffalo Optimization with Decision Tree (ABO-DT) method is then used for feature selection. In order to identify the most crucial characteristics, this nature-inspired metaheuristic algorithm mimics the behavior of African buffalos. A subset of features that optimizes the distinction between normal network traffic and DDoS attacks is chosen by combining ABO with the decision tree. An echo-state network (ESN) classifier is used for detection and prediction following feature selection. An ESN is a type of recurrent neural network (RNN) that has demonstrated promise in handling time-series data.

K. Muthamil Sudar et al. [8], SDN is an organization engineering that used to assemble, plan the equipment parts for all intents and purposes. We can powerfully change the settings of organization associations. In the conventional organization, it's impractical to change powerfully, on the grounds that it's a proper association. SDN is a decent methodology yet at the same time is helpless against DDoS assaults. The DDoS assault is threatening to the web. To forestall the DDoS assault, the AI calculation can be utilized. The DDoS assault is the various worked together frameworks that are utilized to focus on the specific server simultaneously. In SDN control layer is in the middle that connection with the application and foundation layer, where the gadgets in the framework layer constrained by the product. In this paper, we propose an AI procedure specifically Decision Tree and Support Vector Machine (SVM) to recognize noxious traffic. Our test result shows that the Decision Tree and Support Vector Machine (SVM) calculation gives better exactness and identification rate.

Muthamil Sudar et al. [9], SDN has as of late arisen as an organization worldview because of its high organization programmability and adaptability which can conquer the issue in customary organizations by decoupling the control plane from the information plane. The information plane will advance the parcels according to the choice made by the regulator in the control plane. This brought together control will assist with giving the theoretical perspective on the whole organization framework. Since the regulator is a center piece of SDN, it is more inclined for assaults and turns as a significant danger to the whole organization. Conveyed Denial of Service (DDoS) assault can then over-burden the SDN regulator and switch stream table which prompts an exhibition corrupt of the organization. To resolve this issue, we have sent two level security instruments. In level one, an entropy-based instrument is proposed to recognize the DDoS flooding assault in the beginning phase by briefly holding the specific stream. In level two, an AI based C4.5 procedure is proposed to distinguish the assault by breaking down extra elements and send a long-lasting caution to drop the bundles. The outcomes are examined with K-overlap approval strategy as far as responsiveness, particularity and precision.

Dong et al. [10], the Distributed Denial of Service (DDoS) assault has truly impeded organization accessibility for quite a long time and still there is no compelling safeguard system against it. Be that as it may, the arising Software Defined Networking (SDN) gives a better approach to reevaluate the safeguard against DDoS assaults. In this paper, we propose two strategies to distinguish the DDoS assault in SDN. One strategy embraces the level of DDoS assault to distinguish the DDoS assault. The other technique utilizes the superior K-Nearest Neighbors (KNN) calculation in view of Machine Learning (ML) to find the DDoS assault. The aftereffects of the hypothetical investigation and the exploratory outcomes on datasets show that our proposed strategies can more readily distinguish the DDoS assault contrasted and different techniques.

3. DENIAL OF SERVICE

Denials of service attacks are significant in networks than other areas that target the availability goal of security. The threats introduced by such attacks on continued service may be either accidental or malicious.

Attack types:- There are different types of Denial-of-Service attacks that occur in different forms such as transmission failures, flooding of numerous connection, echo-chargen, ping of death, smurf, syn flood, tear drop, redirection of traffic, DNS attacks etc. Transmissions fail

for many reasons. One common reason could be, the line is cut or a noise can make a packet unrecognizable or deliverable. A communicating machine along the transmission path could fail due to hardware or software reasons or have gone for repair or testing. A machine could be overloaded or saturated and due to that it cannot accept packets, until it clears its packets. These problems could be temporary or automatically fixed. Some communication failures such as break in single communication line to a computer cannot be easily repaired, and can be fixed only by forming an alternative link or repairing the damaged one. This can be viewed from malicious stand point that anyone can sever, interrupt of overload capacity to deny service [9, 10].

Failures also could occur due to the nonfunctioning of routers, circuit boards, firewalls, monitoring devices, storage devices and switches, for which age, factory flaws, power surges, heat and tampering can be the reasons. Such component failures may cause the entire network to fail. Even-though such failures are almost natural occurrences, one should also think about the possibilities of them being induced. Flooding is the most common type of attack reported to CERT/CC. It involves sending of an excessive amount of packets to the destination causing an excessive amount of end point, too much of bandwidth consumption, and hogging of a link. Both single source against single destination and multiple sources against multiple destinations are common [11].

There are different packet types that are used for attacks by attack tools. There are different types of flooding attacks that are carried out practically. The most common ones are TCP flooding, where a stream of TCP packets with various flags set are sent to the victim IP address. Syn, ACK and RST are the most common types of flags that are used for this kind of attack. UDP flooding is another kind of flooding attack where stream of UDP packets are sent to the victim IP address [12].

4. DISTRIBUTED DENIAL OF SERVICE (DDOS)

DDoS attacks are two stage attacks constructed by the attackers for multiplying the effect. The first stage concentrates on planting an unnoticeable Trojan horse that may be named for a popular editor or utility on a target machine. The same may be subsequently repeated on many targets, thus making the targets systems as zombies [13]. Then a signal is sent to all zombies to launch the attack, and the victim is led to defend ‘n’attacks from ‘n’ number of zombies, each targeting with different kind of attacks such as syn, smurf , all acting at once. DDoS attacks are considered serious due to their nature of being launched through scripts, where one

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

can easily write procedures for planting Trojan horse to launch one or all the attacks [14]. At the outset, these attacks can be divided into two broad categories as agent handler model and Internet Relay Chat model (IRC). The agent handler model gets further divided into client-handler communication and agent-handler communication, and the IRC model gets divided to secret/private channel and public channel.

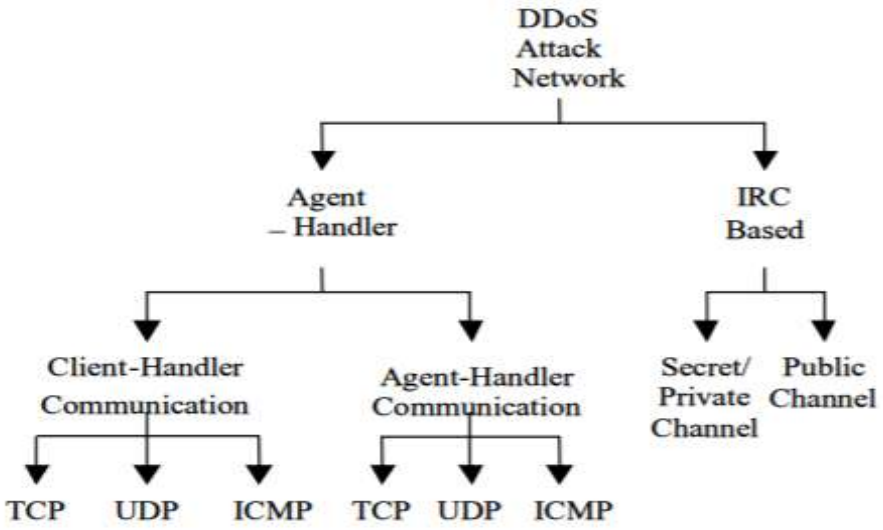

Fig. 1: DDoS Attack Network

5. NEURAL NETWORK

An artificial neural network is a computational model inspired in the natural neurons of a biological nervous system. These models mimic the real life behavior of neurons and the electrical messages they produce between input processing by the brain and the final output from the brain. In other words, artificial neural networks form an attempt to create machines that work in a similar way to the human brain by building these machines using components that behave like biological neurons. The function of an artificial neural network is to produce an output pattern when presented with an input pattern.

Traditionally the term neural network was used to refer to a network or circuit of biological neurons. But the modern usage of the term often refers to artificial neural networks, which are composed of artificial neurons or nodes. Biological neural networks are made up of real human neurons that are connected or functionally related in a nervous system (see Fig. 2). In a typical ANN, input units store the inputs, hidden

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

units transform the inputs into an internal numeric vector and an output unit transforms the hidden values into the prediction. From a practical point of view, an ANN is just a parallel computational system consisting of many simple processing elements like units, connections and weights with numeric inputs and out- puts connected together in a specific way in order to perform a particular task. A simple artificial neural network model with multi-input and single-output is presented in Fig. 3. Basic components of artificial neurons are described as follows:

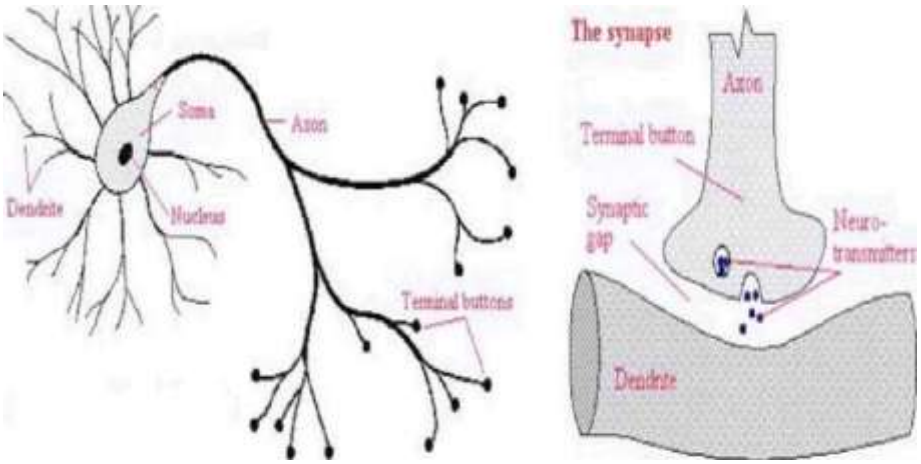

Fig. 2: Schematic diagram of biological neuron

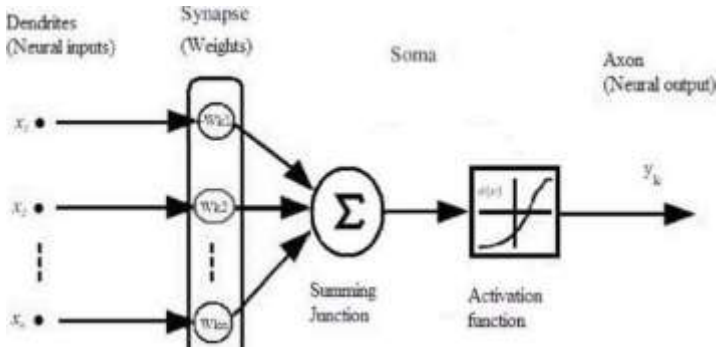

Fig. 3: A simple model of artificial neural network

- A set of connections (that is, synapses) brings in activations from other input neurons (dendrites) and provides long-term memory to the past accumulated experience.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

- A processing unit (soma) sums the inputs and then applies a non-linear activation function (that is, transfer/threshold function); almost all the logical functions of the neuron are carried out in the soma.
- An output line (axon) transmits the result to other neurons.

ANNs processes the information using connectionist approach to computation. In most cases an ANN is an adaptive system that changes its structure based on external or internal information that flows through the network during the learning phase. The typical elements of an artificial neural network are generally described as the network architecture, learning algorithm and activation function.

6. CONCLUSION

The increasing reliance on cloud computing services has amplified the need for robust and intelligent security mechanisms to counteract threats such as Distributed Denial of Service (DDoS) attacks. This study demonstrates the potential of deep learning (DL) techniques in effectively detecting and mitigating DDoS attacks within cloud environments. Unlike traditional security systems, DL models like CNNs, LSTMs, and autoencoders can learn complex patterns in network traffic and adapt to evolving attack strategies with minimal human intervention.

Experimental analysis reveals that deep learning-based Intrusion Detection Systems (IDS) significantly improve detection accuracy, reduce false positives, and enable real-time response to DDoS attacks. The integration of DL into cloud security infrastructure not only enhances service availability and reliability but also builds a proactive and self-learning defense mechanism.

However, challenges such as high computational overhead, model interpretability, and the need for continuous training remain. Future research should focus on lightweight DL models, real-time deployment frameworks, and privacy-preserving solutions such as federated learning. Overall, deep learning presents a promising path forward in safeguarding cloud computing systems against the growing threat of DDoS attacks.

REFERENCES

[1] R. P and S. Kamalakkannan, "Deep Learning Model with Optimization Strategies for DDoS Attack Detection in Cloud Computing," *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India, 2025, pp. 413-417.

[2] Bakro, M., Kumar, R. R., Husain, M., Ashraf, Z., Ali, A., Yaqoob, S. I., … & Parveen, N. (2024). Building a cloud-IDS by hybrid bio-inspired feature selection algorithms along with random forest model. *IEEE Access*, 2024.

[3] Kumar, S., Dwivedi, M., Kumar, M., & Gill, S. S. (2024). A comprehensive review of vulnerabilities and AI -enabled defense against DDoS attacks for securing cloud services. *Computer Science Review*, 53, 100661.

[4] Aliar, A. A. S., Gowri, V., & Abins, A. A. (2024). Detection of distributed denial of service attack using enhanced adaptive deep dilated ensemble with hybrid meta-heuristic approach. *Transactions on Emerging Telecommunications Technologies*, 35 (1), e4921.

[5] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Networks*, 152, 103322.

[6] Han, D., Li, H., Fu, X., & Zhou, S. (2024). Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning. *Sensors*, 24 (13), 4344.

[7] Rao, G. S., Patra, P. S. K., Narayana, V. A., Reddy, A. R., Reddy, G. V., & Eshwar, D. (2024). DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment. *Egyptian Informatics Journal*, 27, 100526.

[8] K. Muthamil Sudar, M. Beulah and P. Deepalakshmi, “Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques”, International Conference on Computer Communication and Informatics (ICCCI), Jan. 27 – 29, 2021, Coimbatore, INDIA.

[9] Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, (Preprint), 1- 22.

[10] Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048.

[11] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.

[12] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[13] A. Raghavan, F. D. Troia, and M. Stamp, ``Hidden Markov models with random restarts versus boosting for malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 2, pp. 97107, Jun. 2019.

[14] T. Young, D. Hazarika, S. Poria, and E. Cambria, ``Recent trends in deep learning based natural language processing [review article]," *IEEE Comput. Intell. Mag.*, vol. 13, no. 3, pp. 5575, Aug. 2018.

[15] X. Lei and Y. Xie, ``Improved XGBoost model based on genetic algorithm for hypertension recipe recognition," *Comput. Sci*, vol. 45, pp. 476481, 2018.

[16] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, ``Deep learning for visual understanding: A review," Neurocomputing, vol. 187, pp. 2748, Apr. 2016.

[17] Abduvaliyev, A., Pathan, A.-S. K., Zhou, J., Roman, R., and Wong, W.-C. "On the Vital areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, Issue 3, pp. no. 1223–1237, 2015.

[18] Abubakar, A. I., Chiroma, H., Muaz, S. A., and Ila, L. B. "A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-driven based Intrusion Detection Systems", Procedia Computer Science, Vol. 62, pp. no. 221–227, 2015.

[19] Bay, S. D., Kibler, D., Pazzani, M. J., and Smyth, P. (2015), "The UCI KDD archive of Large Data Sets for Data Mining Research and Experimentation", ACM SIGKDD Explorations Newsletter, Vol. 2, Issue 2, pp. no. 81–85, 2015.

[20] Aburomman, A. A. and Reaz, M. B. I. "A novel SVM-kNN-PSO ensemble method for Intrusion Detection System. Applied Soft Computing", Vol. 38, pp. no. 360–372, 2015.