International Journal of Computer Sciences and Engineering
Vol.**12**, Issue.**4**, pp.**68-74**, April **2024**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Survey Article

A Survey of DDoS Attack Detection Schemes: Methods, Challenges, and Datasets

V. Sughanthini[1*], P. Bharathisindhu[2]

[1]Dept. of Computer Science, Vellalar College for Women in Thindal, Erode, India
[2]Dept. of Computer Science, Vivekanandha Arts and Science College for Women, India

**Corresponding Author: vsugi91@gmail.com*

Received: 27/Feb/2024; **Accepted**: 02/Apr/2024; **Published**: 30/Apr/2024. **DOI**: https://doi.org/10.26438/ijcse/v12i4.6874

Abstract: Cloud computing makes use of a significant amount of virtual storage to provide services on demand via the Internet. The main benefits of cloud computing are reduced service costs and the elimination of the need for consumers to set up expensive computer hardware. The rapid integration of cloud computing with business and numerous other domains has prompted scholars to investigate novel, related technologies. Because of the cloud storage server's scale and accessibility, individual businesses and users bring their apps, data, and facilities to it for computing operations. Despite the advantages, switching from local to remote computing has created several challenges and security issues for service providers as well as clients. The cloud service provider uses several web technologies to supply its services via the Internet, raising fresh security concerns. The DDoS assault, which aims to prevent legitimate users from accessing a target system or network by overloading it with traffic, is the most serious security issue in cloud computing. In light of this, the article covers the principles of cloud computing, as well as its various forms, security concerns, DDoS assaults, and methods for detecting them using performance metrics and datasets. Lastly, a discussion of cloud computing's difficulties is included.

Keywords: Cloud Computing, Distributed Denial of Services (DDoS), DDoS attack Detection; Machine learning; Deep learning

1. Introduction

To store, manage, and process data instead of depending on local infrastructure or personal computers, one method is known as "cloud computing," which is the practice of using distant servers, frequently housed on the internet. It entails using and gaining access to a variety of computer resources, such as networking, storage, servers, databases, software, and storage, through the internet. Significant benefits of cloud computing include widespread network connectivity, on-demand self-service, quick flexibility, resource assembling, and measurable facilities [1]. Based on the services offered, such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), cloud computing is divided into three groups. Cloud computing deployments include private, public, multi-cloud, and hybrid cloud architectures. Popular cloud service providers include IBM Cloud, Microsoft Azure, Google Cloud Platform, and Amazon Web Services (AWS), among others. To satisfy various company demands, these companies provide a wide range of services and solutions. In general, cloud computing has transformed how businesses use and manage their computer resources, allowing for higher productivity, scalability, and accessibility while also lowering costs and administrative responsibilities. Major problems and difficult tasks in cloud computing are security concerns. DDoS attacks are one of the most significant security problems in a cloud setting [2]. Any happening or malicious movement that decreases or stops a cloud from providing its intended features and services is considered a cloud-related security threat. Economic loss, lost time, and both long and short-term repercussions on the victim CSP were all brought on by DDoS attacks. A DDoS assault is more effective since the attacker doesn't need to build a defense force before attacking using bots or zombies. All of these bots are automated to attack the target and impair their operation. They attempt to flood them using the property the CSP has offered[3].

2. DDoS attack detections

In a cloud context, DDoS is a particularly exciting security problem that causes traffic during resource sharing. Hence, detecting DDoS is important to work to provide end users with more effective resource sharing [4]. Techniques for detecting DDoS attacks may be roughly separated into two kinds: signature [5] and anomaly-based methods [6]. The network traffic gathered by the signature-based detection approach is compared to attack patterns, with packet byte or sequence. Comparing this type of detection system to

anomaly-based detection approaches, they are far simpler to comprehend, create, and produce more meaningful findings.

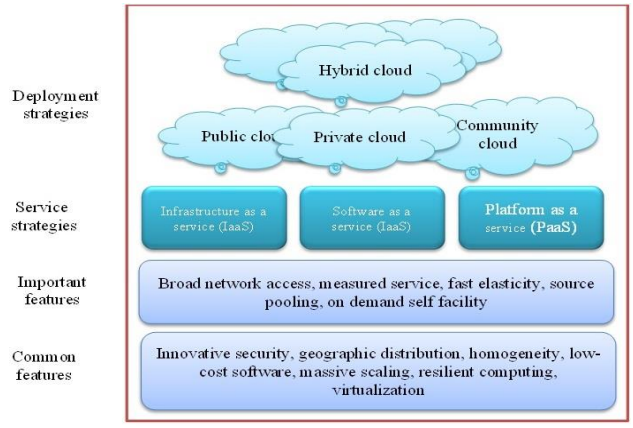

Figure 1 : Architecture of cloud computing

However, only known attacks with a predefined pattern may be detected using a signature-based detection approach. Using behavioral patterns, the anomaly detection technique is laboring to categorize the assault. This detection method can locate the unidentified assault. It does not, however, offer poor precision [7]. The authors of this work undertake a quick survey on artificial intelligence (AI) -based detection methods. The study of techniques and models that enable computers to learn from data to make predictions based on that data without being explicitly automatic is known as machine learning (ML) [8]. It is a subset of AI that gives computers the capability to autonomously learn from their experiences and get better. Consequently, a variety of MLs are employed to identify DDoS attacks in cloud environments [5, 9-13]. DDoS may be divided into two groups: semantic and brute-force[14].

1. High-rate attack

The high-rate / flooding attack) is another name for the brute force attack. The attackers send a massive volume of fraudulent requests to reduce the targeted cloud server's network capacity. By destroying the network capacity and router processing capabilities, the connection is disrupted. A network or transport-level flooding assault is the name given to the high-rate attack. High-rate attacks include those that use the User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) flood. Killing server resources like memory, disc, and CPU makes the cloud service unavailable to authorized users. These attacks, which include a flood attack on the HTTP protocol, a DNS flood attack, and a flood attack on the SMTP protocol, are referred to as application-level attacks [10, 15]. Such attacks start with the attackers discovering the vulnerability of a sizable number of computers to create attack armies known as a botnet. The attacker can establish control and then transfer it to a cloud server, which then distributes it to the many cooperating hosts. The cooperative hosts direct the onslaught of requests to a single or more cloud servers.The botnet computer may launch DDoS assaults using an IP spoofing technique to disguise the real source. Finding the attacker's actual location is therefore a difficult but crucial task.

1. Low-rate attacks

Semantic attacks, which take advantage of protocol weaknesses, are also known as vulnerability attacks or low-rate attacks. A small quantity of malicious traffic is sent to the target application by the attackers. Comparing low-rate assaults against high-rate attacks, finding the lowest-rate attack is a highly difficult and important undertaking. Due to its short traffic volume and quiet behavior, low-rate attacks are more challenging to detect than high-rate attacks. Because the attacker makes malicious requests at a very low rate, traffic volume-based defense measures are unable to detect it. Instead of stopping the cloud services, the attack modifies the Quality-of-Service (QoS) requested by the authorized user. There are four different low-rate attacks: the shrew, RoQ, LoRDAS, and EDoS.

3. The life cycle

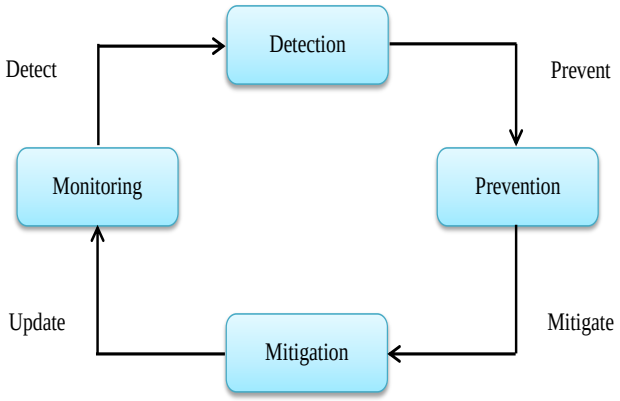

Figure 2 : DDoS life cycle

Figure 2 illustrates the four stages of a DDOS attack: “monitoring, detection, prevention, and mitigation” [16]. Important data about the network or host are gathered during the monitoring phase. To identify the malicious attempt, the detection step examines the network traffic that was collected. The prevention is used to defend the service and resources against certain apps being developed at several locations [17]. The mitigation phase calculates the attack's intensity and takes specific measures to control its effects. The prevention receives the results of the mitigation and updates the preventative measures accordingly. Only the detection phase is being thoroughly reviewed in this work out of four.

4. Related Work

In There are various ML algorithms have been applied to detect attacks. Hence, this section presents some of the most recent research works done in this field**.** S. Velliangiri et al. (2020) [18] have focused on creating a deep learning-based classifier that can detect DDoS attacks. Users' service requests are gathered and characterized as log information. To reduce the training time, numerous vital features from the log file are chosen using the Bhattacharya distance. Here, the EHO is modified with the Taylor series to create a ‘Taylor-EHO-based Deep Belief Network (TEHO-DBN)’ for the finding of DDoS attacks. G. S. Kushwah et al. (2022) [19]

designed a new hybrid ML model based on ELM and adaptive DE (ADE). In the suggested model, weights between hidden and output layers are calculated analytically, whereas weights and biases of ELM is optimized using ADE. During the evolution process, the ADE is altered to select the crossover operator.

M. G. Alam et al. (2022) [20] developed a new detection scheme based on four phases and before employing the data samples to detect attacks, they must first be trained. Later, each file's sample group is made, and during the data pre-processing stage, the data samples are pre-processed. The second step in the feature selection process is the optimization of the chosen features using kernel principal component analysis (KPCA) to provide the best possible features. An SVM-based discrete EHO is then used in the classification phase. A. Rezaeipanah et al. (2021) [21] suggested a new detection technique based on a hybrid approach to combat DDoS attacks in the context of cloud computing.

A. Agarwal et al. (2021)[22] designed a new detection scheme using feature selection with a whale optimization algorithm (FSWOA) and a DL called FS-WOA–DNN to mitigate DDoS attacks effectively. To make the classification process easier, FSWOA is utilized to determine the optimal set of features. DNN is applied to those extracted features to distinguish between genuine and hacked data. The usual data are secured using homomorphic encryption and are safely kept in the cloud to further increase the security of the suggested approach. P. S. Muhuri et al. [23] developed a new approach for intrusion detection by LSTM with a GA for optimal feature selection, the proposed method has improved intrusion detection by utilizing GA-based LSTM classifiers with the best feature set. Wang et al. (2020) [24] used feature selection and feedback to create a dynamic MLP-based DDoS assault detection technique. The best features are chosen sequentially using MLP throughout the training phase, and a feedback mechanism was created to recreate the detector when important dynamic detection mistakes are detected.

Table 1 : Details of datasets

References	NSL-KDD	ISCX IDS 2012	CIDDS-001	UNSW-NB15	CIC-IDS2017	CICDDoS2019	Customized datasets
[18]						✓	✓
[19]	✓	✓	✓				
[20]	✓	✓		✓	✓		
[21]	✓					✓	
[22]					✓		
[23]	✓						
[24]							✓
[25]	✓	✓					✓
[26]	✓	✓		✓		✓	
[27]	✓	✓		✓		✓	
[27]	✓						
[28]	✓	✓					
[29]	✓	✓		✓	✓		
[30]	✓	✓	✓				
[31]	✓				✓		
[32]	✓				✓		
[33]					✓		
[34]	✓				✓		
[35]							✓
[36]	✓						✓
[37]		✓					✓

Ahuja, N et al. (2021) [25] suggest utilizing ML to separate DDoS attack traffic from benign traffic to counteract this assault. Identification of new characteristics for DDoS attack detection is the main contribution. To generate the dataset and train machine learning algorithms, novel characteristics are logged into a CSV file. Arunadevi et al. (2022) [26] developed a brand-new detection method based on artificial plant optimization (APO) and back propagation neural network (BPNN). Enhancing the BPNN's capacity to recognize the global optimal value and preventing it from opting for the local minimum is the aim of optimization. For evaluating effectiveness in tests, the suggested improved APO-BPNN detection approach makes use of four different performance indicators and two benchmark datasets. Kushwah et al. (2020) [27] developed a new DDoS attack detection classically based on ELM created by the author.

Table 2 : Performance measures details

References	Accuracy	Precision	Recall	F-measure	True Positive Rate (TPR)	False Positive Rate (FPR)	False Alarm rate (FAR)
[18]	✓	✓	✓				
[19]	✓	✓	✓	✓			
[20]	✓	✓	✓				
[21]	✓	✓	✓	✓			
[22]	✓	✓	✓	✓			
[23]	✓	✓	✓	✓	✓	✓	
[24]	✓	✓	✓	✓		✓	✓
[25]	✓	✓	✓	✓		✓	✓
[26]	✓	✓	✓	✓	✓		
[27]	✓	✓	✓	✓	✓		✓
[28]	✓	✓	✓				
[29]	✓	✓	✓	✓			
[30]	✓	✓	✓	✓			
[31]	✓	✓	✓				
[32]	✓	✓	✓	✓			
[33]	✓	✓	✓	✓			
[34]	✓	✓	✓	✓			
[35]	✓	✓	✓	✓			
[36]					✓	✓	✓
[37]	✓	✓	✓	✓			✓

Experiments demonstrate the proposed model's rapid training time and good detection accuracy. The same authors (2020) [28] developed a new approach for identifying DDoS attacks. Voting ELM (V-ELM) is used to construct the suggested system. Experiments have demonstrated that the developed system identifies attacks with 99.18% and 92.11% accuracy.

In 2021, [29] developed an enhanced Self-Adaptive Evolutionary ELM called SaE-ELM for detecting attacks.

The SaE-ELM is enhanced by the addition of two extra components. It can start by using the best crossover operator. Next, it can decide on its own how many hidden layer neurons are required. These traits enhance the model's potential for classification and learning. Kushwah, G.S et al. (2022) [30] developed A new hybrid ML-based technique to detect malicious threats is suggested based on ADE and ELM. The connection weights and bias of ELM are optimized via ADE. To choose the appropriate crossover operator during the evolution process, the ADE is adjusted. The same authors (2023) [31] provide a DDoS attack detection technique that is based on bagging ensembles. The base classifier is an ELM with one class. These attacks have been discovered using an outlier detection-based method. Fatani, A et al. (2021) [32] provide an effective AI-based IDS for IoT. The author uses of developments in DL and metaheuristic (MH) algorithms, whose effectiveness in addressing challenging engineering challenges has been validated. CNNs are a feature extraction method to extract relevant characteristics. Furthermore, a novel technique for feature selection utilizing the operators of the DE is an innovative method of transient search optimization (TSO). To better balance the exploitation and exploration stages, the proposed TSODE takes advantage of the DE.

Sanjalawe Y et al. (2023) [33] presented a hybrid DL for DDoS attack detection using hybridizing CNN and LSTM due to its resilience and effectiveness in recognizing normal and attack traffic. Additionally, the most crucial features that would affect the performance of detection in detecting DDoS attacks are chosen using the ensemble feature selection, and mutualization aggregation between various ML approaches. Thangasamy, A et al. (2023) [34] developed a new detection technique based on DBN and a hybrid LSTM. The prediction error is decreased by combining the PSO technology with LSTM weight optimization. DBN is used to extract IP packet features and identify DDoS attacks using the PSO-LSTM model.

Islam, U et al. (2023) [35] developed a hybrid model for SVM-KNN-LR-based real-time MDOS and cloud attack detection is presented. To extract pertinent characteristics for attack detection, the dataset for this study was pre-processed after being gathered from a variety of sources. Additionally, a feature selection procedure was used to determine the most crucial traits for attack detection. Balasubramaniam, S et al. (2023)[36] suggested an efficient method to detect DDoS attacks based on the gradient hybrid leader optimization (GHLBO). The approach is in charge of effectively training a deep-stacked autoencoder (DSA) to recognize an attack. Here, a deep max-out network (DMN) with an overlap coefficient performs feature fusion, while the oversampling process does data augmentation.

M. Malik et al. (2023) [37] offer a feature engineering and ML to detect DDoS attacks. There are two phases to the framework. The complexity study of the feature-engineered data set in the second phase suggests an ML model. To effectively combat DDoS attacks, it is required to take a complete approach that includes proactive monitoring, real-time traffic analysis, scalable mitigation technologies, and cooperation between cloud providers and clients. The system takes too long to locate the anomalous instances since the detection method necessitates additional calculations. Therefore, detection speed rather than accuracy must take precedence for the real-time revelation of assaults.

5. Challenges of DDoS attacks

In this survey article, numerous detection approaches are offered as theories in response to a recent survey on the detection of DDoS attack schemes. It is difficult to create and implement a flawless real-time detection technique. Due to the increasing demands for detection and reaction, researchers are having a difficult time coming up with an effective detection strategy. In cloud computing systems, DDoS attacks provide serious difficulties. The following are some difficulties brought on by DDoS assaults in cloud computing:

1. Scalability

The high rate (flooding attack) is another name for the brute force attack. The attackers send a massive volume of fraudulent requests to reduce the targeted cloud server's network capacity. By destroying the network capacity and router processing capabilities, the connection is disrupted. A network or transport-level flooding assault is the name given to the high-rate attack. High-rate attacks include those that use the TCP, UDP, and ICMP flood. Killing server resources like memory, disc, and CPU makes the cloud service unavailable to authorized users. These attacks, which include a flood attack on the HTTP protocol, a DNS flood attack, and a flood attack on the SMTP protocol, are referred to as application-level attacks [10, 15]. Such assaults start with the attackers discovering the vulnerability of a sizable number of computers to create attack armies known as a botnet. The attacker can establish control and then transfer it to a cloud server, which then distributes it to the many cooperating hosts. The cooperative hosts direct the onslaught of requests to a single or more cloud servers.The botnet computer may launch DDoS assaults using an IP spoofing technique to disguise the real source. Finding the attacker's actual location is therefore a difficult but crucial task.

2. Multi-tenancy

Platforms for cloud computing are frequently multi-tenant settings where several users and applications share a single underlying infrastructure. The performance and accessibility of resources and services used by other tenants may be impacted by a DDoS assault on one tenant or application. Isolating and reducing attack traffic while guaranteeing minimum effect on genuine users is the difficulty.

3. Network complexity

Virtual networks, load balancers, and other network elements are all part of the intricate network topologies seen in cloud settings. These components are vulnerable to DDoS assaults, making it difficult to efficiently identify and stop unwanted traffic. The malicious traffic can also overload network connections and prevent genuine users and services from connecting.

4. Attack variability
DDoS attacks can take many different forms, including protocol attacks, application-layer attacks, and volumetric attacks. Attackers' strategies are always changing, making it difficult to anticipate and fight against new attack vectors. To keep one step ahead of attackers, cloud providers must regularly improve their DDoS mitigation techniques.

5. Shared security responsibility
A shared responsibility paradigm exists in cloud computing between the cloud provider and the client. While the underlying infrastructure's security is normally ensured by the cloud provider, consumers are still in charge of protecting their apps and data. To properly identify, mitigate, and recover from a DDoS attack, the cloud provider and the client must work together.

6. Detection and mitigation of latency
DDoS attacks must be promptly detected and mitigated to have as little damage as possible. However, the process of identification and mitigation might cause delays, particularly in expansive cloud settings. Long-lasting service interruptions caused by slow response times can hurt both the cloud provider and its clients.

7. Cost
DDoS attack mitigation can be costly, especially for cloud providers that need to spend on a strong infrastructure, monitoring tools, and qualified security people. In addition, service outages can have a big financial impact and risk losing customers' confidence.

To effectively combat DDoS attacks, it is necessary to take a complete approach that includes proactive monitoring, real-time traffic analysis, scalable mitigation technologies, and cooperation between cloud providers and clients. The system takes too long to locate the anomalous instances since the detection method necessitates additional calculations. Therefore, detection speed rather than accuracy must take precedence for the real-time revelation of assaults.

6. Discussion

Cloud computing also needs a security solution to protect against insider threats and DDoS attacks. Other options are still useful for the cloud. However, the attacker's danger cannot be resolved with the current options. An active area of research in these phenomena is the identification of DDoS attacks in cloud computing. Create a marker that may be used in this situation to identify DDoS attacks. The likelihood of protecting the cloud system will rise as a result of this signal. Similarly, it is still difficult in a cloud environment to distinguish between legitimate users and criminal users. Defense strategies based on machine learning have grown popular for stopping DDoS attacks. They are capable enough to properly deal with vulnerabilities since they can reliably identify and anticipate millions of network intrusions when compared to other mitigation and prevention-based security measures. Any defensive model must include detection since it serves as the foundation for subsequent categorization of network abnormalities. Hence, the present paper conducts reviews based on recent publications which are collected from various journals, conference proceedings, and books. Table 1 demonstrates the particulars of datasets used in the collected papers and Table 2 shows the details of performance measures which are indicated with tick symbols. DDoS protection is progressively fetching the consideration of learning into probable solutions for dealing with the reorganized world of today. Academics and security experts are now more intent on exerting their best efforts in quest of new potential solutions to close the security holes by addressing the changing problems and obstacles.

7. Conclusion and Future Scope

Rapid system development, minimal prices, lots of storage, and easy system access from anywhere at any time are all benefits of cloud computing. Thus, it is apparent that cloud computing is an emerging technology and that it is a widely utilized computing environment worldwide. However, using cloud computing is challenging due to several security and privacy risks. All cloud users should have a thorough understanding of the vulnerabilities, hazards, and threats that might occur there. In this paper, we have covered both the fundamentals of cloud computing and the security concerns that arise from its virtualized, distributed, shared, and public nature. A particularly difficult problem is differentiating between DDoS attacks with various rates and patterns and normal traffic. Over the years, other effective ML methods for detecting DDoS attacks have been put forth by other researchers. The readers will benefit tremendously from the tabular presentation of dataset details and performance measures and solutions. The discussion of certain unresolved cloud difficulties at the end of the paper will spur academics and researchers to study the topic.

Declarations

Data Availability
None

Conflict of Interest - Authors declare that they do not have any conflict of interest.

Funding Source
None

Authors' Contributions: Both authors designed the study and gathered the literature and articles. The final version of the manuscript was approved by all authors after it had been reviewed and modified.

References

[1] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Security and Communication Networks*, Vol.**9**, No.**16**, pp.**3724-3751, 2016.**

[2] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert systems with applications*, Vol.**34**, No.**3**, pp.**1659-1665, 2008.**

[3] N. Aslam, S. Srivastava, and M. Gore, "A comprehensive analysis of machine learning-and deep learning-based solutions for DDoS attack detection in SDN," *Arabian Journal for Science and Engineering*, Vol.**49**, No.**3**, pp.**3533-3573, 2024.**

[4] N. Agrawal and S. Tapaswi, "Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey," *Information Security Journal: A Global Perspective*, Vol.**26**, No.**2**, pp.**61-73, 2017.**

[5] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, Vol.**67**, pp.**147-165, 2016.**

[6] A. Rawashdeh, M. Alkasassbeh, and M. Al-Hawawreh, "An anomaly-based approach for DDoS attack detection in cloud environment," *International Journal of Computer Applications in Technology*, vol. 57, no. 4, pp. **312-324, 2018.**

[7] N. Agrawal and S. Tapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol.21, no.4, pp.**3769-3795, 2019**, doi: 10.1109/COMST.2019.2934468.

[8] R. Kavitha, K. Saravanan, S. A. Jebakumari, and K. Velusamy, "Machine learning algorithms for IoT applications," *Artificial Intelligence for Internet of Things: Design Principle, Modernization, and Techniques*, p. 185, 2022.

[9] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," *Sustainability*, vol. 12, no. 3, p. 1035, 2020.

[10] M. Idhammad, K. Afdel, and M. Belouch, "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest," *Security and Communication Networks*, vol. **2018, 2018.**

[11] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. **385-393, 2016.**

[12] A. Amjad, T. Alyas, U. Farooq, and M. Tariq, "Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 6, no. 23, 2019.

[13] M. Ghanbari and W. Kinsner, "Detecting DDoS Attacks Using Polyscale Analysis and Deep Learning," *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI)*, vol. 14, no. 1, pp. 17-34, 2020.

[14] A. Naithani, S. N. Singh, K. K. Singh, and S. Kumar, "Machine Learning for Cloud-Based DDoS Attack Detection: A Comprehensive Algorithmic Evaluation," in *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2024: IEEE, pp. 561-567.

[15] O. A. Osanaiye and M. Dlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment," in *IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON)*,: IEEE, pp. **1-6, 2015.**

[16] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*, vol. 107, pp. 30-48, 2017.

[17] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, pp. 3655-3682, 2017.

[18] S. Velliangiri, P. Karthikeyan, and V. Vinoth Kumar, "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 33, no. 3, pp. 405-424, 2021.

[19] G. S. Kushwah and V. Ranga, "Detecting DDoS Attacks in Cloud Computing Using Extreme Learning Machine and Adaptive Differential Evolution," *Wireless Personal Communications*, pp. 1-**24, 2022**.

[20] M. G. Alam, S. J. N. Kumar, R. U. Mageswari, and T. M. Raj, "An Efficient SVM Based DEHO Classifier to Detect DDoS Attack in Cloud Computing Environment," *Computer Networks*, p. 109138, **2022**.

[21] A. Rezaeipanah, S. E. Mousavipoor, M. Asayeshjoo, and M. Sadeghzadeh, "Combining Particle Swarm Optimization and Entropy to Detect DDoS Attacks in the Cloud Computing," *Journal of Business Data Science Research*, vol. 1, no. 1, pp. 33-43, 2021.

[22] A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS attack using deep learning model in cloud storage application," *Wireless Personal Communications*, pp. **1-21, 2021.**

[23] P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, "Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks," *Information*, vol. 11, no. 5, pp. **243, 2020.**

[24] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Computers & Security*, vol. 88, p. **101645, 2020.**

[25] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *Journal of Network and Computer Applications*, vol.**187**, pp.**103108, 2021.**

[26] M. Arunadevi and V. Sathya, "DDoS Attack Detection using Optimized Back Propagation Neural Network with Artificial Plant Optimization in Cloud Computing," in *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)*,: IEEE, pp.**815-820, 2022.**

[27] G. S. Kushwah and S. T. Ali, "Distributed denial of service attacks detection in cloud computing using extreme learning machine," *International Journal of Communication Networks and Distributed Systems*, vol.23, no.3, pp. **328-351, 2019.**

[28] G. S. Kushwah and V. Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," *Journal of Information Security and Applications*, vol. 53, p. 102532, 2020.

[29] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Computers & Security*, vol. 105, pp.**102260, 2021.**

[30] G. S. Kushwah and V. Ranga, "Detecting DDoS attacks in cloud computing using extreme learning machine and adaptive differential evolution," *Wireless Personal Communications*, vol. 124, no. 3, pp. **2613-2636, 2022.**

[31] G. S. Kushwah, S. Singh, and S. K. Mahana, "One-Class ELM Ensemble-Based DDoS Attack Detection in Multimedia Cloud Computing," in *Examining Multimedia Forensics and Content Integrity*: IGI Global, 2023, pp. 38-55.

[32] A. Fatani, M. Abd Elaziz, A. Dahou, M. A. Al-Qaness, and S. Lu, "IoT intrusion detection system using deep learning and enhanced transient search optimization," *IEEE Access*, vol.9, pp.**123448-123464, 2021.**

[33] Y. Sanjalawe and T. Althobaiti, "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning," *Computers, Materials & Continua*, vol. 75, no. 2, 2023.

[34] A. Thangasamy, B. Sundan, and L. Govindaraj, "A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques," *Computer Systems Science & Engineering*, vol. 45, no. 3**, 2023**.

[35] U. Islam, A. Al-Atawi, H. S. Alwageed, M. Ahsan, F. A. Awwad, and M. R. Abonazel, "Real-Time Detection schemes for Memory DoS (M-DoS) Attacks on Cloud Computing Applications," *IEEE Access*, **2023**.

[36] S. Balasubramaniam *et al.*, "Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing," *International Journal of Intelligent Systems*, vol. **2023, 2023.**

[37] M. Malik and M. Dutta, "Feature engineering and machine learning framework for DDoS attack detection in the standardized internet of things," *IEEE Internet of Things Journal*, **2023.**

AUTHORS PROFILE

V. Sughanthini holds the position of Assistant Professor in the Department of Computer Science at Vivekanandha Arts and Science College for Women in Sankari. She has completed both her undergraduate and postgraduate studies in Computer Science. Her pursuing a Ph.D. in computer science, specializing in Soft computing, under the guidance of Dr.P.Bharathisndhu in the Department of Computer Applications at Vellalar College for Women in Thindal, Erode at Bharathiar University. V.Sughanthini's professional interests are Machine Learning and coding. She attended morethan 4 National and international conferences and presented a paper in various topics.

Dr. P. Bharathisndhu holds the position of Assistant Professor in the Department of Computer Applications at Vellalar College for Women in Thindal, Erode. She has completed both her undergraduate and postgraduate studies in computer applications. Her Ph.D. in computer science, specializing in Mobile hoc networks, was conferred by Bharathiar University. Additionally, she has demonstrated her expertise by clearing the State Eligibility Test (SET). Dr. Bharathisndhu's professional interests span Machine Learning, Deep Learning, and MANET. At present, she is actively guiding four Ph.D. scholars and has an impressive record of 15 publications in international journals.

Commencing her career as an assistant professor in 2011, Dr. Bharathisndhu has further enriched her skill set by completing a course in Effective Public Speaking and Training. She is also an engaged member of Lions Clubs International. Beyond academia, she has conducted numerous motivational training sessions for school and college students in and around Erode, impacting more than 1500 students. She is actively involved in providing NET/SET coaching for faculty members in computer science. She also serves as a resource person for workshops and acts as a keynote speaker for various colleges and schools.

