JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 5 No. 2 (2024) 29-51
https://publisher.uthm.edu.my/ojs/index.php/jscdm

Comprehensive Examination of Learning-based DDoS Defence Methods for Cloud Computing Networks

Nafea A. Majeed Alhammadi[1]*, Mohamed Mabrouk[1], Mounir Zrigui[1]

[1] *Research Laboratory in Algebra, Numbers Theory and Intelligent Systems, University of Monastir, 5000, Monastir, TUNISIA*

*Corresponding Author: nafeaalhamadi@yahoo.com
DOI: https://doi.org/10.30880/jscdm.2024.05.02.003

Article Info

Received: 1 June 2024
Accepted: 13 November 2024
Available online: 18 December 2024

Keywords

Flooding attack, DDoS, machine learning, deep learning, reinforcement learning, intrusion detection systems

Abstract

Cloud computing is a valuable technology whose resources, data storage, software, infrastructure, and platform services are a few of its perks. The majority of cloud services are executed through an Internet connection. Thus, they are susceptible to a large extent of attacks that can lead to the disclosure of sensitive information. Malicious activities such as distributed denial-of-service (DDoS) attacks immediately threaten the cloud environment and the services offered to bona fide users. This study examines the various machine learning (ML)-based, deep learning (DL)-based, and Reinforcement Learning (RL) DDoS detection methods used across different cloud environments. The primary goal of this literature review paper is to provide a comprehensive analysis of the existing literature regarding the latest trends in advanced flooding attack detection and intrusion detection systems (IDS) approaches used for defending cloud computing networks. The review is limited to the papers that have been published between 2016 and 2023 addressing methods of flood or DDoS defense for cloud computing networks. It focuses on advanced learning-based DDoS detection techniques based on ML, DL, and RL. It also describes other forms of flooding attacks and the testing dataset. Finally, it identifies a number of research issues, limitations, and directions for further research in the context of DDoS attack detection and prevention in cloud computing networks.

1. Introduction

Many sectors have greatly benefited from cloud computing since it results in scalability, cost-cutting, and better cooperation; hence, a company is well-placed to meet the directions of the market. However, it also has difficulties, such as security risks, data privacy, and correlation with reliable internet connection [1]. Cloud computing networks are often exposed to the harmful Distributed Denial of Service (DDoS) attacks. These attack attempts use many hacked systems, usually working as a group on the Internet, to overflow a targeted computer or network system [2]. This flood of requests causes too much traffic and stops real or legitimate users from using that system because the system is busy processing many requests, and they can't get in. These attacks exploit cloud resources' shared and expandable features, making them very hard to manage [3]. To find DDoS attacks in cloud setups, use traffic analysis tools that watch how data flows, analyze patterns, look for strange patterns, and learn past actions. Progressively, analyzing traffic patterns on the network can help identify DDoS attacks [4], [5].

There are two major ways of launching DDoS attacks through the Internet. The first type of attack requires the attacker to send malicious packets to the targeted system to confuse the user or the protocol running on the system (i.e., vulnerability attack) [6]. The second type of attack involves the attacker flooding the network/transport/application layers of the targeted network in a bid to cause network failure by exhausting the

network resources [7]. It consumes the bandwidth or processing capacity of the router or interrupts the services provided to legitimate users by exhausting the server's resources, like the I/O bandwidth, memory, central processing unit (CPU), and disk/database bandwidth [8].

The literature suggests several Artificial Intelligence (AI) types of learning algorithms like reinforcement learning (RL) [2], [4], [6], [9], Machine Learning (ML) [5], [7], [10], [11], and Deep Learning (DL) [3], [12], [13] algorithms to create an intrusion detection systems (IDS) method that complements filters for protecting cloud computing environment against DDoS attacks. Learning-based methods are gradually used in order to estimate and detect attack schemes through the analysis of historical data. Usually, these methods are used in iterations to improve the accuracy and speed of detection, which helps react in a timely and adequate manner to reduce the impact of DDoS attacks on cloud services [14], [15]. Usually, these IDS methods are used in iterations to improve the accuracy and speed of detection, which helps react in a timely and adequate manner to reduce the impact of DDoS attacks on cloud services. A combination of ML, DL, and RL has also been investigated in previous works, and examples are [16], [17], and [18]. These methods can instantly detect the attacks and keep the cloud computing network functional even under a DDoS attack.

Performing a survey on cloud computing security is necessary to comprehend the range of attacks against these networks, especially the kind and complexity of the flood attacks, including DDoS, which are difficult to protect against due to their volume and diffusion. It is also aimed at revealing learning-based defense measures based on identifying threats with the help of AI and subsequent countermeasures. Moreover, by acknowledging the downsides of current defense strategies, which may include high false positives or high resource necessities, the general analysis offers suggestions for further improvement or the development of new methods that improve the efficiency and credibility of cloud security solutions. This issue helps ensure that defense follows the growing complexity of cybercrime threats and protects the cloud infrastructure and data. Our previous work [19] focuses on analyzing the review papers and their outcomes. This study aims to enhance the effectiveness and efficiency of anomaly detection defense methods deployed in cloud computing networks for combating DDoS flooding attacks by analyzing the state-of-the-art ML, DL, RL and their possible combinations. There are five main questions that this review attempts to satisfy as follows:

1. what are the common attacks targeting cloud computing networks?
2. Why are flooding attacks considered challenging compared to other attacks?
3. what are the well-known learning-based defense methods?
4. What are the major issues in the existing defense methods?
5. How to improve these methods to deliver more reliable defense results?

This review paper is segmented into eight sections. Section 2 gives an overview of the review framework of the study. Section 3 presents various security issues in cloud computing. Types of attacks in cloud computing are illustrated in Section 3. Section 4 describes the defense methods against flood attacks in cloud computing. The most efficient ML, DL, and RL detection methods of DDoS attack target cloud computing are discussed in detail in this section. Section 5 discusses the advanced learning-based models in flood attack detection methods of several studies and presents the research direction. Furthermore, the recent flooding attack dataset has been highlighted in this section. Section 6 summarizes the review with concluding remarks.

2. Review Framework

This review presents the recent trends in sophisticated flooding attack detection methods for cloud computing systems. It covers eight years, from 2016 until the end of 2023. The keywords used for the search are flood attack, DDoS attack, cloud computing, IDS, RL, ML, and DL. Figure 1 shows the framework of the review process, including the main themes and direction of the literature review of the DDoS research topic.

This literature review part of the study covers 66 research publications, including several review articles. This review's scope is divided into four main points: the cloud computing domain, the attack approaches, the detection and defense methods, and the testing and evaluation of these methods. The review is directed to focus more on the existing various DDoS attacks and defense methods targeting cloud services.

Various ML techniques, including DT, NB, ANNs, SVM, and K-NN, were examined to solve the security issues in cloud computing. Also, the most effective DL techniques, such as DNN, CNN, LSTM, and GRU, have been presented. Also, the study covers the Sophisticated types of flooding attacks using SA, MAS, and RL. Furthermore, the study examined and evaluated the offered methods, noting their advantages and disadvantages. Subsequently, the review of the contributions of various studies to developing sophisticated and efficient DDoS attacks defines techniques.

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 29-51

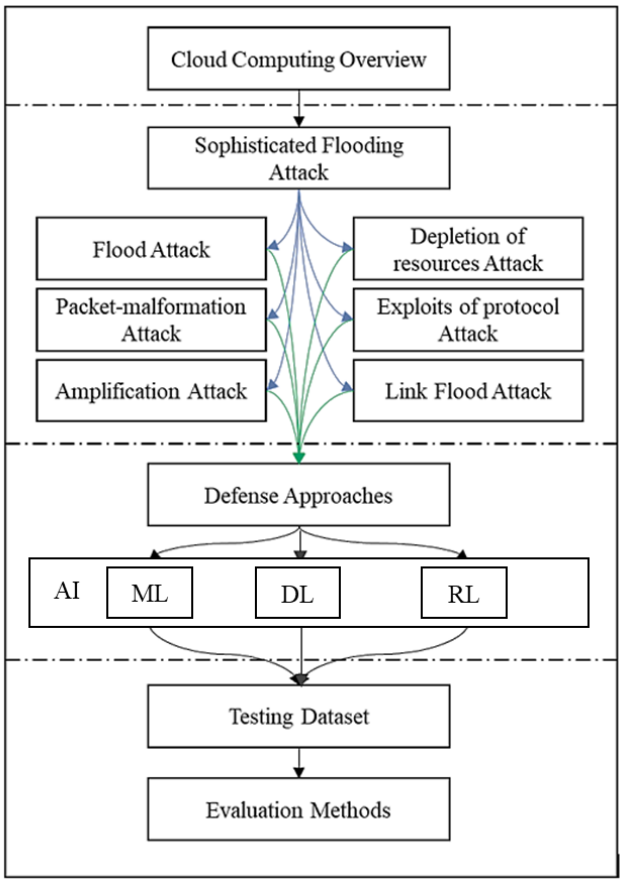

Fig. 1 *The framework of the review process*

3. Security Issues in Cloud Computing Networks

Cloud computing is a model that offers computing resources for applications on request and with minimum effort and maintenance. It is the technique of using Internet services to process and store information and data within a particular server [8]. The infrastructure and services are provided through cloud computing on a "need basis." It includes the use of the Internet in the sharing of computer resources. Such resources can be software, a developer interface, virtual hardware, or storage. A possible future paradigm termed 'cloud computing' delivers applications, platforms, and IT infrastructure as a service. It is totally virtual and does not require direct access to specific computers or memory. Fig. 2 shows the organization of data security and privacy in cloud computing.

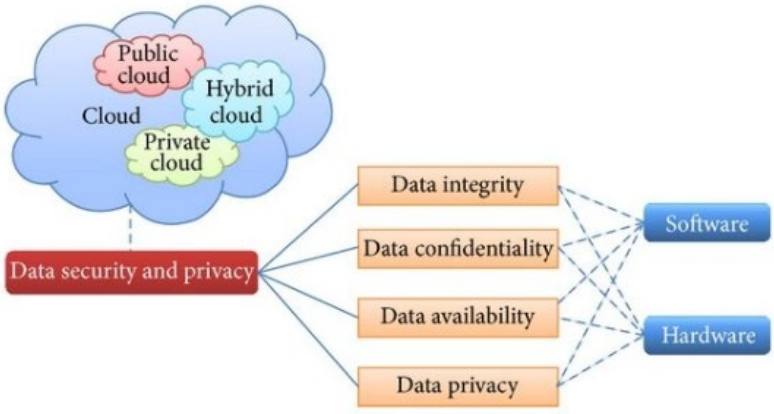

Fig. 2 *The organization of data security and privacy in cloud computing [19]*

Furthermore, the industrial cloud is also rising as more consumers migrate their data and applications to a remote cloud. Customers obtain more elastic use of the data and applications [20]. Many businesses' common approach has been enhancing their competency to manage with existing software while not adding extra structures. The future of technology is embodied in computing, providing users with a practical paradigm for Internet-based access to cloud resources and services. With this development, the technique is revolutionizing from desktop to utility computing. The cloud employs several access models, namely private, public, community, and hybrid, to deliver software, infrastructure, and platform as a service [19]. Over the last several years, utilizing the Internet as their platform, many organizations, schools, hospitals, and banks have started overhauling the corporal large cloud computing corporations such as International Business Machines (IBM), Microsoft, Google, and Amazon corporations [6].

3.1 Categories of Cloud Computing Security Concerns

To formulate quality of Quality of Service (QoS) of experience criteria, stricter quality criteria must be met in cloud computing, meaning a network-enabled scalable assured QoS, low cost of computation and infrastructure, and simple accessibility [21]. Despite the benefits associated with cloud computing, there are several impediments to this technology in so far as integrity, security, availability, cost, and performance are concerned, and most of these challenges are new born and have not fully evolved [22], [23], [24]. The greatest barrier that has been observed in cloud computing is security, so many individuals are afraid to use someone else's hard drive to store or run software [25], [26], [27].

Confidentiality, integrity, availability, and privacy are the four main categories used to categorize cloud computing security risks. These concerns are briefly examined as follows.

- Confidentiality: The risks associated with this problem are an internal threat, an external threat, and data concerns. The first of these is the risk of the employees of a Cloud Service Provider (CSP) getting unauthorized or illegal access to the Cloud service customers (CSCs) [28]. Second, cognizance of the risk of an external attack on cloud services running in an unsecured environment escalates. Third, because of human error, a lack of tools, and protected access failures, information leakage is an indefinite danger for cloud-based data; after that, anything is possible [29].
- Integrity: This is associated with issues with client access control, other data-related issues and complications such as data quality issues, and problems of data silos, all of which pose potential dangers. Overlapping the definition of security parameters with an inferior virtual machine (VM) design and a flimsy client-side hypervisor exposes the first danger of isolating information. This is still an issue in the cloud since it offers resources that connect the clients; if the resources transform, the credibility of the info may be affected [26], [30]. The second is weak client access control, which is accompanied by a number of problems and dangers because of the ineffectiveness of client access and character control and attack information assets. While analyzing the degree of compliance based on confidentiality and integrity, it can be seen that a good security system is constructed from Blockchain and cryptography algorithms [23].
- Availability: The threats might include advancement across the board, hassle in accessibility of an organization, physical damage in assets, and ineffective recovery systems. Firstly, the role of advancement on the board encompasses the influence of change in founding and the influence of client entrant tests for various customers. Both equipment and application evolution in the cloud could cause considerable impacts on the availability of cloud-based organizations [32], [33]. Cloud computing is applied in almost all fields, and it has several advantages it also has its disadvantages, such as security issues, risks, and challenges. The surveys show that one of the main issues of research in cloud computing is security [21]. There is a brief elaboration of numerous possibilities of security threats in cloud service delivery. Replicability of services is an essential aspect of cloud commerce. Thus, availability is the leading security concern among the multiple ones [26]. Of all discussed threat types, the DDoS attack seems to represent the biggest threat to the availability of resources and services linked to cloud computing. The problem of service accessibility also compounds this; for instance, the inability to register a domain name through a DNS organization is caused by the organization's lack of adequate system data transmission capacity or assets and software [30]. As is clearly stated, all cloud models are at risk since it is an external threat [34]. The third is the organization's ability to handle service providers, cloud customers, and wide area networks (WANs) even with disruptions to the physical network. Another example of wrong recovery strategies is insufficient recovery from failures; such an approach can considerably affect the recovery's tempo and rate of success.
- Privacy: The nature of cloud services is to store and manage data on remote servers accessed through the Internet. Therefore, data privacy issues in cloud computing are a major headache [28]. These problems arise more so because data is often saved elsewhere, where it may be at risk of unauthorized access, data breaches (hostile entities breaking in and stealing the database), or loss of data control. Distrust about

privacy due to the uncertainty involved in how cloud service providers treat data. This matter encompasses issues such as mining, surveillance, and compliance with national data protection laws in different countries. The multitenant nature of cloud computing is another facet that compounds these problems, as users on different accounts all share the same infrastructure resources, increasing the risk of data leakage [30]. The transfer of data between different jurisdictions may also encounter legal or regulatory problems, particularly in regions with strict data protection. Addressing these difficulties requires strong encryption, secure access controls, and clear policies in terms of data storage to protect both the privacy and security of cloud-based data.

3.2 Types of Attack in Cloud Computing Networks

In general, infrastructure as a whole has become frequently attacked due to the increased usage of the technique called virtualization [35]-[37]. Two of the threats characterized in the article are attacks on bandwidth and resource depletion in cloud computing systems. Such kinds of assaults feed the victim's network with information, such as unwanted traffic, to prevent the real traffic from entering the victim's network, effectively occupying all of the victims' or targeted systems' bandwidth [38]. Such attacks are carried out with new algorithms, which have been created recently or well-known software and tools [13]. These attacks are divided into the subcategories as follows [27], [31]:

- DDoS flood attack is a furious type of attack resulting in denial of service attacks. DDoS attacks are distributed counterparts and are considered the most dangerous malicious actions among all cloud security threats [39], [40].
- Link flood attack is one of the most lethal attacks that targets contemporary networks. These attacks can potentially result in the complete black out of the entire network since the vital links can be choked by means of a denial of service [41]. In a crossfire link flood attack, low-rate genuine traffic is flooded around the destination to isolate it and ensure it is easily distinguishable from the other traffic.
- Denial of Service (DoS) attacks are a significant threat to the dilemma of availability in cloud security. It is noted that DoS attacks have caused more problems in cloud computing than in single-tenanted architecture because millions of users will share the same cloud infrastructure [23].
- Protocol attacks intend to drain the victim's system of resources with the help of the exploits in the protocol stack. TCP-syn attacks act as a prototype of this type of attack. The system's hand-shake protocol of the connection is also in danger of this attack [12].
- A packet malformation attack concerns the packet bedeviled with undesirable information. These malicious data are sent to the victim by the aggressor by means of an IP address or IP packet to bring about its crashing or freezing. In IP address-based attacks, data is encapsulated with the same IP addresses as the source and destination, which ravages the victim's operating system. Due to this attack, the system slows down, leading to system failure [27], [31].
- Resource denial of service is performed to limit the resources accessible by the victim, with a view of denying any resources that can lead to the handling of appropriate user requests [28].
- The amplification attack intends several infected data frames to a particular NB IP address to generate epidemic data traffic. In this way, with the return of the feedback response, the systems being attacked will send a broadcast response to the devices in the broadcast address. Those targeting broadcast address services are vulnerable to being performed on many conventional networking devices [23], [32].

This DDoS flooding attack is categorized as the new generation of DoS attacks, but unlike those, they do not simply overload a server. Rather, they employ a number of compromised computers, sometimes called bots, to attack a single cloud server, the state of service-based cloud computing security vulnerabilities up to the present time. Recently, DDoS attacks have targeted large cloud-based corporations such as Amazon EC2, Sony, Microsoft, and RackSpace [14]. The DDoS attack scenario in the cloud server is displayed below in Fig. 3.

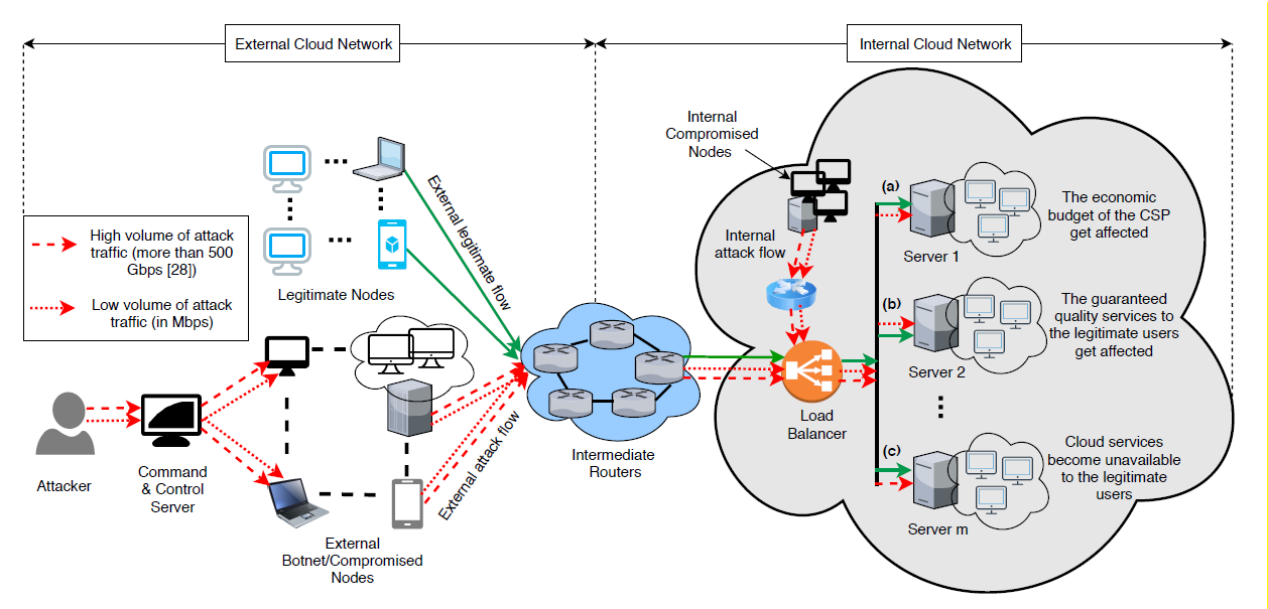

Fig. 3 *DDoS attacks in cloud computing networks [28]*

Parast et al. [21] conducted their study was expounded by investigating the development of a uniform taxonomy of the security threats within the three-layered scheme, IaaS, PaaS, and SaaS. The first and main submission is to look at how the output of CS has occurred over the last ten years with respect to DDoS attacks. Some of them respond to some of the recent critiques of cloud computing, testing datasets, or defensive approaches. Security experts have disclosed the DDoS flooding attack problem for quite some time, but the frequency and the consequences of such attacks are only growing. Therefore, it is currently absolutely essential to introduce the principles of adaptation and self-organization into the processes for creating effective cloud security solutions [23]. DDoS attacks can be initiated from a certain service, a cluster, a node, a virtual machine, or even the whole cloud. An attacker employs multiple zombie machines that he has already compromised to send many fake packets in a single direction toward a server [21]. Botnets are now a major problem, and the attackers are now targeting their victims well [5].

However, as indicated by studies, other equally pervasive opportunities and gains might be found in cloud computing [21]. It is also important to note that the opposite of the phenomena are risks and hurdles [22]. Flood attacks are furious attacks that create denial of service assaults. DDoS attacks are its distributed versions, and they are considered to be the most threatening actions among all security issues related to cloud computing. By exhausting their cloud resources and services, these attacks, in essence, are an effort to make the service unavailable to real customers.

4. Detection Method of Flood Attacks

Several types of defined methods for securing cloud computing environments against flooding attacks have been proposed. There are drawbacks to using conventional methods, such as high rates of false alarms and the need to update software constantly to keep up with emerging threats. In contrast to conventional methods, ML, DL, and RL techniques are well-versed in drawing attention to the risks. Furthermore, previous studies show that the most effective defense methods are based on ML, DL, and RL algorithms. The most effective and efficient detection and defense methods against flood attacks based on ML and DL have been illustrated and discussed in detail in this section. The ML algorithms include Artificial Neural Networks (ANN), K-Nearest Neighbors algorithm (K-NN), Decision Tree (DT), and Support Vector Machine (SVM). Popular algorithms like Naive Bayes (NB) and Random Forest (RF) are also presented. The DL algorithms include general Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent units (GRU). Another means used in flood attack detection is the agent-based method. This method includes three main types of architecture: Software Agent (SA), Multi-Agent System (MAS), and Reinforcement Learning (RL). The learning-based flood attack detection algorithms are displayed in Fig 4.

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 29-51

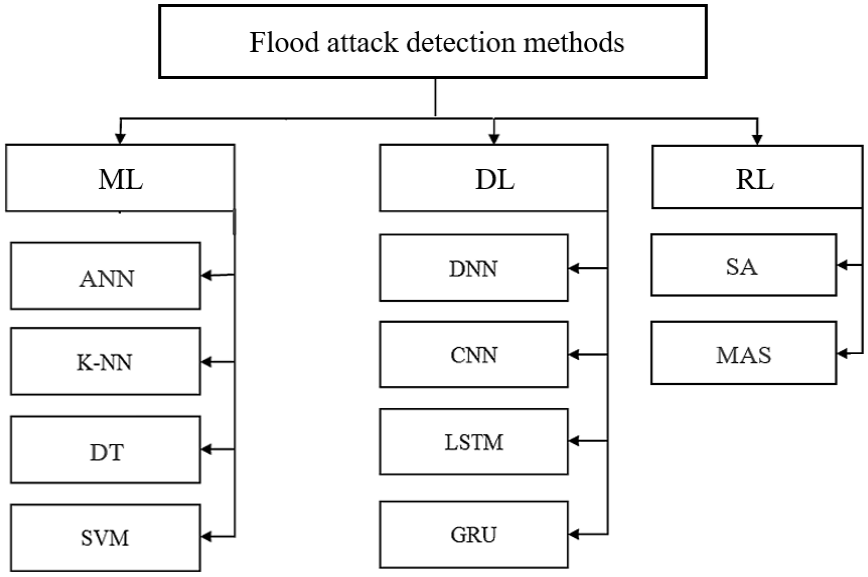

Fig. 4 *Learning-based detection methods of flood attacks*

4.1 Machine Learning Detection Methods

ML is a type of AI logic that explains how a certain task is accomplished in the process by showing the computations and measurable models and others that the headers, contingent models, and acceptance don't require [37]. In supervised learning, a form of ML, a limit is learned that maps or translates commitments into yields measured in model data yield sets. It assumes a bound from information about several planning models [33]. The need for cloud-based machine learning is such that all clouds will incorporate it in the near future. In that manner, it is possible that properly allocating and focusing ML could increase the safety of distributed computing. While more and more simple data migrated to cloud storage, more and more confidential data migrated to cloud storage, requiring higher security in cloud computing. To protect against such risks and to achieve real-time identification of risk factors with even higher accuracy than all the solutions mentioned above, further methodologies are described in [31]. First, describe an exemplar of a risk and threat definition procedure for each degree of danger. Then, the ways for handling threats that use both the methods of signature identification and anomaly detection are described and integrated into a single threat detection model.

4.1.1 Artificial Neural Networks

Artificial Neural Networks, abbreviated as ANN, is the basic modules of an information processing model intended to have some characteristics of the human brain. These ML institutions are charged with solving problems that would ordinarily be hard for humans to solve or involve complexities that cannot be handled by statistical means. The authors in [24] employed ANN algorithms to predict the most frequent risks in distributed computing. Security vulnerability of an Internet of Things (IoT) network was detected with the help of an ANN algorithm. This study employed the ANN to amplify the cognitive functions concerning learning and performance. Fig 5 represents a Single-Layer Perceptron (SLP) ANN with one input layer, hidden layer, and output layer.

The prediction of the cloud security presentation was made based on the Levenberg-Marquardt base point (LMBP). Mean square error (MSE) is the measure adopted to assess the prediction's accuracy and appraise the extent of the improvement. LMBP, the nonlinear improvement model, is used to improve the accuracy of the prediction and reduce the gap between actual yields and the overall presentation process. The cloud Delphi technique was employed for more informal meetings and inquiries [25]. The knowledge was collected with the help of the Delphi method, and the given data is classified as authoritative. To predict issues that may arise with distributed computing, there is a need for information to be measured, and this model uses the ANN algorithm [26], [27]. Security issues concerning clouds were foreseen with the help of the LMBP algorithm. Nevertheless, the algorithms can potentially safeguard cloud computing with good performance.

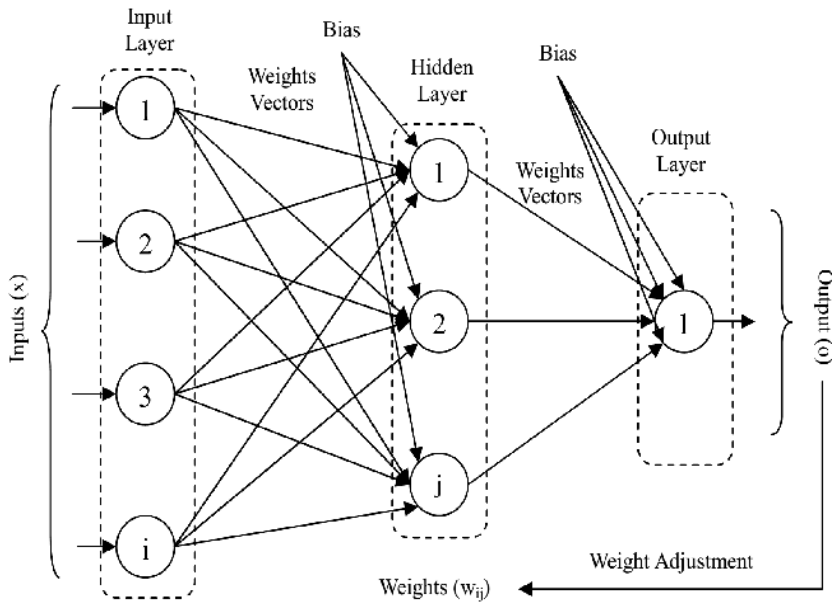

Fig. 5 *An ANN architecture for DDoS detection [24]*

Among other ML approaches for cybersecurity, artificial neural networks (ANNs) are two exceptional. The prior work of Shamshirb and Chronopoulos [29], which this study aims to extend, plans to use two datasets of malware and a High-Performance Extreme Learning Machine (HP-ELM) type of ANN to detect possible anomalous characteristics. The size of a botnet, a network of compromised computers, is proportional to the success of a distributed denial of service attack. Thirdly, botnets are used for large-scale scams and identity thefts. Managers of both systems and frameworks may utilize an IDPS because of its ability to detect disruption. If the IDPS picks up an interruption, email alerts may be sent to the authorized managers. The militancy level identification and protection abilities of ML IDPS are boosted.

Khan et al. [28], the authors proposed employing ANNs on top of encrypted data from a homomorphically safe semantic cryptosystem. Even though there are novelties in data protection, the insecurity surrounding data that is being held, managed, and shaped by an external party still comes as a discouragement for owners who want to be actively involved in utilizing the data. Any data owner who stores their information in the cloud should apply an accurate information governance system. One of the most basic skills in many branches of knowledge is synchronizing the examples. Nguyen et al. [31] detected mobile cloud computing cyberattacks using ANN. They proved that their architecture can raise the accuracy of attack detection to up to 97 percent. 11%. Attack and intrusion were detected using ANN [43]. The authors' presented model was evaluated using NSL-KDD and KDD-CUP datasets. They said that this could be detected using a proposed methodology to point out malicious actions of individuals who have not been authorized.

Similarly, ANN is used by [44] for the improvement of intrusion detection, by [45] for the protection of cloud computing, and by [46] for network security protection of edge computing systems. Wan et al. [47] proposed the four-layer cloud-assisted smart factory (CaSF) idea to improve the results of flow inquiries in the manufacturing domain. Four-layer ANN approaches are used to address this problem. From the ANN approaches and techniques, there is more trust, flexibility, and efficiency in a manufacturing organization, but the following are some challenges and technology barriers for the sector. Contemporary engineering designs encompass smart products, smart systems, smart use of the cloud, and smart applications. It is useful in handling CaSF problems. Therefore, the present paper employed a four-layered CaSF architecture for greater efficiency.

4.1.2 K-Nearest Neighbors Algorithm

Among all the applied ML algorithms, K-Nearest Neighbors (K-NN) can be attributed as the simplest for dealing with regression and classification [30]. K-NN uses and explains new data regarding similarity measurements (for instance, distance). The majority vote for its neighbors rounds up the classification [32]. Regarding privacy protection, particularly regarding online medical records, the authors of Park and Lee's cited work [30] proceed into the discussion. They provided a method that masks the access pattern of the medical datasets, symptoms, and diagnostic outcomes while preserving the confidentiality of the information. They proposed a method for finding the most similar k sets without revealing the participants' identities.

Mohsin et al. [33] used the k-NN algorithm as a basis for the method of data categorization they proposed. The aspects of information security and protection are also important for the information grouping outlined by the authors. Cloud services and digital arrangements were used to perform K-NN data arrangements. The K-NN aims to partition the data based on the amount of safety that is wanted. Two categories were created for the data: emotional and perceptive. Thus, the order of the information helped to identify the recognizable evidence of the information that is supposed to be guaranteed. In this case, the two specialized communities requiring privacy were the closed and sensitive information communities. Drawing upon a paradigm for decentralized computing, the authors suggested a security and privacy-related data hierarchy. The security of data led to another examination, which was the layout of the data. The K-NN classifier is the conclusion of this inquiry to the information privacy order process.

4.1.3 Decision Tree

A decision tree algorithm works by repeatedly splitting a dataset into smaller subsets based on different criteria, visualized as a branching method where each internal node represents a test on an attribute, each branch represents the outcome of the test, and each leaf node represents a class label or a final decision. This structure makes decision trees intuitive and easy to interpret, resembling human decision-making processes [14]. The tree is constructed by selecting the attributes that most effectively classify the dataset, often using information gain or Gini impurity measures. The C4.5 algorithms are widely used decision tree learning techniques developed by Ross Quinlan. It serves as an improvement over its predecessor, the ID3 algorithm. C4.5 constructs DT using the information entropy concept from a training data set.

To counter DDoS attacks [34], a DDoS detection system was implemented using the DT (C4. 5) algorithms. B bugs and security flaws lay in undiscovered new ground and the old rule-set to throw the attackers off. These are destructive and can have an adverse effect on cloud performance, most especially the DDoS attacks. Classification trees are used to distinguish between the sources of threats. C4. 5 performed a computation to get the smallest decision tree in shape. The C4. An ordering criteria may be generated from the five-generated decision tree. As stated in the research outcomes, C4. The method of clustering that is found most efficient here is 5. However, a good result was obtained in the proposed detection system for the identification of DDoS attacks, as the accuracy level was estimated to be 98%. The C4. 5 applies to discrete and continuous data, making its result more accurate compared to other detection algorithms thanks to appropriate handling of the missing data issue.

In proactively developing an environment for cloud computing that is sacrosafe and free from risks, Said et al. [36] scrutinized and discussed techniques that could render threats to the system negligible. The primary objective was to attain a defensive state for distributed computing by debating and attaining moderation on security concerns in relation to distributed computing. As a result of the study, it was concluded that an uncomplicated decision tree with a Chaid algorithm security rating of the ordering method is an effective way for the leader to assess the cloudiness of the environment and guarantee the correct level of support as needed. They used the NB, MLP, SVM, C4 classifiers, and PART algorithms for data protection. Several risks are inevitable with distributed computing that might put important services and data at risk. The study revealed that a rather unsophisticated decision tree model known as the Chaid algorithm security rating is potentially accurate for the grouping technique content; it allows the chief to evaluate the extent of cloud-making and the kinds of support offered. The effectiveness level of any kind of motion may be neatly contained in the pre-specified classes of the ML processes. NB, multi-layer perceptron ANN, SVM, C4. 5, and partial least squares (PART) are among the ML techniques that Mishra et al. [37] employed. The use of these algorithms was helpful is mitigating possible security concerns.

Hussien and Sulaiman [38] explore the pre-fetching strategies with the Web that are incorporated with ML as a solution in a mobile computing environment through DT and NB algorithms. Internet traffic management delay can be reduced by using the following enhancements: pre-fetching data. As for information management, this report introduced this creative approach to using mobile cloud computing circumstances to overcome such issues as inactivity. Due to the storage of related but irrelevant item information before the carrying capability of an update is available and due to the large capacity restriction of a handheld device, carrying out the pre-bringing technique leads to way too much additional work and the slowing of the framework's speed. This is because, as the reader should know, a mobile device will not have that much storage space to begin with. For instance, Arjunan and Modi [44] propose an advanced security model for intrusion detection in cloud computing. Among the ML algorithms applied by the authors, we can point out that DT, RF, and NB are used for signature analysis and anomaly detection to define the intrusions that have taken place. They applied ML algorithms to make their suggested method, known as their 'method,' more effective.

4.1.4 Support Vector Machine

Support Vector Machine (SVM) is a learning algorithm that is used for classification and prediction [35]. As a rule, SVM creates a guide, which is an ordered representation of data, where the distance between two categories is as

far as possible [45], [48]. Fig. 6 shows the application of the SVM algorithm for DDoS detection in the SDN of a cloud computing environment.

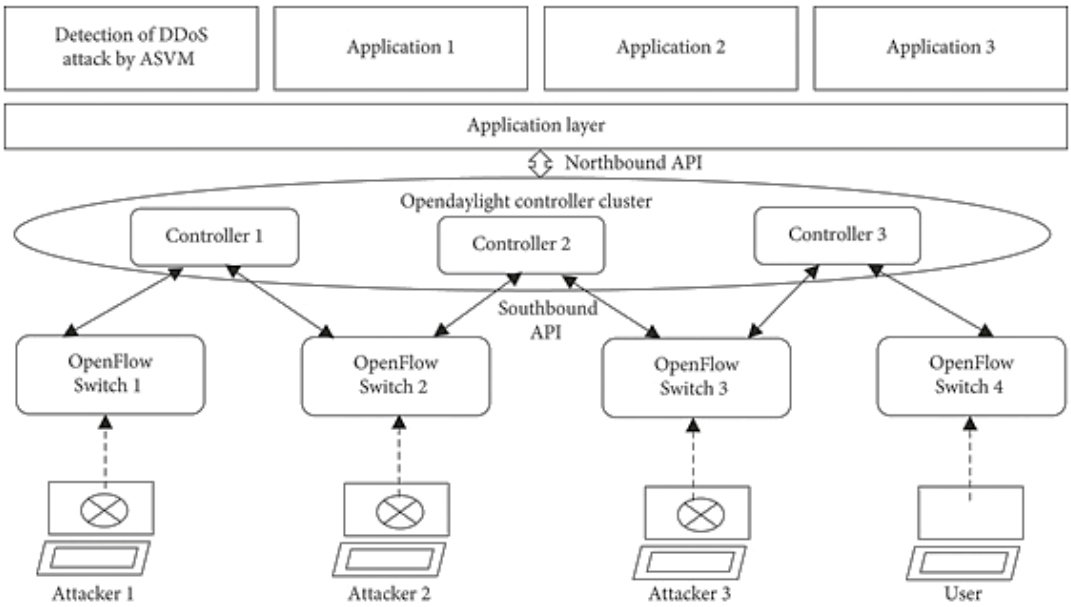

Fig. 6 *An SVM model for DDoS detection in SDN [48]*

The study by Khalaf et al. [14] contributes to DDoS attack identification with the help of ML algorithms in a cloud computing environment. The final decision regarding the learning methodology of the work was made using a statistical ranking procedure. They use NB, MLP, SVM, and C4. 5 decision tree, Partial Tree algorithm to protect data. Many threats could potentially harm the feasibility of the services and data that are underpinned by distributed computing. The results confirm the validity of the decision tree with no intricate features. The algorithms determine security ratings for the grouping technique, which is a reliable method for the head to evaluate the degree of cloud assurance and the nature of the support options.

In their study, Hou et al. [46] explained how applying ML to identify the network security of edge computing platforms is possible. DDoS attacks are considered advanced attacks, which are hardly detectable on this particular web site. They employed a simulation of smart home architecture that the Alibaba ECS has as part of its tools for their assessment. An edge computing innovation was used in the equipment architect's design, which we shall be developing later in this paper. The whole technique serves as a reasonable classifier to arrive at the boundary between regular and transformation codes. It could be used in the decomposition of the system change code. The aim was to separate the dataset into positive and negative types by a vector, and the study confirms that the RBF-based SVM technique is effective in completing this task. The use of ML algorithms has enhanced the security of IoT systems.

4.2 Deep Learning Detection Methods

DL algorithms have a big role in defending against DDoS attacks in cloud computing and network intrusion. The most common and effective DL algorithms have been illustrated in this section.

4.2.1 Deep Neural Networks

Deep Neural Networks (DNNs) include multiple hidden layers and are able to spot the complex and nonlinear relationships hidden in data sets. For DDoS detection, DNNs process network traffic data from the backbone and learn to distinguish between normal patterns of activity in the networks and abnormal patterns typical of DDoS attacks [49]. Here, large quantities of network data must be processed to detect aberrations that indicate an impending attack. These include packet sizes and intervals and the direction and volume of network flow. Deep networks allow for the extraction of high-level features from raw input data, an absolute necessity in DDoS attacks due to their subtleties and developments. The fact that DNNs can constantly be trained by new data also makes them agile at keeping up with the changing character of cybersecurity threats [50]. When implementing DNNs, organizations can strengthen their defenses against DDoS attacks by fully using the model's ability to detect

attacks quickly and accurately, as shown in Fig 7. As a result, networks are more secure and resilient than ever before.

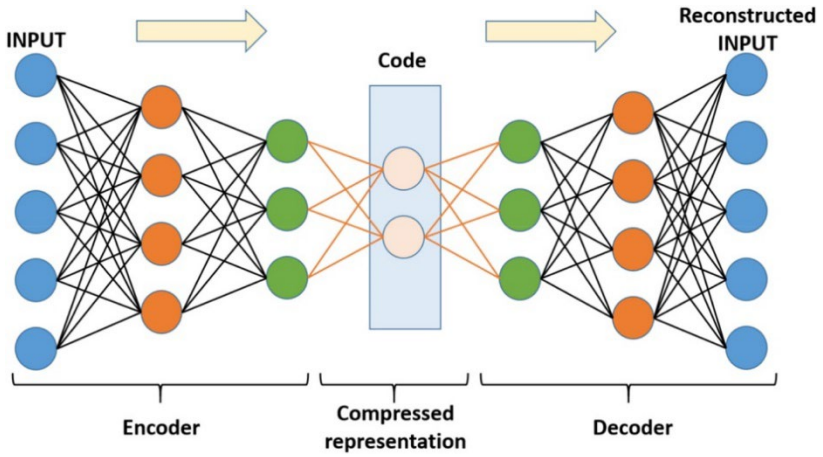

Fig. 7 *A DNN architecture for DDoS detection [51]*

Sabeel et al. [52] introduced the DNN model for the prediction of unseen DoS/DDoS attacks. In this study, the authors used only one dataset: CICIDS. Although the authors cleaned the samples and labeled them before using them to train their models, they also tested and improved their models using the synthetic ANTS2019 dataset. In section two, the authors integrate the synthesized dataset with the CICIDS2017 dataset. Once the models are retrained, the performance of identifying novel, never seen before attacks at the time they are synthesized is evaluated. The performances of both DNN and LSTM were seen to improve in the second half of the trial, with DNN attaining 98 percent accuracy. 72% percent and LSTM of 96. 15%. Values of 0. 987 and 0. 989 by the DNN and LSTM in the AUC test were used to estimate the performance. The ANTS2019 is another simulation model that represents the domain and variety of real-world cyber assaults. Although we are done classifying the two classes, we have not implemented the real-time detection setup.

As for private clouds, such important services as hosting have reference to the fact that DDoS attacks are the only circumstances under which services have to be of lower quality. Virupakshar et al. [53] are focused on bandwidth and connection flooding DDoS attacks in OpenStack-based cloud DDoS attack detection using DT, KNN, NB, and DNN algorithms. The authors have also explored several classifiers and used the best accuracy and precision. DNN is the preferred model out of the available models because of the high accuracy emanating from the use of a dataset generated on the fly. The authors have chosen a rather old set of data (KDDCUP99) and offer very limited information on LAN and cloud-based components of their dataset. For the KDDCUP99 dataset, the DNN algorithm has the lowest accuracy value compared to other methods.

Asad et al. [54] first introduced what is known as the DNN architecture, also referred to as DeepDetect. This one is designed as a feed-forward backpropagation. Preventing DDoS attacks at the application layer is the main focus of this paper's proposed paradigm. To validate the proposed method against DDoS attacks, the CICIDS2017 dataset was employed for evaluation. In this study, a comparison has been made between RF and DeepGFL. DeepDetect gave the F1-score number of 0, though the increased neuron density of the ConvNet-50 of the authors is from 0. 99 percent as compared to the other form of examination, which is 64 percent, making the former superior. The 'Pseudo R squared' known as the AUC is close to 1, thus showing the high relevance of the proposed model. This article explains how researchers distinguished between the data classes to develop a cloud-based service to shield the application layer against DDoS assaults. So far, this method has only been employed to test Application layer DDoS attacks.

4.2.2 Convolutional Neural Network

The use of Convolutional Neural Networks (CNNs) for DDoS attack detection is a novel approach in the area of network security. Here, CNNs, noted especially for their success in image processing applications, are used to analyze network traffic patterns [13]. In this case, the network traffic data is turned into a format that serves as input to CNN and tends to look like image or time-series data. The CNN's convolutional layers extract spatial and temporal features from this data, as shown in Fig. 8. Typically, a DDoS attack (unlike normal network traffic) has abnormal patterns in the time-series data. This ability is important for distinguishing between real, high-traffic scenarios and malicious DDoS attacks. Using CNN's capability of learning complex patterns and its own built-in feature extraction capabilities, this method could combine high accuracy with good efficiency in detecting DDoS

attacks. It may be a tool for future cybersecurity against today's increasingly advanced threats [17], [18]. Fortunately, using CNNs in this field is just another example of how adaptable neural network models are to different kinds of data beyond traditional image applications. CNN is one of the most successful DL algorithms, according to CNN.

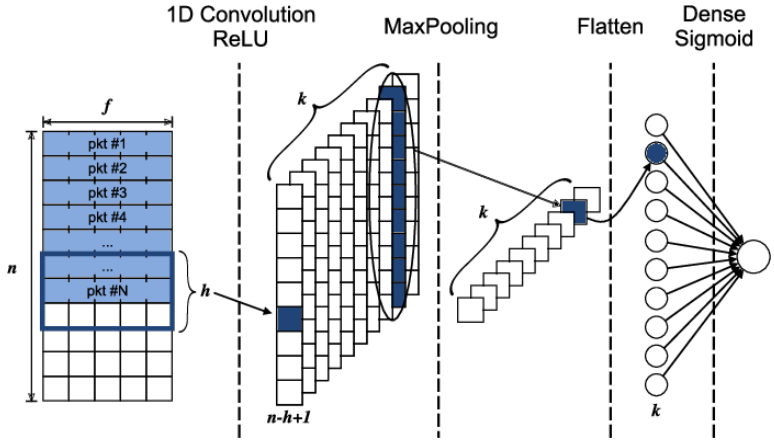

Fig. 8 *A CNN architecture for DDoS detection [55]*

In [20], the authors posit that due to the small sample size of the datasets, traditional ML algorithms like NB, KNN, and SVM do not produce the required results. Hence, the authors propose the deep CNN model. The performances for the proposed framework were compared with three ML methods for a dataset with fewer features. The proposed model was trained and assessed against 11 criteria types and was fairly successful in this multiclass categorization. Nevertheless, some kinds of traffic are not presented in the test data for the proposed model. CNN has been used to detect DoS attacks [22]. They benchmark the CNN model on two datasets of the simulated network traffic against conventional classification algorithms like SVM, KNN, and ANN. Among the five classification methodologies tested, the CNN model is statistically higher than all the other methods in accuracy, resulting in 99% for both datasets. In this case, one-column padding is used to achieve the data's matrix representation. This may affect the model in terms of learning capability in a particular training session or through a specific task.

The authors in [26] propose a method for identifying DoS attacks via Vector Convolutional Deep Feature Learning (VCDeepFL). VCDeep, FL blends Vector with CNN (VCNN). The suggested process is split into two parts: As for training and testing, Khosla et a. pursue a similar strategy to Weiss et a. In the first training phase, the VCNN, also known as unsupervised learning, is used, while in the second phase CNN, which is the supervised learning. Testing is also carried out in VCDeepFL based on the obtained weights. In order to assess the effectiveness of the proposed method, it was tested on the NSL KDD dataset and compared to both conventional classifiers (MLP and SVM) and modern attack detection systems. As can be seen from the results, the improved method provides higher accuracy than baseline classifiers and the currently used benchmark for attack detection in terms of false alarm rate and detection rate. The authors used an old database and have not presented any studies to determine unknown attacks.

Regarding DDoS attack detection, Sabeel et al. [52] proposed a system known as DAD-MCNN, which is a multichannel Convolutional Neural Network. The more channels used, the more feature groups are used. The authors separate the features into distinct tiers: the packet, host, and traffic levels. In this experiment, the authors used incremental training to train their MC-CNN model. The authors have carried out a number of tests and comparisons with two datasets: KDDCUP99 with the binary category and CICIDS2017 datasets with the multiclass category in KDDCUP99. The use of MC-CNN also revealed a better performance than the state-of-the-art methods for both binary and multiclass classification. As is with the experimental results of DDoS detection systems where training data is scarce, the results indicated that MC-CNN stands out as the best solution. The findings of multichannel and single-channel models are not as far from each other as is thought. In addition, there is an issue to do with the efficiency of the multichannel models when put into practice.

4.2.3 Long Short-Term Memory

Long Short-Term Memory (LSTM) networks are a special recurrent neural network (RNN) type tailored to cope with long-term dependencies in sequential data [56]. The LSTM was initially developed in 1997 to solve the vanishing gradient problem that makes standard RNNs unable to learn from data where the important information is frequently far separated by seemingly unrelated data (e.g., handwritten characters). The core of

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 29-51

LSTM is its cell state, which stretches down the entire chain. There are only modest linear interactions. Information moves unimpeded along this design. LSTMs also have a sophisticated gating mechanism composed of three gates: the input gate controls how much of an activation flows into a memory cell; the forget gate controls whether some value dies out or remains in the cell to be active for another time step, and the output gate determines just how actively a value in the cell participates in generating network outputs [57], [58]. Because these gates allow the LSTM both to retain and discard information from the cell state and have high overall effectiveness across about a dozen sequential data tasks, they are often used for and very suitable indeed [59], [60]. Fig. 9 shows an LSTM architecture for DDoS detection.

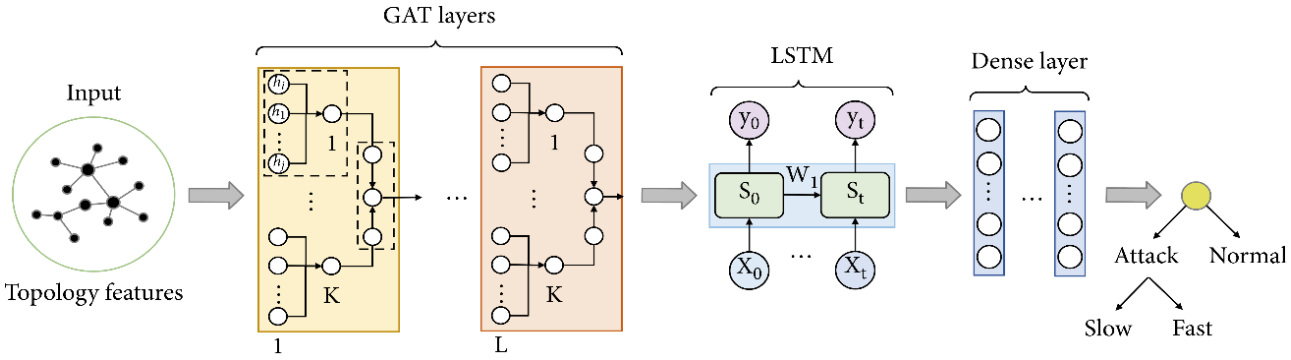

Fig. 9 *An LSTM architecture for DDoS detection [59]*

Li and Lu have used DL to detect DDoS in an SDN [56]. The model contains a hidden layer, input layer, reverse recursive layer through FC, forward recursive layer with FC, and output layer. While also encompassing RNNs and LSTMs, the model also integrates CNNs. To that end, the authors developed not one but four models, all of which could be called LSTM, CNN/LSTM, GRU, and 3LSTM. Applying the DDoS attack to the ISCX dataset gives a precision of 98%. The DDoS attack detection and defense system is built on the Ubuntu 14.04 operating system, and real-time DDoS attacks are employed to evaluate performance. But the Ping of Death assault, ARP flood inundation, SYN flood inundation, and UDP flood inundation are the only real-time distributed denial of service attacks till now. More real-time DDoS attacks are possible; there are many choices:

To mitigate DDoS assaults in a fog network, authors in [57] proposed a DL-based model. A variant of LSTM has been used to detect network- and transport-level DDoS attacks. The parameters for the LSTM model were constructed based on two different kinds of input data sets. Applying the DL model to the CTU13 Botnet, the authors made the following conclusions demonstrated in the first case discussed here. The second case is also a confrontation of the DL model at work on a subset of the Hogzilla dataset and some real-time DDoS attacks. The authors also compared the model to other methods. LSTM has been established to work with an accuracy of 98 percent for the identified medical devices. The efficiency of the proposed STTM is considered high for the compilation success rate, having been tested at 88% for all the test cases. Since SDN utilizes an OpenFlow switch, the DDoS defender module may block the malicious packet from reaching the cloud server.

Subrmanian et al. [61] suggest a four-layer structure with two layers of the LSTM algorithm: The dropout layer and FC layers are part of this controller, which are explained below in detail. Unlike other methods, network traffic behavior is learned from a small collection of packets without having to make features manually. In this study, we perform three experiments on the CICIDS 2017 Wednesday and Friday datasets using three different approaches, namely discrete time, ANN, and SVM. The outcomes reveal that the proposed LSTM-based model outperforms the competitors' models in terms of accuracy by 99.19% on this dataset.

4.2.4 Gated Recurrent Unit

The Gated Recurrent Unit (GRU) is a type of RNN architecture used in DL, particularly effective in processing data sequences for tasks like language modeling, machine translation, and speech recognition [62]. Developed as a variation of the more complex LSTM units, GRUs aim to solve the vanishing gradient problem that traditional RNNs face, which makes them ineffective at learning dependencies from long input sequences [63]. Fig. 10 shows the GRU architecture for DDoS detection.

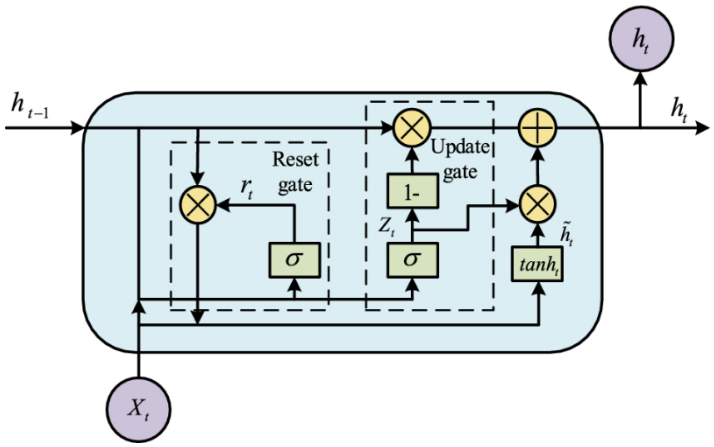

Fig. 10 *A GRU architecture for DDoS detection [64]*

In the Assis et al. [62] study, the authors proposed a defense mechanism for the interruption and intrusion threats in the context of an SDN. The suggested system has two main parts: the first part, the detection part, and the second part, the mitigation part. There is a detection module that will detect an attack in the event that there is one. To detect DDoS and intrusion attacks, the makers of this module employ a DL-based GRU technique for analyzing the individual IP traffic data. The mitigation module will start immediately, trying to stop an attack once it has been detected. On two datasets, CICDDoS 2019 and CICIDS 2018, the authors tested their proposed model against seven ML methods. Listed in the following are various approaches of ML: CNN, DNN, LSTM, K-NN, and SVM. The authors used two datasets, CICDDoS 2019 and CICIDS2018, as test cases. It has been analyzed how accurate, precise, and relevant the metrics of the proposed model consisting of the classifier based on ACM F, along with the usefulness of the strategies adopted in the context of separating normal and attack flows from those that have been identified when comparing with other existing ML techniques. The GRU proved capable of identifying DDoS and incursion attacks without exception. Further, a feasibility test is conducted to quantify the number of typical flows per second that can be scrutinized and categorized by the detecting techniques. It employs real IP traffic data of The State University of Londrina collected during the time of the experiment. Accordingly, GRU appears to be a viable strategy. The technique, as mentioned above, fetches average values of 99.94% and 97. The accuracy, recall, precision, and f-measure results were 09% on the CICDDoS2019 and CICIDS2018 datasets. Some offline data sets have been analyzed, and the detection or training time for publication is not calculated.

4.3 Reinforcement Learning Detection Methods

In terms of IDS, software agents are particularly important. They are software agents that monitor the network traffic and system activities for any signs of criminal activity or policy violations [2]. They work by processing large quantities of data, spotting trends, and getting alerts from predefined rules or learned behavior [22]. Under IDS, these agents may also be distributed within the network at critical points to intercept the flow of traffic, or they can be installed on individual machines to monitor system activities. Because of their flexibility and adaptability, software agents are especially well-suited to rapidly changing cybersecurity environments [7]. They can be trained to learn new, more complex kinds of cyber threats and unknown attacks. This ability makes the IDS system tougher and better equipped for attack. Fig. 11 shows a MAS architecture for DDoS detection.

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 29-51

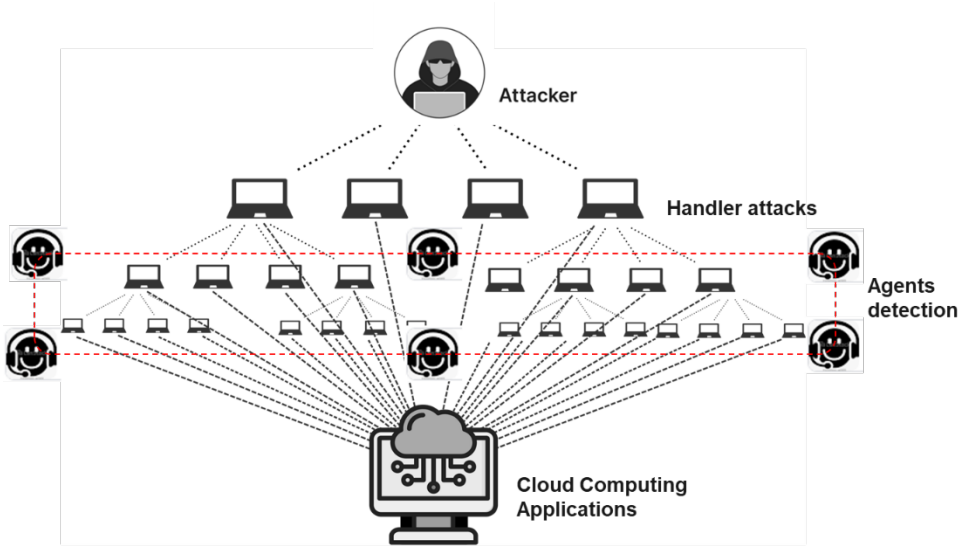

Fig. 11 *A MAS architecture for DDoS detection*

Systems running on several software agents as a MAS who work together and exchange information to complete a single task: in this case, the identification and halting of DDoS attacks [14], [15]. However, single-agent systems, whether the agent is human or machine, could be completely swamped by a DDoS attack (in which the attack involves overwhelming a network with traffic from many sources). However, in the context of a larger MAS, each agent can be specialized to monitor different parts of a network or certain types of traffic or behavior. This specialization makes for a more complete and less crude approach to detection [24], [25]. In addition, only through communicating and working together can these agents reconstruct a fuller picture of an ongoing attack, adapt more quickly to changes in the attack pattern, and react more powerfully. These collective intelligence and adaptability are what make multi-agent systems so especially suited to dealing with the rapidly changing, ever more sophisticated DDoS attacks [26].

5. Advanced Detection Methods

The study presents a detailed and thorough overview of numerous techniques for detecting and mitigating DDoS attacks employing functional DL, ML, and SA techniques in cloud computing environments. This review summarizes 66 research articles, including several review articles. In the review, the strategies of defense in the identification, reduction, or prevention of DDoS attacks are discussed. Depending on the used algorithms, it classifies methods for DDoS detection. The classification of many types of flood attacks involving DDoS assault and defense strategies keeps stressing a tangible approach and the tables of relations. Also, the commonly used testing databases and evaluation strategies are provided in this work.

5.1 Learning-based Detection Methods

Computing IoT services requires cloud Internet of Things (CIoT), which are frequently the targets of security breaches and other cyber threats. These systems pose significant challenges when attackers exploit their vulnerabilities. As a result, CIoT must implement IDPSs. However, today's IDS systems have flaws: they cannot recognize new types of attacks and suffer from single points of failure.

Using a learning-based model, Javadpour et al. [2] present a new distributed multi-agent IDS to resolve shortcomings in existing models. The model works through a six-step process in which learning agents determine whether network behavior is normal or compromised. KDD Cup 99 and NSL-KDD datasets are used to evaluate the model. Compared to existing ML methods, the model shows an average improvement of 16.81 % in recall, 16.05 % in accuracy, and 18.23 % in f-scores on average.

Janakiraman et al. [9] present a network-level mitigation model to solve the problem of DDoS attacks based on RL and LSTM. This scheme is performed in cloud computing environments and relies on SDN technology, among other methods. A defense mechanism is introduced and incorporated within the SDN controller. This model is designed to recognize the anomalous nature of DDoS attacks at the transport or network layer simulated by the intrusion detection evaluation dataset (ISCXIDS2012). The model can successfully separate legitimate packets from infected ones, filtering and forwarding them while dealing with threats presented by dangerous attack data through "high-tech" network traffic analysis. Through this model, the aim is to increase cloud-computing services' resistance to disruptive DDoS attacks.

Kesavamoorthy et al. [15] emphasize the role of cloud computing in our daily lives, in which millions of users store and work with data in the cloud daily. The DDoS attack represents one of the biggest obstacles to cloud resources and services for all this extensive use. The authors introduce a novel approach to automatically detect and attack distributed DDoS attacks using an autonomous MAS. Detection of DDoS attacks is achieved through several agents. These agents use particle swarm optimization (PSO) to improve the accuracy of communication and decision-making. A central agent continuously updates and coordinates the MAS. The coordinator agent uses entropy and covariance methods to analyze the current state and detect DDoS attacks. Also, a monitoring agent passively observes cloud resources and networks; in case of any abnormal activity, it will send out detection and recovery agents. Testing this system reveals improved performance, but the performance accuracy decreases with the increase in the number of attack nodes.

Chemchem et al. [16] suggest an ML and DL classification through the SA reasoning. They propose ML and data mining methods (DM), including DL, ML, and SA algorithms. It presents an idea concerning meta-knowledge extraction and incorporates it into an agent architecture to enhance inference efficiency. One approach is to extend MLDM methods for induction rule mining and compare their performance. The study focuses on enhancing the decision-making ability of agents by selecting operable rule classes and demonstrates results through experimentation with different datasets, looking at metrics such as accuracy and execution time. The results show that integrating the proposed method into the cognitive agent architecture enhances decision-making, particularly in environments with large and complex datasets.

In pursuit of greater network security (especially intrusion detection), Louati and Ktata [17] describe the DL-based MAS model to improve detection abilities and efficiency. The model employs DL autoencoders to reduce features and MLP along with the K-NN algorithms for classification. The model is meant to overcome the limitations of the IDS, including vulnerability to single points of failure and inefficiency in handling distributed attacks like DDoS. The evaluation was performed based on the KDD CUP99 dataset. These results showed that the proposed model improved detection accuracy and reduced detection time over traditional methods. Combining DL with MAS is thus an effective approach to intrusion detection.

Soltani et al. [18] propose an architecture combining MAS with DL to detect network intrusion effectively. The DL includes CNN and LSTM to identify attack patterns and the MAS to accommodate changing network behaviors. The architecture is trained and tested on CIC-IDS2017 and CSE-CIC-IDS2018 datasets. The test evaluates the effectiveness of detecting various types of network attacks, including DDoS. In terms of successful adaptation to concept drift in traffic, the CNN models have high detection rates, and LSTM successfully labels the sequence packets for early intrusion detection. These results show that the architecture is robust in a distributed, dynamic security environment.

Subrmanian et al. [61] focus on DDoS attacks where multiple systems attack in a concerted fashion to block the legitimate use of a service, which can impact many OSI model layers. In application, network, and transport layers, the focus is on using LSTM and GRU DL models to detect and identify DDoS attacks. The study tests these models against the CICDDoS2019 dataset, which includes DDoS attacks at these layers. LSTM and GRU models were employed for testing, and they achieved an average accuracy of 99.4 % and 92.5 %, respectively, in which the LSTM had a particularly high accuracy.

Pankajashan et al. [66] focus on the application of ML and DL techniques to improve the efficiency of anomaly detection, especially in different kinds of data generated by IoT devices and cloud computing networks. In particular, they attempt a number of ML methods, such as SVM and Isolation Forest classifiers (IFC). It presents a combination of Deep Auto-Encoder (DA) and LSTM to formulate a DA-LSTM model for preprocessing and anomaly detection. The DA-LSTM model is an advanced version of LSTM with a DNN model, which turns unstructured log data into features used for training and classifying anomalies. The performance of the model is evaluated using CIDDS benchmark datasets. The results indicate that the DA-LSTM model outperforms other ML methods. It achieves about 99.1 % accuracy in detecting anomalies on the CIDDS dataset, which is far superior to the 81 % and 79 % attained by IFC and SVM classifiers.

This review seeks to expand the scope of interest and guide the future direction of DDoS research. It also presents some conclusions pointing to specific unresolved issues of the research and several suggestions for further investigation. That being said, the current study is unique to the previous study in that it has considered the limitations of the most recent related review articles, as has been stated. Contemporary approaches in network protection and intrusion detection methodologies, such as Javadpour et al. [2] and Kesavamoorthy et al. [15], have incorporated various studies. Javadpour et al. [2] paid much attention to improving the ability to detect cyber threats with ML to analyze the traffic in networks and give specific recommendations on improving the efficiency of protection of cloud computing systems. Their study focuses on the use of AI in enhancing the IDS to enhance both the effectiveness and efficiency of the systems. Likewise, Kesavamoorthy et al. [15] used hybrid DL with normal modes. They investigated the necessity for more solid and versatile ways of solving difficulties that exist in the constantly evolving domain of cyber threats. As can be observed from this study, interdisciplinary is an essential factor in developing network security technologies. Table 1 shows the comparison results of our study with the most related work.

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 29-51

Table 1 *Comparison between different flood attack detection methods*

Reference	Flood Attack		Defense Method	Dataset	Research Outcome	Issue Addressed
Year	Low Rate	High Rate				
Javadpour et al. [2] 2023	-	✓	MAS	KDD CUP99, NSL-KDD	Developed advanced ML algorithms to enhance the detection of cyber threats in cloud computing environments.	Focused on optimizing security protocols and improving the accuracy and efficiency of IDS in cloud networks.
Janakiraman et al. [9] 2023	✓	✓	LSTM, RL	ISCXIDS2012	Investigated ML strategies for enhancing network security, highlighting real-time detection capabilities.	Emphasized the importance of timely threat detection in reducing network vulnerabilities.
Kesavamoorthy et al. [15] 2019	✓	-	MAS, PSO	Simulation tools	Proposed a hybrid approach combining DL with traditional methods to detect anomalies in network systems.	Addressed the challenge of adapting to evolving cyber threats with robust and scalable solutions.
Chemchem et al. [16] 2018	✓	✓	DT, RF, SVM, k-NN, NB, ANN, CNN, MAS	Data SMS, San Francisco Crime Classification, News Aggregator, Amazon Fine Food Reviews	Explored vulnerabilities in network protocols and proposed enhancements to prevent exploitation by attackers.	Highlighted weaknesses in existing network security frameworks and the need for stronger protection mechanisms against data breaches.
Louati and Ktata [17] 2020	✓	✓	Autoencoders, MLP, K-NN, MAS	KDD CUP99, NSL-KDD	Developed a real-time detection method for DDoS attacks using network traffic analytics.	Tackled the difficulty of detecting and responding to DDoS attacks promptly and effectively.
Soltani et al. [18] 2023	-	✓	CNN, LSTM, MAS	CIC-IDS2017, CSE-CIC-IDS2018	Implemented AI-driven models for proactive threat detection, emphasizing adaptive learning techniques.	Focused on preemptively identifying and counteracting network threats to enhance system resilience.
Subrmanian et al. [61] 2022	✓	✓	LSTM, GRU	CICDDoD2019	Advanced the use of ML for comprehensive threat identification, integrating predictive analytics into security frameworks.	Addressed the need for predictive security measures to keep up with new attack vectors.
Pankajashan et al. [66] 2022	✓	✓	LSTM, DNN, DA, IFC, SVM	CIDDS	Focused on the application of AI to improve the adaptability and precision of IDS.	Dealt with the challenge of ensuring that IDS remains effective against a constantly changing threat landscape.

Moreover, Chemchem et al. [16] and Louati and Ktata [17]' work is helpful to explain the DDoS attacks and the measures to counter them. Chemchem et al. [16] have identified weaknesses in the presently used protocols of the networks and suggested modifications to curtail them as exploitable by attackers. Their work focuses on the need to improve secure security structures in order to safeguard such information. At the same time, Louati & Ktata [17] have also come up with a more efficient approach to detecting DDoS attacks in real-time using network traffic analysis, reflecting the use of real-time data processing in intrusion detection. In addition to this, Soltani et al. [18], Subrmanian et al. [61], Janakiraman et al. [9], and Pankajashan et al. [66] provide emphasis using ML- and AI-driven models for the prediction and counteraction of the network threats; these works explain the future of preventive security models that adapts to the new threats. These papers signal the continual shift in the approaches to cybersecurity, especially stressing the fact that there should always be proactive measures when it comes to protecting networks.

The synthesis of the selected references has shown major contributions and approaches to the study of network security, emphasizing threat identification and prevention with the application of ML and AI. Javadpour et al. [2] and Kesavamoorthy et al. [15] agree with the proposition that AI is essential in improving the effectiveness and flexibility of IDSs because of their function in responding to the ever-changing nature of cyber threats. Similar to Chemchem et al. [16] and Louati and Ktata [17], other studies within the network protocols reveal the weak points of networks and post new methods for the real-time detection of DDoS attacks while identifying the need for effective frameworks to counter large scale network attacks. Soltani et al. [18], Subrmanian et al. [61], Janakiraman et al. [9], and Pankajashan et al. [66] are the works that are also aligned with this research agenda by proposing the use of ML models to identify threats before their occurrence, which aligns well with the described emphasis on the predictive security. Altogether, these papers describe a new paradigm in the further development of cybersecurity, based not only on the expanded use of AI and ML for the detection of cyber threats but also on the ability of these systems to actively respond in the fight against threats that threaten the stability and security of network infrastructures.

5.2 Evaluation Datasets

In the context of cybersecurity, different datasets were used to improve the detection and prevention methods of DDoS attacks. It also enables the improvement of ML models, aiding in the creation of strongly built IDS that are very useful for researchers. IS CX 2012 Dataset, UNSW NB 15 Dataset, CIC IDS 2017 Dataset, CSE-CIC-IDS2018 Dataset, CIC DDOS 2019 Dataset, and CIDDS Dataset are some of the significant datasets. Each of these datasets possesses its own qualities; for example, application areas of the datasets, number of classes and features, and extensive descriptions that help in understanding characteristics of network attacks are provided. These datasets are used as fundamental resources in building new models to mitigate the effects of DDoS attacks and other unlawful conducts on networks. Table 2 gives a detailed description of the flood attack datasets.

Table 2 *The flood attack datasets*

Dataset Name	Application Area	Classes and Features	Description and Link
ISCX2012	IDS	- 2 - 20	- Contains labeled data for various attack types, including DDoS, facilitating the evaluation of network IDS. - https://www.unb.ca/cic/datasets/ids.html
UNSWNB15	Network and system security	- 10 - 49	- It provides a comprehensive set of network traffic with normal and malicious activities, including DDoS attacks, and is used for training and testing intrusion detection models. - https://research.unsw.edu.au/projects/unsw-nb15-dataset
CICIDS2017	IDS	- 15 - 80	- Includes a variety of up-to-date attack scenarios, covering different aspects of network security and allowing for comprehensive IDS evaluation. - https://www.unb.ca/cic/datasets/ids-2017.html
CSE-CIC-IDS2018	Cybersecurity analytics	- Multiple - Varies	- Encompasses datasets focusing on cybersecurity analytics, aiding in the development of security models and detection systems. - https://www.unb.ca/cic/datasets/ids-2018.html

CICDDoS 2019	DDoS attack detection	- Multiple - 80	- Focuses specifically on DDoS attack types across different layers, providing detailed information for DDoS detection and prevention systems. - https://www.unb.ca/cic/datasets/ddos-2019.html
CIDDS	Anomaly and intrusion detection	- 2 - 15	- It aims to detect anomalies and intrusions, including DDoS attacks, focusing on providing realistic network traffic for testing IDS models. - https://www.hs-coburg.de/forschung/forschungsprojekte-oeffentlich/informationstechnologie/cidds-coburg-intrusion-detection-data-sets.html

All the presented datasets are crucial for carrying on with the establishments in the research and development field of network security, specifically in addressing the issue of DDoS attacks. Two datasets differ from one another in features and scenarios, and they provide an opportunity for the researchers to test and improve their IDS. When using all of these datasets, the researchers can be in a position to create models that are more realistic and sensitive to any threats in the real network. These datasets are diverse and wide-ranging and are instrumental in improving the efficiency of cybersecurity and supporting the constant enhancement campaigns of cyberspace protection against topical cyber threats.

Even though all the mentioned datasets can enhance the research in the field of network security, quite specifically, the CICDDoS 2019 Dataset and CICIDS2017 Dataset are oriented to simulate DDoS or flood attacks in cloud computing environment as these datasets are dedicated to the DDoS scenes and are rich in data. UNSWNB15 Dataset can also be used for other attacks, including DDoS, as explained by the large number of attack types and their features. The established datasets of this study will provide a stable ground for formulating effective and efficient DDoS detection and prevention mechanisms, especially for cloud networks.

5.3 Analysis and Discussion

Different algorithms based on ML, DL, and RL are used as decision-making methods for cloud computing security. However, these methods face some common difficulties, such as the emergence of new forms and more advanced techniques for attack, an increase in the volume and scale of DDoS attacks, detection latency of an attack, or merely shutting out legitimate traffic. This change in attack patterns also happens dynamically. Because of this, SA, ML, and DL methods are unable to identify new vectors of attack with both speed and accuracy [15], [19], [22], [24]. But these could lead to false positives, marking harmless traffic as dangerous, or false negatives, derecognizing real attacks [35], [36]. This problem can cause missed attacks or wasted resources. While DL and LSTMs have shown promise in detecting DDoS attacks, they have certain drawbacks and issues. The following are some issues related to deploying ML, DL, and RL in DDoS detection.

- Cloud computing network traffic data need to be transformed into a format suitable for ML or DL analysis, which can be complex and might lead to the loss of important information.
- If training data is not comprehensive, reflects the variety and complexity of DDoS attacks, or the existence of biased or skewed data can result in more false positives (identifying legitimate traffic as malicious) or false negatives (failing to detect actual attacks), seriously affecting the quality and reliability of ML and DL detection.
- ML or DL might not effectively capture the dynamic temporal patterns in network traffic. This issue is crucial for identifying sophisticated or unseen DDoS attacks, as they typically learn from extensive historical and labeled data. ML and DL can still struggle with learning long-term dependencies, which might be necessary to detect subtle and slowly emerging DDoS patterns.
- Training DL, especially deep ones, can be computationally expensive and time-consuming, requiring significant hardware resources and leading to latency in detection, which might only be feasible in some operational environments. Moreover, the DL's large number of parameters can hinder training and fine-tuning in rapidly evolving attack scenarios.
- Due to ML and DL complexity, they are prone to overfitting, especially when trained on limited or non-diverse data sets, leading to poor generalization to new types of DDoS attacks.
- The performance of ML and DL is susceptible to the choice of hyperparameters, and finding the optimal configuration can be challenging and time-consuming.
- Although the LSTM has shown good performance in detecting DDoS attacks, due to their recurrent nature, LSTMs require significant memory and processing power, which can be a limitation in resource-constrained environments.

- Detecting intrusions like DDoS attacks largely depends on the cooperation and communication among various agents. This inter-agent coordination can be complex, and sophisticated algorithms are needed to ensure efficient data sharing and decision-making. Lack of coordination can cause delayed or inaccurate responses to DDoS attacks. Also, the complexity of these systems increases the probability of getting false positives and negative detection results.
- Another issue when using SA and MAS for DDoS detection is that they may require a great deal of processing power and memory, which can be expensive. As network traffic volume and the number of SA monitoring and data analyses increase, so does complexity. Because DDoS attacks often involve a large amount of traffic, agents must process and analyze this data in real time, which stretches resource inclusion.

6. Conclusion

This study identified security threats and attacks as the most pressing concerns in cloud computing. DT, NB, ANNs, SVM, and K-NN were investigated to analyze the security concerns in the cloud computing environment. Moreover, the best-known DL approaches, including DNN, CNN, LSTM, and GRU, have been introduced. Also, the study includes the Sophisticated types of flooding attacks using SA, MAS, and RL. In addition, the study focused on analyzing and assessing the provided techniques, pointing out their strengths and weaknesses. Furthermore, the study helps enhance complex and effective defense mechanisms against DDoS attacks. Besides, constant revision and enhancements are necessary to categorize the linked DDoS attack aspects to mitigate newer, more sophisticated threats. At the same time, several areas of research have been defined and discussed further. This review has carefully analyzed the security challenges in cloud computing, focusing on the disruptive nature of flooding attacks like DDoS. These attacks are extremely challenging due to their massive size and nature, and decent defensive measures are required to deal with them. In this paper, we will describe and discuss different learning-based defense methods based on recent developments in artificial intelligence to have a better and more accurate approach to threat detection. However, the strength of these proposed methods is still shadowed by considerable drawbacks, such as high false positive rates and severe demands for resources. The review further points out the need to keep actively updating the defense mechanisms, calling for combining models encompassing different aggressive stance methods to reduce errors and increase effectiveness. Therefore, the growth of more flexible and economically effective cloud solutions will play a significant role in creating reliable defense in the future against intensified acts of cyber warfare.

Acknowledgment

The authors would like to thank the Shatt Al-Arab University College, and University of Monastir, for supporting this work.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***review:*** *Nafea A. Majeed Alhammadi, Mohamed Mabrouk;* ***review analysis:*** *Nafea A. Majeed Alhammadi, Mounir Zrigui;* ***draft manuscript preparation:*** *Nafea A. Majeed Alhammadi, Mohamed Mabrouk. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction, 122, 103441.

[2] Javadpour, A., Pinto, P., Ja'fari, F., & Zhang, W. (2023). DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Cluster Computing, 26(1), 367-384.

[3] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.

[4] Kassimi, D., Kazar, O., Barka, E., Merizig, A., Houhamdi, Z., Athamena, B., & Zaoui, M. (2022, December). A New Approach Based on a Multi–Agent System for IDS in Cloud Computing. In 2022 Ninth International Conference on Software Defined Systems (SDS) (pp. 1-8). IEEE.

[5] Dalal, S., Manoharan, P., Lilhore, U. K., Seth, B., Mohammed alsekait, D., Simaiya, S., ... & Raahemifar, K. (2023). Extremely boosted neural network for more accurate multi-stage Cyberattack prediction in cloud computing environment. Journal of Cloud Computing, 12(1), 14.

[6] Tariq, M. I. (2019). Agent-based information security framework for hybrid cloud computing. KSII Transactions on Internet & Information Systems, 13(1).
[7] Jaber, A. N., & Rehman, S. U. (2020). FCM–SVM based intrusion detection system for cloud computing environment. Cluster Computing, 23, 3221-3231.
[8] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
[9] Janakiraman, S., & Deva Priya, M. (2023). A Deep Reinforcement Learning-based DDoS Attack Mitigation Scheme for Securing Big Data in Fog-Assisted Cloud Environment. Wireless Personal Communications, 130(4), 2869-2886.
[10] Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. IEEE access, 9, 22351-22370.
[11] Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 105, 102260.
[12] Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. Soft computing, 27(18), 13039-13075.
[13] Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., & González, J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems, 111, 763-779.
[14] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713.
[15] Kesavamoorthy, R., & Ruba Soundar, K. (2019). Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system. Cluster Computing, 22(Suppl 4), 9469-9476.
[16] Chemchem, A., Alin, F., & Krajecki, M. (2018). Deep Learning and Data Mining Classification Through the Intelligent Agent Reasoning. International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2018, Barcelone, Spain.
[17] Louati, F., & Ktata, F. B. (2020). A deep learning-based multi-agent system for intrusion detection. SN Applied Sciences, 2(4), 675.
[18] Soltani, M., Khajavi, K., Siavoshani, M. J., & Jahangir, A. H. (2023). A Multi-Agent Adaptive Deep Learning Framework for Online Intrusion Detection. arXiv preprint arXiv:2303.02622.
[19] Alhammadi N. A. M., Zaboon, K. H., & Abdullah, A. A. (2021). A review of the common DDoS attack: types and protection approaches based on artificial intelligence. Review Article, 7(1), 08-8.
[20] Alashhab, Z. R., Anbar, M., Singh, M. M., Hasbullah, I. H., Jain, P., & Al-Amiedy, T. A. (2022). Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy. Applied Sciences, 12(23), 12441.
[21] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580.
[22] Aziz, I. T., Abdulqadder, I. H., & Jawad, T. A. (2022). Distributed Denial of Service Attacks on Cloud Computing EnvironmentCih .an University-Erbil Scientific Journal, 6(1), 47-52.
[23] Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. International Journal of Information Management Data Insights, 2(2), 100134.
[24] Soe, Y. N., Santosa, P. I., & Hartanto, R. (2019, October). DDoS attack detection based on simple ANN with smote for IoT environment. In 2019 fourth international conference on informatics and computing (ICIC) (pp. 1-5). IEEE.
[25] Guha, S., Yau, S. S., & Buduru, A. B. (2016, August). Attack detection in cloud infrastructures using artificial neural network with genetic feature selection. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 414-419). IEEE.
[26] El-Boghdadi, H., & Rabie, A. (2019). Resource scheduling for offline cloud computing using deep reinforcement learning. Int. J. Comput. Sci. Netw, 19, 342-356.
[27] Nawrocki, P., Sniezynski, B., & Slojewski, H. (2019). Adaptable mobile cloud computing environment with code transfer based on machine learning. Pervasive and Mobile Computing, 57, 49-63.
[28] Khan, A. N., Fan, M. Y., Malik, A., & Memon, R. A. (2019, January). Learning from privacy preserved encrypted data on cloud through supervised and unsupervised machine learning. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-5). IEEE.
[29] Shamshirb and, S., & Chronopoulos, A. T. (2019, June). A new malware detection system using a high performance-ELM method. In Proceedings of the 23rd international database applications & engineering symposium (pp. 1-10).

[30] Park, J., & Lee, D. H. (2018). Privacy preserving k-nearest neighbor for medical diagnosis in e-health cloud. Journal of healthcare engineering, 2018.
[31] Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018, April). Cyberattack detection in mobile cloud computing: A deep learning approach. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE.
[32] Saljoughi, A. S., Mehrvarz, M., & Mirvaziri, H. (2017). Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms. Emerging Science Journal, 1(4), 179-191.
[33] Mohsin, M. A., & Hamad, A. H. (2022). Performance evaluation of SDN DDoS attack detection and mitigation based random forest and K-nearest neighbors machine learning algorithms. *Revue d'Intelligence Artificielle*, *36*(2), 233.
[34] Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A., & Kumar, C. V. (2022). DDoS detection using machine learning techniques. Journal of IoT in Social, Mobile, Analytics, and Cloud, 4(1), 24-32.
[35] Babatunde, O. S., Ahmad, A. R., & Mostafa, S. A. (2020). A smart network intrusion detection system based on network data analyzer and support vector machine. International Journal of Emerging Trends in Engineering Research, 8(1), 213-220.
[36] Said, H. M., El Emary, I., Alyoubi, B. A., & Alyoubi, A. A. (2016). Application of intelligent data mining approach in securing the cloud computing. International Journal of Advanced Computer Science and Applications, 7(9).
[37] Mishra, A., Gupta, N., & Gupta, B. B. (2020). Security threats and recent countermeasures in cloud computing. In Modern principles, practices, and algorithms for cloud security (pp. 145-161). IGI Global.
[38] Hussien, N., & Sulaiman, S. (2017). Web pre-fetching schemes using machine learning for mobile cloud computing. Int. J. Adv. Soft Comput. Appl, 9, 154-187.
[39] Bamasag, O., Alsaeedi, A., Munshi, A., Alghazzawi, D., Alshehri, S., & Jamjoom, A. (2022). Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing. PeerJ Computer Science, 7, e814.
[40] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., Mahmoud, M. A., Al-Rimy, B. A. S., ... & Marks, A. (2021). An adaptive protection of flooding attacks model for complex network environments. *Security and Communication Networks*, *2021*(1), 5542919.
[41] ur Rasool, R., Wang, H., Ashraf, U., Ahmed, K., Anwar, Z., & Rafique, W. (2020). A survey of link flooding attacks in software defined network ecosystems. Journal of Network and Computer Applications, 172, 102803.
[42] Radain, D., Almalki, S., Alsaadi, H., & Salama, S. (2021, March). A review on defense mechanisms against distributed denial of service (DDoS) attacks on cloud computing. In 2021 International Conference of Women in Data Science at Taif University (WiDSTaif) (pp. 1-6). IEEE.
[43] Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Dinesh Kumar, A. (2020). A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. In Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019 (pp. 252-270). Springer International Publishing.
[44] Arjunan, K., & Modi, C. N. (2017, January). An enhanced intrusion detection framework for securing network layer of cloud computing. In 2017 ISEA Asia Security and Privacy (ISEASP) (pp. 1-10). IEEE.
[45] Grusho, A. A., Zabezhailo, M. I., Zatsarinnyi, A. A., & Piskovskii, V. O. (2017). On some artificial intelligence methods and technologies for cloud-computing protection. Automatic Documentation and Mathematical Linguistics, 51, 62-74.
[46] Hou, S., & Huang, X. (2019, March). Use of machine learning in detecting network security of edge computing system. In 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA) (pp. 252-256). IEEE.
[47] Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019, February). Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In 2019 Amity International conference on artificial intelligence (AICAI) (pp. 870-875). IEEE.
[48] Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T., & Vasupongayya, S. (2019). Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). Journal of Computer Networks and Communications, 2019.
[49] Kong, B., Yang, K., Sun, D., Li, M., & Shi, Z. (2017). Distinguishing Flooding Distributed Denial of Service from Flash Crowds Using Four Data Mining Approaches. Computer Science and Information Systems journal, 14 (3), pp. 839-856.
[50] Yuan, X., Li, C., & Li, X. (2017, May). DeepDefense: identifying DDoS attack via deep learning. In 2017 IEEE international conference on smart computing (SMARTCOMP) (pp. 1-8). IEEE.
[51] Setitra, M. A., Fan, M., & Bensalem, Z. E. A. (2023). An efficient approach to detect distributed denial of service attacks for software defined Internet of things combining autoencoder and extreme gradient boosting with feature selection and hyperparameter tuning optimization. Transactions on Emerging Telecommunications Technologies, 34(9), e4827.
[52] Sabeel, U., Heydari, S. S., Mohanka, H., Bendhaou, Y., Elgazzar, K., & El-Khatib, K. (2019, December). Evaluation of deep learning in detecting unknown network attacks. In 2019 International Conference on Smart Applications, Communications and Networking (SmartNets) (pp. 1-6). IEEE.

[53] Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. G. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Computer Science, 167, 2297-2307.
[54] Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). Deepdetect: detection of distributed denial of service attacks using deep learning. The Computer Journal, 63(7), 983-994.
[55] Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J., & Siracusa, D. (2020). LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), 876-889.
[56] Li, Y., & Lu, Y. (2019, September). LSTM-BA: DDoS detection approach combining LSTM and Bayes. In 2019 seventh international conference on advanced cloud and big data (CBD) (pp. 180-185). IEEE.
[57] Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. Computers & Security, 118, 102725.
[58] Bashaiwth, A., Binsalleeh, H., & AsSadhan, B. (2023). An explanation of the LSTM model used for DDoS attacks classification. Applied Sciences, 13(15), 8820.
[59] Guo, W., Qiu, H., Liu, Z., Zhu, J., & Wang, Q. (2022). GLD-Net: Deep Learning to Detect DDoS Attack via Topological and Traffic Feature Fusion. Computational Intelligence and Neuroscience, 2022.
[60] Gupta, N., Jindal, V., & Bedi, P. (2021). LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. Computer Networks, 192, 108076.
[61] Subrmanian, M., Shanmugavadivel, K., Nandhini, P. S., & Sowmya, R. (2022, September). Evaluating the Performance of LSTM and GRU in Detection of Distributed Denial of Service Attacks Using CICDDoS2019 Dataset. In Proceedings of 7th International Conference on Harmony Search, Soft Computing and Applications: ICHSA 2022 (pp. 395-406). Singapore: Springer Nature Singapore.
[62] Assis, M. V., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). A GRU deep learning system against attacks in software defined networks. Journal of Network and Computer Applications, 177, 102942.
[63] Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019, October). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.
[64] Liu, X., & Liu, J. (2021). Malicious traffic detection combined deep neural network with hierarchical attention mechanism. Scientific Reports, 11(1), 12363.
[65] Ring, M., Wunderlich, S., Gruedl, D., Landes, D., Hotho, A.: "Flow-based benchmark data sets for intrusion detection." In: Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), pp. 361-369. ACPI (2017)
[66] Pankajashan, S., Maragatham, G., & Kirthiga Devi, T. (2022). Hybrid approach with Deep Auto-Encoder and optimized LSTM based Deep Learning approach to detect anomaly in cloud logs. Journal of Intelligent & Fuzzy Systems, 42(6), 6257-6271.