Recent Trends on Sophisticated types of Flooding Attacks and Detection Methods based on Multi Sensors Fusion Data for Cloud Computing Systems

Nafea A. Majeed Alhammadi[1,2*], Mohamed Mabrouk[2], Mounir Zrigui[2]

[1]Research Laboratory in Algebra, Numbers Theory and Intelligent Systems RLANTIS, University of Monastir, Monastir, Tunisia

[2]Department of Computer Sciences, Shatt Al-Arab University College, Basrah, Iraq

Emails: nafeaalhamadi@yahoo.com ; mab.mohamed@gmail.com ; mounirzrigur3030@gmail.com

Abstract

Data storage, software services, infrastructure services, and platform services are only some of the benefits of today's widespread use of cloud computing. Since most cloud services run via the internet, they are vulnerable to a comprehensive range of attacks that might end it the disclosure of sensitive information. The distributed denial-of-service (DDoS) is amongst the attacks that pose an active threat to the cloud environment and disrupts the provided services for the legitimate participants. The main aim of this review paper is to present the recent trends on sophisticated flooding attacks detection methods for cloud computing systems. The review only considers the papers published within the period of 2014 until 2022.This study aims to examine the various deep learning-based DDoS detection algorithms and machine learning used across different cloud environments. Also, the study covers the Sophisticated types of Flooding Attacks and the testing dataset. The review outcomes several research challenges, gaps and future research guidelines related to protection of DDoS attack in cloud computing environment.

Keywords: Flooding Attacks; Detection Methods; Machine Learning; Deep learning; Multi Sensors Fusion Data; Cloud Computing Systems.

1. Introduction

The management, processing, access, and storage of information and other data within a specific server is known as cloud computing [1]. Infrastructure and services are made available "on-need" through the use of cloud computing. More specifically, network-enabled, scalable, assured Quality of Service (QoS), low-cost computing infrastructure, and simple accessibility are all included in cloud computing. Moreover, the industrial cloud computing is becoming increasingly popular as more and more consumers move their data and applications to a remote cloud. Consumers get more flexible access to the data and applications [2]. Although cloud computing has many advantages, it is still in early stages and faces numerous hurdles in terms of integrity, security, availability, cost, and performance. The biggest challenge in cloud computing is security because many people find it intimidating to use someone else's hard drive to store or operate software [3].

A model for providing on-demand computing resources with the least amount of work and maintenance is called cloud computing [2]. It involves the internet-based sharing of computer resources. Software, a developer interface, virtual hardware, or storage are all examples of these shared resources. A potential paradigm known as "cloud computing" uses the internet to provide software, platforms, and infrastructure as a service that is entirely virtual and does not depend on

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

local computers or memory requirements. Many businesses have concentrated on improving their ability to operate with their current software without stressing extra infrastructures. In addition to the widely acknowledged offerings and advantages, cloud computing may also provide risks and obstacles [4]. Denial of service assaults and their distributed counterpart, DDoS attacks, are regarded as the most dangerous malicious actions among all cloud security challenges. Through the depletion of their cloud resources and services, these attacks are a simple attempt to render the service inaccessible to actual customers [3].

Security experts have been making great efforts to report this problem for a while, but the frequency and impact of these attacks have increased despite their efforts. As a result, it is urgently necessary to incorporate the concepts of adaptation and self-organization into the design of effective cloud security measures. DDoS attacks, however, can be launched from a variety of contexts, including a specific service, cluster, node, virtual machine or the entire cloud environment. When an attacker uses numerous zombie machines that are already under their control to transmit a large number of false packets from one direction to a server, DDoS happens [5]. DDoS attacks have grown to be a significant issue, and attackers are now focusing on victims in sophisticated ways.

Nevertheless, Infrastructure as a whole has become a frequent target for attacks due to the widespread usage of virtualization technology. In particular, privilege escalation and Denial of Service (DoS) attacks [6]. The dilemma of availability in cloud security is seriously threatened by DoS attacks. DoS attacks have a higher potential in cloud computing than they do in single tenanted architecture because millions of users share their infrastructure. There are two ways that DoS attacks can be deployed across the Internet. The first strategy entails the attacker delivering the victim malicious packets in an effort to confuse any program or protocol that is using it (i.e., a vulnerability attack) [7]. Whereas, the second case can be done at the level of transport and application layer. The attacker attempts to consume the network resource and prevent the legitimate user to access to the network [8]. Moreover, the architecture of DDoS on a cloud server was displayed in bellow Figure 1.

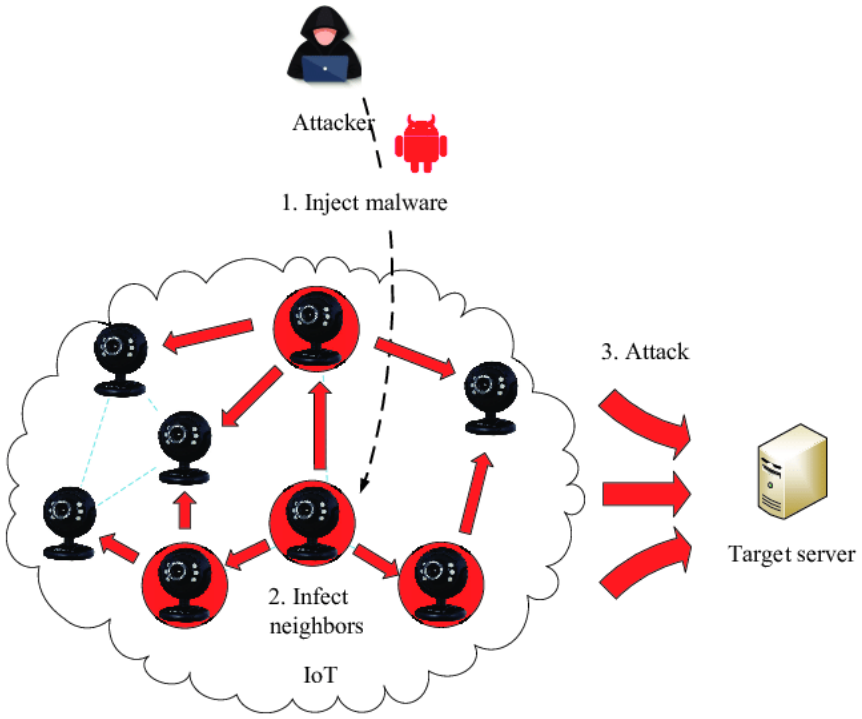

Figure 1: The architecture of DDoS attack on cloud server [8].

Meanwhile, the current cloud security infrastructure is facing increasingly complex problems. The significant technical challenges include managing hundreds or thousands of security rules and identify suspicious tools independently in a corporation with many privacy and security plans, which can lead to poor administration. Despite these obstacles, the current cloud privacy and security society is advocating for and moving toward incredible keys that are powered by self-regulating bio mechanisms that are inherent to the natural world.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

The increased usage of cloud computing by companies also presents greater potential for hackers to gain unauthorized access to virtual worlds. A revolutionary virtualization security solution has therefore been created by developers to enable an abstraction layer that mimics a device and counteract the threats. In the form of Virtual Machines (VMs), virtualization can also make it easier for multiple guests utilizing various platforms to share resources [9].

This study is segmented into eight sections; section 1 give an overview of the study. Section 2 presents the review methodology. Whereas, cloud computing background is illustrated in section 4. The most efficient detection methods of DDoS attack target cloud computing were discussed in detail under section 5. Furthermore, the recent flooding attack dataset have been highlighted under section 6. Section 7 discus the overview of study and presents the Research direction. Section 8 conclude the study.

2. Review Methodology

This review paper attempts to present the recent trends on sophisticated flooding attacks detection methods for cloud computing systems. The review covers the period of 9 years from 2014 until the end of 2022. The used keywords for the search are flood attack, DDoS attack, cloud computing and IDS, machine learning and deep learning. A total number of 29 research papers and 6 review papers are covered in this review study. Furthermore, Figure 2 displays the number of articles that were included in this review according to the year they were published, while the * indicates the total number of review articles that were included in this study within a particular year.

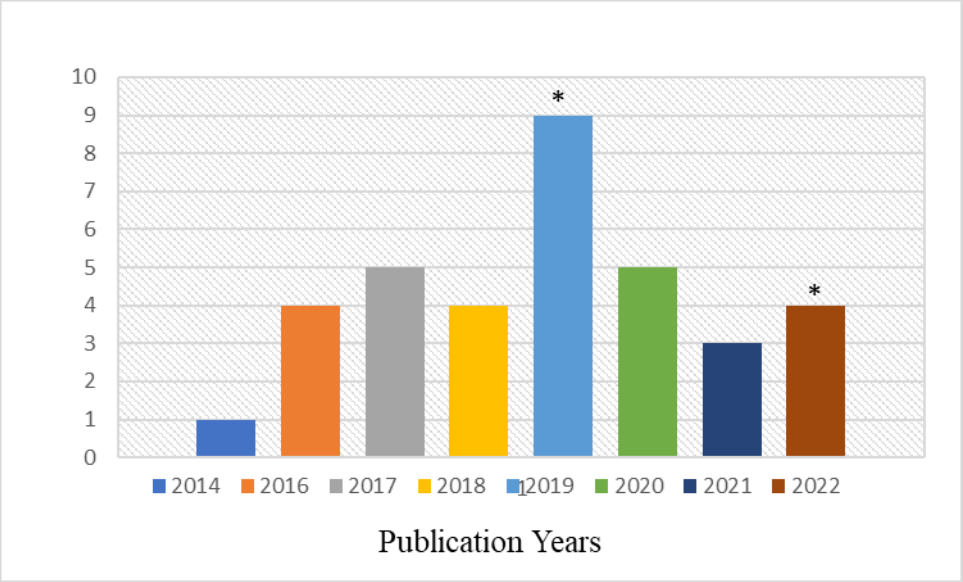

Figure 2: an overview of the reviewed papers

There are several review papers that have discuss the same topics presented in this paper. The existing reviews include the work of Parast et al., [1], Alashhab et al., [2] and Agrawal and Tapaswi, [3]. Also, the recent reviews include the work of; and Khalaf et al., [4], Aziz et al., [5]; and Lata and Singh, 2022 [6]. Nevertheless, the scope of this review is divided to four main points: the cloud computing domain, the attack approaches, the detection and defence methods and the testing and evaluation of these methods. This paper is directed to focus more on the existing various DDoS attacks and defence methods targeting cloud services. However, Figure 3 shows the main scope of this review.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

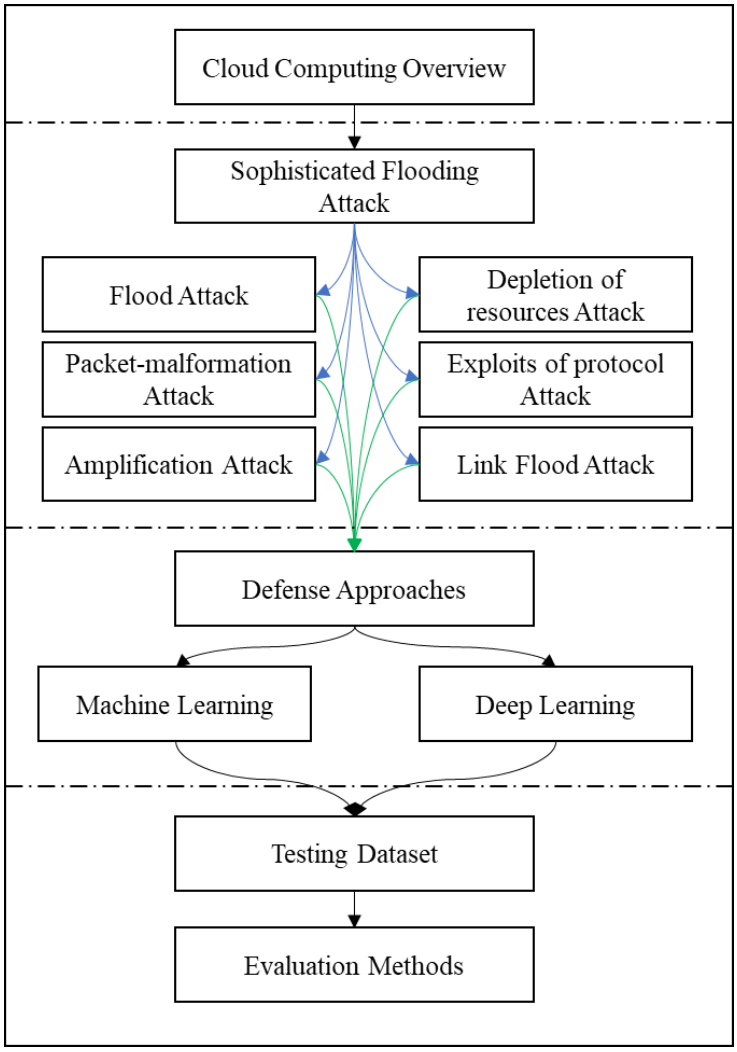

Figure 3: The main scope of this review

3. Cloud Computing

The future of technology lies in computing, which offers users a practical foundation for Internet-based access to cloud resources and services. By adopting this technology, desktop computing is evolving into utility computing [3]. The cloud uses a variety of delivery methods, including private, public, communal, and hybrid, to offer software, infrastructure and platform as a service. Over the last several years, many types of organisations, including schools, hospitals, and banks, have begun to use cloud computing, following in the footsteps of big cloud corporations like Microsoft, Google, IBM, and Amazon [1].

4. Cloud Threats and Attack Approaches

Cloud computing is applicable in many fields and it has many benefits, but it also has a number of security problems, risks, and obstacles. According to the surveys, cloud computing security is a significant research challenge [3]. A summary of various security issues with cloud service delivery is provided. The provision of on-demand services is the primary goal of cloud computing, making availability the most crucial issue among several security considerations [9]. The DDoS attack poses the gravest danger to the accessibility of resources and services related to cloud computing

4.1. Cloud Threats

Confidentiality, integrity, and availability are the three categories used to categories the main security risks in CC. Here, these concerns are briefly examined.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

- **Confidentiality** threats include the possibility of an internal attack, the chance of an external attack, and data problems. One of the primary concerns is the possibility of a cloud service provider's own employees gaining unauthorized or illegal access to its customers' sensitive data [11]. Second, the importance of the danger of an external attack on cloud services operating in an unsecured location is growing. Third, because of human error, a lack of tools, and protected access failures, information leakage is an indefinite danger to cloud-based data, after which anything is conceivable [15].
- **Integrity** problems with client access control, data quality problems, and data siloing are all potential dangers. Incorrectly combining the specifications of security parameters with subpar VM design and unstable client-side hypervisors poses the initial risk of information isolation. This is a complex problem within the cloud, which provides resources linking the clients; if resources change, it might impair the reliability of the information [9] [16]. The second is weak client access control, which has a number of problems and dangers due to ineffective access and character control, allowing attackers to damage information assets. However, in both confidentiality and integrity levels, it is observed that the good security system is based on the combination of Blockchain and cryptography algorithms [6].
- **Availability** the threats might include the impact of advancement across the board, accessibility issues with an organization, physical damage to assets, and ineffective recovery techniques. Firstly, the significance of advancement on the board, which includes the effect of foundation changes and the effect of client entrance testing for diverse customers. Equipment and application evolution in the cloud both have substantial effects on the availability of cloud-based organizations. There is also a problem with the availability of services, such as the inability to register a domain name via a DNS organization due to a lack of system data transmission capacity, assets, and software [16]. All cloud models are susceptible since it is an external risk [17]. The third is the organization's skill in managing service providers, cloud customers, and wide area networks (WANs) despite physical disruptions to the network. Inadequate failure recovery is an example of a poor recovery approach, which may have a significant impact on both the speed and success of a recovery.

4.2. Attack Types

Attacks on bandwidth and resource depletion are two risk factors for cloud computing systems. These kinds of assaults flood the victim's network with data including unwanted traffic in an effort to block genuine traffic from entering the victim's network, using up all of the victim's or targeted system's bandwidth in the process. These assaults are conducted utilizing recently developed algorithms or easily accessible software tools like Trinoo [4]. These attacks are divided into the aforementioned subcategories [10] [12]:

- **Flood-Attacks:** These kinds of attacks are carried out by an attacker who, with the assistance of zombies, sends a significant amount of data traffic to the network system of the victim. The victim's network bandwidth is impacted negatively as a result of this IP traffic data. The victim's computer system suffers a decrease in network capacity and speeds up significantly, which disrupts the flow of lawful traffic data that is essential for gaining access to network services. The attacks that are being carried out here make use of user datagram packets as well as data packets that are formatted according to the Internet control message protocol. Other examples include flood assaults on DNS, VoIP, and media-data. Flood attacks have also been used against DNS and VoIP. Another illustration of this is fragmentation.
- **The Packet-malformation attack:** The term malformed is referring to the packet that containing malignant data. The aggressor sends these malicious data to the victim using an IP address or IP packet with the express purpose of crashing or freezing it. In IP-address-based attacks, malicious data is encapsulated along identical source and destination IP addresses, wreaking havoc on the victim's operating system. As a result of this attack, the system becomes slow, resulting in system failure. The IP-packet options attack makes use of the fact that each IP packet has an additional optional field in order to transmit the attack's supplemental data. These extra-fields are utilised in order to construct malignant data. Assigning a value of one to each service bit in an IP packet's header effectively encloses the extra data. Therefore, the victim must devote additional effort to assembling these packets. These attacks are most susceptible to penetration when carried out on a large scale or by multiple zombies.
- **Amplification-attack:** The attacker's goal is to send several infected data frames to a specific network broadcast IP-address in order to create contagious data traffic. By doing this, the

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

systems that are being attacked will receive a feedback response from devices that are within the broadcast address's range. Attacks that concentrate on broadcast address services are susceptible to being carried out on a large number of typical networking devices. These devices include hubs, routers, switches, and others. This type of distributed denial of service attack is open to both the aggressor and the zombies as a potential target (compromised systems). Attacks of this type include the Smurf and Fraggle varieties; their common goal is to cause widespread disruption to a target's systems.

- **Depletion of resources attack:** Attacks of this sort are carried out in order to starve the victim's system of its available resources, making it impossible for it to handle legitimate requests from users.
- **Exploits of protocol attacks:** The primary goal of these attacks is to exhaust the victim's system's resources by exploiting vulnerabilities in the protocol stack, with tcp-syn attacks serving as a prototypical example of this kind of attack.The connection's hand-shake protocol is likewise vulnerable to this attack. Other forms of protocol vulnerabilities that may be used to get into a system include push + ack attacks, Common Gateway Interface request attacks, and authentication server attacks.
- **Link Flood Attack (LFA):** is among the deadliest attacks aimed at contemporary networks. These attacks have the potential to shut down the entire network by choking vital links as a result of a denial of service. Through the use of the crossfire LFA, low-rate genuine traffic is flooded around the destination to separate it, making harder to spot among them.

4.3. DDoS Attack

This type of attack is considering as a new version of DoS attacks but it is following a sophisticated methods in which a large amount of infected computers, sometimes known as bots, work together to bring down a single cloud server. According to Arbor Networks, the share of DDoS attacks aimed at cloud computing grows annually. In recent years, DDoS attacks have focused on major cloud-based organisations including RackSpace, Amazon EC2, Microsoft, and Sony [4]. As a result of the attacks, affected Cloud Service Providers experienced disruptions in service, financial losses, and a variety of other negative outcomes (CSPs). Multiple DDoS attack variants exist in a cloud environment, each with their own unique goal, method of execution, and impact [10]. The DDoS attack scenario in the cloud server is displayed in bellow Figure 4.

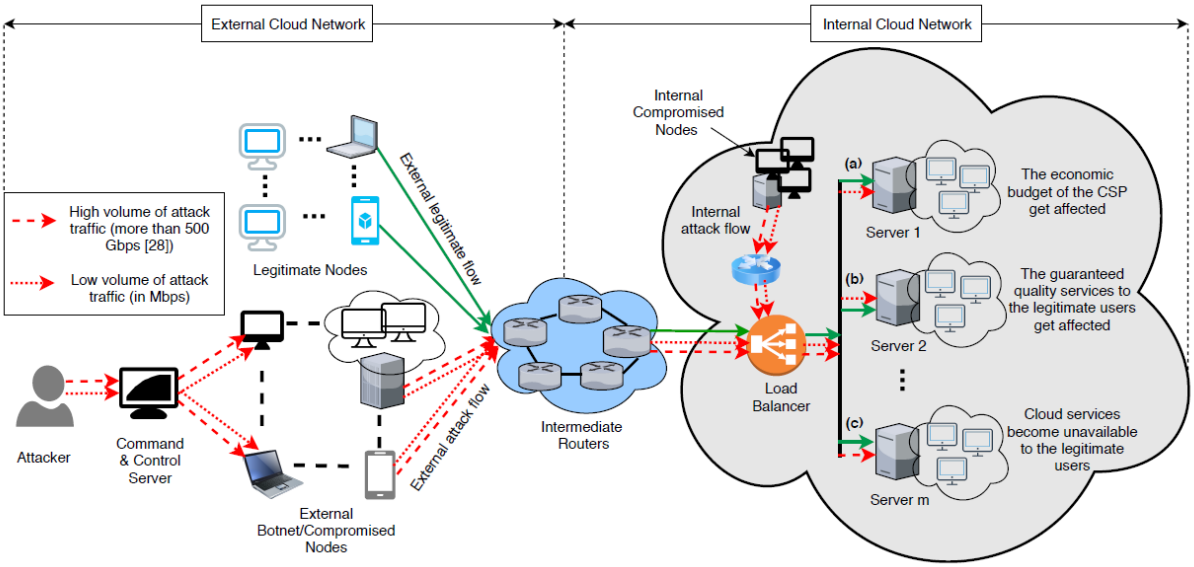

Figure 4: DDoS attacks in cloud computing [11]

Generally, brute-force and semantic DDoS attacks are the two most common types. The enormous volume of attack traffic makes it easy for defence systems to spot these kinds of attacks [11]. Semantic attacks target the protocols themselves rather than the underlying infrastructure, such as cloud computing resources network bandwidth. A tiny amount of malicious communication is generated by the attacker in order to compromise a single protocol or programme. These kinds of

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

attacks are referred to as distributed denial of service (DDoS) attacks. It's easy to mistake low-rate attack traffic for genuine traffic [18] [19].

5. Detection Methods

Several types of defines methods for securing cloud computing environment against flooding attacks have been proposed. Furthermore, according to the previous studies it observed that the most effective defence methods are based on Machine learning and Deep learning. Therefore, in this study, the most effective and efficient defence methods based on the ML and DL have been illustrated and discussed in detail, the highlighted algorithms were displayed in Figure 5.

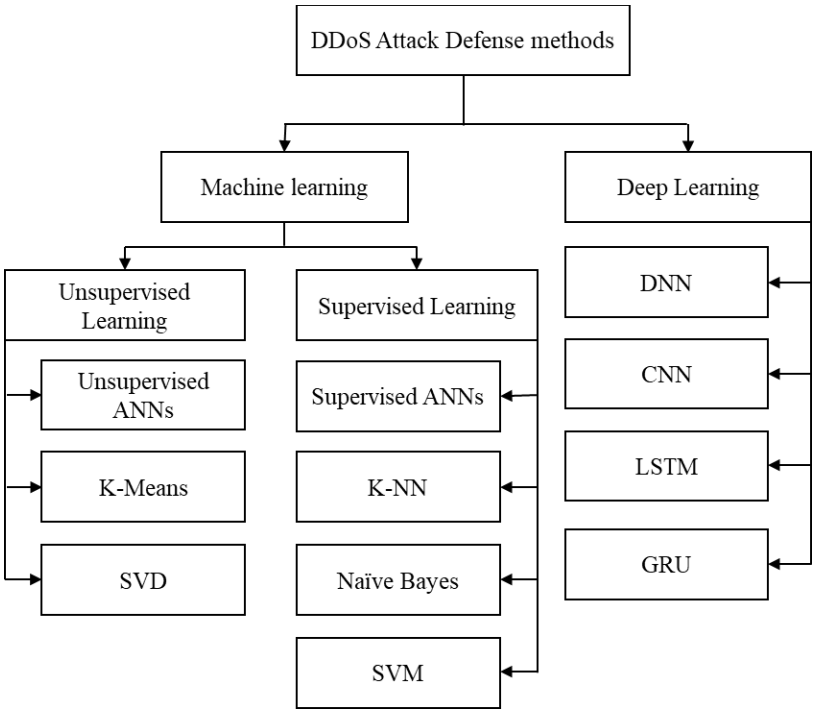

Figure 5: DDoS attack Défense Methods

5.1. Defence Methods based on Machine Learning

ML is the study of how computers accomplish a task by analysing the computations and measurable models they utilise without the need for explicit headers, contingent models, and acceptance. It's a kind of artificial intelligence logic [20]. The importance of ML in the cloud is such that it will soon be used by all clouds. Here, we will not be discussing how ML might improve the safety of distributed computing, but rather we will be talking about how to properly assign and concentrate on assets. As cloud storage has grown to accommodate more mundane data, it has also grown to accommodate more sensitive data, prompting the need for more security in CC. Methodologies for more precise risk detection in the cloud are described in [12]. First, we lay out a standard procedure for determining risks and threats by adding up individual degrees of danger. Then, we lay out the methods for dealing with threats that combine signature identification and anomaly detection into a combined model for threat detection.

5.1.1. Supervised Learning

In "supervised learning," a type of machine learning, a limit is learned that transforms commitments into yields based on model data yield sets. From information about several planning models, it infers a bound [14]. Algorithms in machine learning that need supervision are called "supervised machine learning".

- **Supervised Artificial Neural Networks**
  It is the building blocks of a computational framework designed to mimic the way the human brain processes information. These ML institutions are responsible for finding answers to problems that

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

would be too difficult for people to handle or too complex to be resolved using just statistical methods. The authors in [7] used Artificial Neural Networks (ANN) algorithms to foresee common vulnerabilities in distributed computing. Security flaws in a bank were identified with the aid of an ANN algorithm. Artificial neural networks were utilized to enhance cognitive abilities, including both execution and learning. The cloud security presentation prediction was made using Levenberg-Marquardt (LMBP) algorithms. Prediction accuracy is measured using mean square error (MSE), and a nonlinear improvement model called LMBP is utilized to evaluate the accuracy of the predictions and cut down on the difference between actual yields and focus over the whole presentation process. The cloud Delphi technique was utilized for less formal get-togethers and investigations. The information was gathered using the Delphi method, which is considered to be a reliable source. Foreseeing problems in distributed computing required a quantifiable information model, and this model was the ANN algorithm. Problems with cloud security were anticipated using the LMBP algorithm. However, the algorithms have the ability to secure the cloud computing with good results.

Because cloud designs are distributed and composite, it is challenging to identify advanced assaults in cloud systems. The fact that several different portable registering and storing devices are connected to cloud structures to support a client's admission adds to the already complex nature and complexity of detecting digital attacks. The threats of digital attacks in cloud environments, as described by Guha et al. [8], are crucial to address while designing defenses for cloud systems. The detection of cyberattacks in cloud infrastructures and distant computing nodes was also given a competent approach. The use of an ANN was linked to the suggested approach. The ANN was built using data from the cloud stops ' connecting nodes' traffic systems. The invention and adoption of an approach that uses a hereditary calculation to decrease the amount of structures mined from the system-traffic data was required due to the computationally costly nature of ANN. Methods for two large informative collections of system-traffic showcased this approach, displaying better results compared to existing procedures for detecting cyberattacks in the cloud. With this approach, the ANN is trained and tested using directed ML, which is prepared using informative collections of system-traffic that have been arranged in an orderly fashion. The names of the various types of attacks are included in the pre-planning data bank, so they may be easily recognized.

To solve the scheduling issue in the cloud, we adapted DeepRM and DeepRM2. One of the most difficult tasks in CC is resource scheduling, which entails dividing up available resources among various activities and processes in accordance with the Quality of Service (QoS) standards set by the various cloud applications. Existing strategies cannot be applied to resource allocation in the cloud because of its unpredictability and heterogeneity. El-Baghdadi et al. [9] used one of the ML emergent algorithms, deep RL (DRL), also known as DRL for Cloud Scheduling (DRLCS), to handle the problem of resource scheduling in CC. Using the same strategy as DeepRM and DeepRM2, cloud scheduling takes into account a number of factors, including CPU, memory, task deadline, and VM load balancing. On the other hand, DeepRM and DeepRM2 solely care about how much time and space they have to work with.

The authors of [10] created and implemented a standard version of the setup. The flexible MCC criteria for developing Internet apps has been reached thanks to cross-stage innovation. This innovation made it possible to construct hybrid apps with code migration to satisfy the significant rise in demand for various operating systems because the same code runs on a mobile device and in the cloud (like Android or Windows).

In [11], the authors explored supervised and unsupervised ML capabilities using ANNs on top of encrypted data from a homomorphically safe semantic cryptosystem. Despite improvements in data security, the insecurity of data held, managed, and shaped by an external party continues to discourage owners from taking an active role in its utilization. Owners of data stored in the cloud should use a reliable information governance system. One of the fundamental strategies in many disciplines is to coordinate examples.

The authors of [12] used ANN to try to identify cyberattacks in MCC. They showed that their architecture can increase attack detection accuracy by as much as 97.11%. An ANN was utilized to identify intrusions and attacks in Reference[28]. Both the NSL-KDD and the KDD-CUP datasets were used to evaluate the authors' model. They said that their suggested methodology might identify malicious actions performed by unauthorized individuals.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

- **K-Nearest Neighbors algorithm (K-NN)**

Among ML algorithms, K-NN is the most straightforward solution to regression and classification problems. K-Nearest Neighbors (K-NN) employs and describes novel data through similarity measurements (e.g., distance). A majority vote to its neighbours completes the classification [13].

Data protection in the cloud is still an open question. Cloud data security is being improved with the use of many frameworks, including encryption. Information security practices cannot be implemented. Understanding the importance of security needs is crucial for the appropriate implementation of these procedures Information privacy was the basis for the data categorization method provided by Zardari et al. [14]. Information security and protection are key to the information grouping process outlined by the authors. K-Nearest Neighbor (NN) data arrangement was carried out in cloud services and digital environments. The goal of using K-NN is to categories data according to its required level of safety. There were two categories created for the data: sensitive and open. Recognizable evidence of the information that is supposed to be guaranteed was aided by the information's order. In this case, just the sensitive and closed-information communities needed to be protected. Using a paradigm for decentralized computing, a suggested hierarchy of security and privacy-related data was developed. Data security requirements led to an analysis of the data layout. The K-NN classifier technique of ML is the commitment of this inquiry into the information privacy order process. More stringent encryption methods, such as the RSA algorithm, are needed to protect such sensitive and confidential data.

In the prior work of Shamshirband et al. [15], the study intends to use two malware datasets and a High-Performance Extreme Learning Machine (HP-ELM) to identify potential anomalies. The scale of a botnet directly correlates to the efficacy of a distributed denial of service attack. Additionally, botnets are utilized for massive-scale fraud and data theft. Managers of both systems and frameworks may benefit from the usage of an IDPS because of its ability to detect disruptions. When an interruption is detected by the IDPS, the authorized managers may get email warnings. The defensive capabilities of ML IDPS are improved. Artificial neural networks (ANNs) and ML genetic algorithms (GAs) are two exceptional ML approaches for cybersecurity. To make decisions about novel situations that the framework cannot predict, GA looks to previously solved problems for guidance. Hackers are becoming more and better at creating new AI-powered exploit devices. This lets them conceal their objectives while doing system tests and spreading malware.

In [16], the authors go into the topic of privacy protection in the context of online medical records. They presented a method that conceals data access patterns while protecting the confidentiality of medical datasets, symptoms, and diagnostic outcomes. To locate the k sets of information that are most comparable, they developed a unique privacy-preserving approach.

- **Naive Bayes**

Navies Bayes classifiers, a subset of "probabilistic classifiers," put Bayes' hypothesis into practice by making strong (naive) freedom assumptions in between the key points. These are the most basic of the Bayesian system models.

Using the C4.5 algorithm, Kour et al. [17] developed a DDoS detection system to protect against these attacks. Bugs and security flaws exist in the undiscovered developments and old norms, allowing for disruption by the attackers. Attacks, especially DDoS attacks, are very damaging and may negatively impact cloud performance. A distributed denial of service attack (DDoS) happens when an attacker gains access to a network of computers in order to launch an attack on that network. When infected with malware, computers and other machines (such Internet of Things devices) become bots (or zombie). A botnet is the resultant collection of infected computers, and the attacker can control it remotely. There are drawbacks to using conventional methods of intrusion detection, such as high rates of false alarms and the need to constantly update software to keep up with emerging threats. In contrast to conventional IDS, ML techniques are well-versed in drawing attention to the risks. A distributed denial of service attack is analyzed using specialized ML algorithms to determine the source of the danger.C4.5 ran a computation to find the minimal decision tree. The C4.5-generated decision tree may be utilized as the ordering criteria. According to findings, C4.5 is the most effective method for clustering. However, the proposed detection system achieved a good result in detecting DDoS attack with accuracy of 98%. The C4.5 algorithm works with both discrete and continuous data, and it yields a more precise result than competing detection methods by properly addressing the problem of missing data.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

As a first step in creating a secure and risk-free setting for CC, Hanna et al. [18] reviewed and examined methods for mitigating potential threats to the system. The major goal was to acquire a secure condition for distributed computing by discussing and achieving moderation for security issues associated with distributed computing [19]. Based on the findings, it was determined that a basic decision tree model employing a Chaid algorithm security rating for the ordering method is an efficient mechanism for the leader to gauge the cloudiness of the situation and ensure the appropriate levels of assistance are provided. For data protection, we employed the Naive Bayes, MLP, SVM, C4.5, and PART algorithms. There are dangers associated with distributed computing that might jeopardise services and data that rely on it. The results showed that a simple decision tree model (the Chaid algorithm security rating) for the grouping technique is a reliable method that gives the chief the ability to assess the level of cloud making and the sorts of support provided. Any kind of motion may be neatly categorized using ML processes' preset classes. The CI web allows access to ML methods. Naive Bayes, a multi-layer perceptron, support vector machine (SVM), decision tree (C4.5), and partial least squares (PART) are only some of the ML techniques that were used by the authors of [20]. The use of these algorithms helped address potential security issues.

The authors of [21] consider Web pre-fetching strategies that make use of ML algorithms in mobile computing to be a potential solution to the problem. The process of pre-fetching data is one of the enhancements that can be used to lessen the delay that is associated with managing Internet traffic. In the context of information management, the report presented this innovative strategy for making use of MCC conditions to address concerns regarding inactivity. Because of the pre-fetching of irrelevant item information storage and the capacity restriction of a mobile device, using the pre-bringing technique an excessive amount results in additional work and slows down the execution of the framework. This is due to the fact that a mobile device only has so much storage space available. The authors of [22] present a more robust security architecture for intrusion detection in CC. The authors used a hybrid approach that was based on signature analysis and anomaly detection in order to identify the intrusions that were made. They made their method, which they suggested, more effective by using the Navie Bayes algorithm as well as other algorithms.

- **The Support Vector Machine (SVM)**

SVM is a ML technique which employed for classification and prediction. The SVM is a supervised learning method for categorizing data into two groups. The guide that is produced by an SVM is a representation of the ordered data, with the boundaries between the two categories being as large as is practical [23].

In the prior work of Khalaf et al. [1] the research provided the effectiveness of machine learning algorithms used to attack identification in a cloud computing scenario. A statistical ranking procedure was used to make the final choice about the work's learning methodology. It was concluded from the results that a straightforward decision tree model Chaid algorithm security rating for ordering approach is a useful way for the leader to gauge the cloud's level of assurance regarding the kinds of support it offers.For data protection, we use the Naive Bayes, MLP, SVM, C4.5 decision tree, and Partial Tree algorithms [1]. Numerous threats exist that might significantly impact the viability of the services and data that are supported by distributed computing. The findings support the application of a straightforward decision tree model. The Chaid algorithm security rating for the grouping approach is a dependable method that provides the head with the ability to measure the extent of cloud guaranteeing and the different types of support that are available. For the purpose of classifying our data, we decided to use, from the machine learning (ML) methods that were available, the Naive Bayes algorithm, a multi-layer perceptron, a support vector machine (SVM), a decision tree (C4.5), and partial least squares (PART). These algorithms are helpful for addressing potential dangers and threats to security that may arise.

In order to address the issue, Hou et al. [24] described how to use ML to detect the network security of edge computing platforms. They used the Alibaba ECS's built simulation of a smart home architecture as part of their analysis. An edge computing innovation was used in the equipment architect's design. In order to determine the boundary between regular and transformation codes, the entire technique would structure a reasonable classifier. It could be utilised to determine the system change code. The objective involved dividing the dataset into positive and negative types using a vector, and the results show that the RBF-work SVM technique performs well in this task. This study has improved IoT frameworks' understanding of system security and broadened the applications of ML. DDoS attacks are regarded as sophisticated attacks, and it is now difficult to identify them.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

5.1.2. Unsupervised Learning

Unsupervised learning is a class of machine learning techniques that extracts conclusions from data sets without the aid of labels. The grouping assessment, which is used to find latent models or clusters, is the most common unsupervised learning technique in data analysis. Several characteristics are taken from the data and fed into the unsupervised learning algorithms [21]. Whenever fresh data are introduced, the algorithm employs the most recent characteristics acquired to make an inference about the data's category. Clustering and feature reduction are two common applications.

- **Unsupervised ANNs**

To enhance the results of flow inquiries in the manufacturing sector, Jiafu et al. [25] introduced the four-layer cloud-assisted smart factory (CaSF) concept. Four-layer ML approaches are used to resolve this issue. Greater trust, flexibility, and efficiency are shown by the use of ML approaches and techniques for a manufacturing organisation, but there are still a number of difficulties and technological obstacles in this sector. Intelligent devices, systems, the cloud, and applications are all part of today's engineering designs. In order to address CaSF problems, this method is useful. To boost efficiency, we use a four-layer CaSF design.

In addition to traffic constructing and administration, mobile traffic order is a crucial tool for gathering and analysing social event high-value, significant profile data, due to the increasing number of portable devices. Modern ML methods struggle to deal with mobile traffic because the quickly evolving and expanding variety of apps responsible for traffic destruction. The usage of large data was advocated since deep learning (DL) may solve the problem but would take more time to implement. DL was used to categorise secure mobile communications in Reference [1]. Based on a realistic exploratory setup, the authors looked at BD-enabled arrangement of encrypted mobile traffic using DL for the first time, describing general plan rules on an open cloud platform. The study's authors discovered that although big data may be a simple speeding agent for certain activities, it can't be for the time it takes to set up deep learning models for characterising traffic. The experiment design relies on a triangulated analysis of the Big Data selection with regards to the non-trivial trade-off, the amount of time it takes to finish, the amount of money it costs to transmit, and the accuracy with which it can classify data.

The rapid development of the Internet of Things and smart phones has lately greatly encouraged the growth of edge registration. While edge computing has proven very useful for small devices doing complex tasks, its rapid development has led to a widespread disregard of security risks in edge computing platforms and the apps they power.ML approaches were used to address security concerns raised by Xiao et al. [26].Their research provides a thorough analysis of the most convincing and basic attacks that can be deployed to practical edge computing frameworks using the comparable guard systems that include edge computing explicit properties.

- **K-Means**

One of the most popular and widely used unsupervised ML methods is K-means clustering It does this by scouring a dataset for a specified number of bunches, k. The term "group" is used to describe a collection of data organized according to shared characteristics. In order to counteract potential security risks, the authors of [27] investigated the topic of attack disruption. The authors detailed how K-means and other ML algorithms may be used to make CC systems safer.

A comprehensive review of ML approaches to a safe Cloud was conducted by Khan et al. [28]. Third parties' insecure data storage, management, and processing continues to discourage data owners from taking an active role. The door to miuse is still open. The data has been processed in a secure environment using SMC. Cloud-based data owners must have access to secure data storage and management tools. Pattern matching is a fundamental technique used in many disciplines. Also, K-means was presented as a novel method for intrusion detection by the authors in [29]. Our first focus was on identifying CC's unique traits and security requirements. Both common and unusual forms of attack in CC were uncovered. The authors said that the suggested strategy sped up the detection of intrusions while simultaneously reducing the false positive and false negative rates.

- **Singular Value Decomposition (SVD)**

It is also possible to utilise SVD to decompose a grid into its component vectors and attributes. SVD is often used in ML for information reduction and for counting various matrix operations such as framework conversion.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

The trust-based user access control strategy was studied by Khilar et al. in [30]. In order to better understand their cloud-based services, the researchers classified their clientele. The unique application is founded on a different kind of trust as well. The suggested ML method was able to efficiently handle a huge influx of activity data in a very short amount of time, which is a major time saver. The proposed model outperforms the related models. When compared to similar models, the one that was presented performs better. Dimensionality reduction in large data using data science techniques was suggested by Feng et al. in [31] and it may be used in cyber security and cyber forensics. They introduced a dimensionality reduction method based on orthogonal tensor SVD and high-order lanczos. For the purpose of moving the computational load of the orthogonal SVD technique to the cloud, they also created a secure orthogonal tensor SVD approach.

The methodology, difficulties, and unanswered problems for implementing ML-based security detection in the cloud were all outlined by Kumar et al. [32]. Investigators looking at security incidents in the Cloud have found that routinely recognizing irregularities does not provide desirable results. Because there aren't any good "gold standard" datasets, assessing models is problematic. In the process of transmitting these findings, you'll need to deal with difficulties like model consistency, confinement, and data storage. The authors framed the "attack interruption" problem as a viable strategy in the field of security information science in their study. They laid forth the framework, obstacles, open questions, and strategy around the successful deployment of ML-based security locations in the cloud. Results were better when ML and rules were combined, and it was shown that the two could be combined into a single ML unit by using channels.

5.2 Defence Methods based on Deep Learning

The deep learning algorithms have a big role in defending against DDoS attack against cloud computing and traffics controlling, the most common and effective deep learning algorithms have been illustrated

- **Deep Neural Networks (DNN)**

Two deep learning models, DNN and LSTM, were suggested by Sabeel et al. [33] to forecast unknown DoS/DDoS attacks. The authors of this study initially trained their models using the cleaned and labelled DoS/DDoS samples from the CICIDS2017 dataset, and then they tested and refined their models using the synthetic ANTS2019 dataset. The authors combine the synthesized dataset with the CICIDS2017 dataset in the second section. After the models have been retrained, the ability to identify freshly synthesized, previously unseen attacks is assessed. On the second half of the trial, both DNN and LSTM demonstrated significant performance improvements, with DNN reaching an accuracy of 98.72% and LSTM of 96.15%. Values of 0.987 and 0.989 are achieved by the DNN and LSTM in the AUC test, respectively. The ANTS2019 dataset is a synthetic model designed to reflect the complexity and diversity of actual cyberattacks. While we have completed the binary class classification, we have yet to implement the real-time detection setup.

When it comes to private clouds, DDoS attacks are a common reason why services must be lowered in quality. Virupakshar et al. [34] concentrate in on DDoS attacks that use bandwidth and connection flooding. OpenStack-based cloud DDoS attack detection using DT, KNN, NB, and DNN algorithms. The authors have also examined a number of classifiers and settled on one that provides the highest levels of accuracy and precision. When using a dataset that is produced on-the-fly, DNN has been selected as the model of choice because to its superior accuracy and precision. The authors have utilised an outdated dataset (KDDCUP99) and have provided little information regarding the LAN and cloud-based components of their data. For the KDDCUP99 dataset, the DNN algorithm has a lower accuracy value than competing methods.

The DNN architecture was first described by the authors in [6], (i.e. DeepDetect). It uses a feed-forward backpropagation design. Protecting services against DDoS attacks at the application layer is the goal of this suggested paradigm. The CICIDS2017 dataset was used to test the effectiveness of the suggested method against DDoS attacks. Comparisons between RF and DeepGFL have been made by the authors of this study. The F1-score number that DeepDetect produced was 0.99, making it the superior method. The AUC is quite near to 1, which demonstrates the excellent accuracy of the suggested model. This article describes how researchers used multiclass classification to build a cloud-based service for protecting against application-layer Distributed Denial of Service (DDoS) attacks. Only Application layer DDoS assaults have been tested using this method so far.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

To identify HTTP sluggish DoS attacks, in the review of Khalaf [4] the authors suggested a deep neural classification model based on flow data. Specifically, a deep FC feed-forward network was utilised as a classification model. Only the DoS samples from the CICIDS2017 dataset are used to assess the model. Types of DDoS attacks may be identified using the classifier. The acquired findings demonstrate the model's capability of accurately categorizing the assaults at the 99.61% level. Just HTTP slow DoS attacks (Slowloris, SlowHTTP, Hulk, and GoldenEye) have been tested using this method on the CICIDS2017 dataset.

- **Convolutional Neural Network (CNN)**

CNN consider as a one of the most effective deep learning algorithms. The authors in [2] state that traditional machine learning methods such as NB, KNN, and SVM are ineffective because to the small sample sizes of the datasets. Therefore, a Deep CNN model is what the authors recommend. Our tests revealed that, for a particular dataset with less characteristics, the suggested strategy outperformed three machine learning approaches. The model was tested across 11 different criteria, and it performed well in this multiclass classification. Unfortunately, not all traffic types are included in the dataset used to test the proposed model.

A strategy to detecting denial-of-service (DoS) assaults using Vector Convolutional Deep Feature Learning (VCDeepFL) is presented in the study by the authors in [9]. VCDeepFL combines Vector VCNN with Fully Convolutional Neural Networks. The suggested process is split into two parts: training and testing. In the training phase, VCNN (an unsupervised learning technique) is used for pre-training, followed by FCNN (a supervised learning technique). In VCDeepFL, testing is performed with the help of the weights that were acquired during training. In order to evaluate the efficacy of the proposed method, it has been applied to the NSL KDD dataset and compared to both traditional classifiers (MLP, SVM) and cutting-edge attack detection tools. As can be seen from the findings, the suggested method outperforms both baseline classifiers and the current gold standard for attack detection in terms of accuracy, false alarm rate, and detection rate. The authors have utilized an outdated dataset and have not shown any studies aimed at identifying unknown attacks.

For DDoS attack detection, in the work of Sabeel et al. [33] suggested a DAD-MCNN (i.e. multichannel CNN) system. How many channels are used is determined by how many feature groups are used. The features are separated by the authors into distinct tiers, such as the packet, host, and traffic levels. The authors have trained MC-CNN using the incremental training method. The authors have run a battery of experiments across the KDDCUP99 and CICIDS2017 datasets, with the former used for binary classification and the latter for multiclass category in KDDCUP99. For both binary and multiclass classification, MC-CNN was shown to perform better than state-of-the-art approaches. When training data is limited, such as in the case of DDoS detection systems, the findings revealed that MC-CNN performed better than alternatives. In practice, the outcomes of multichannel and single channel models are quite similar. As an added complication, multichannel models may not be adequate when tested in real-world conditions.

The CNN model has been developed to identify DoS attacks in [5].Over two datasets, dataset1 (simulated network traffic) and dataset2, the authors compare their proposed model against popular classification techniques such as support vector machine (SVM), support vector machine (KNN), and neural network (NN) (NSL-KDD). The suggested model outperforms the other four classification methods (DT, SVM, KNN, and NN) on both datasets, providing an accuracy of 99%.Here, a matrix representation of the data is achieved by the use of one-column padding. This may have an impact on the model's ability to learn.

- **Long Short-Term Memory algorithm**

Deep learning has been proposed by Li et al. [6] as a method for detecting distributed denial of service (DDoS) attacks in a software-defined network (SDN). The model consists of a hidden layer, an input layer, a reverse recursive layer, a forward recursive layer using FC, and an output layer. The model also includes CNNs in addition to RNNs and LSTMs. As a result, the authors created not just one, but four different models that go by the names of LSTM, CNN/LSTM, GRU, and 3LSTM. Applying the DDoS attack to the ISCX dataset yields a precision of 98%. The Ubuntu 14.04 operating system serves as the foundation for the DDoS attack detection and defense system, and real-time DDoS attacks are used to assess the system's effectiveness. However, 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 that have been tested up to this date. Further real-time DDoS attacks could be launched, and there are numerous options available.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

To overcome DDoS assaults in a fog network, the authors in [8] developed a DL-based approach. Network and transport-level DDoS attacks have been detected using LSTM. The parameters of the LSTM model were built using two different sets of input data. By applying the DL model to the CTU13 Botnet, the authors were able to get the findings shown here in the first scenario. The second case involves testing the DL model in action against a subset of the Hogzilla dataset and some real-time DDoS attacks. The model was compared to other methods by the authors. The LSTM model has been shown to perform with a 98.88% rate of success across all test cases. Since SDN uses an OpenFlow switch, the DDoS defender module may prevent the malicious packet from reaching the cloud server. This page solely reports on Network/transport-level DDoS assaults; no real-time feasibility investigation of the suggested has been performed.

Modeling a multi-layered architecture, the authors in [9] suggest a four-layer structure with two layers of LSTM algorithm, which are a dropout layer, and an FC layer. In this method, network traffic behavior is learnt directly from a brief series of packets, eliminating the need for handmade feature engineering. In this study, we do three experiments on the CICIDS 2017 Wednesday and Friday datasets using three different methods (discrete time, artificial neural network, support vector machine). Experiment 1 demonstrated that the LSTM-based strategy outperformed the competition by effectively learning the complicated flow-level feature descriptions inherent in raw input. The outcome of Experiment 2 confirmed the effectiveness of the suggested approach in effectively capturing the dynamic behaviors of unknown network traffic. The third experiment confirmed that it is no longer always beneficial to allow the model to test more packets for every flow, with higher n values. The aforementioned model makes use of a selection (i.e., S F) from the whole set of n packets. The suggested model's learning and performance can be negatively impacted by the padding values used.

Two approaches were presented by Shurman et al. [3]. The first technique is a hybrid-based intrusion detection system (IDS), while the second is a deep learning model based on a recurrent neural network (RNN) that can spot DoS/DDoS attacks. First, a program known as an intrusion detection system (IDS) may monitor traffic on any network node and identify suspicious IP addresses. It may filter out unwanted Internet Protocol addresses. The CICDDoS2019 dataset includes several different kinds of DrDoS attacks, and the LSTM was employed in the second way. Different models are compared to the second one. The outcomes demonstrate that the model is superior than its competitors. Only the reflection-based CICDDoS2019 dataset has been utilized, although the LSTM-based model demonstrates an accuracy of 99.19% on this dataset. Separation of concerns also characterizes the hybrid IDS and LSTM approaches.

- **Gated Recurrent Unit (GRU)**

In the previous work of Assis et al. [36] established a defense mechanism against DDoS and intrusion threats in an SDN setting (2021). The suggested system has two main parts: the detection part and the mitigation part. In the event of an attack, the detection module will identify it. The makers of this module use a DL-based GRU technique to analyses individual IP traffic data in order to identify DDoS and intrusion attacks. Once an attack has been identified, the mitigation module will immediately begin working to stop it. On two datasets (CICDDoS 2019 and CICIDS 2018), the authors put their proposed model through its paces against seven different ML techniques. Different ML methods include: CNN, DNN, LR, LSTM, KNN, SVM, and GD. The authors have used the CICDDoS 2019 dataset and the CICIDS2018 dataset as test cases. Both the accuracy, precision, recall, and f-measure of the proposed model, as well as the usefulness of the strategies in categorising normal and attack flows separately, have been evaluated in comparison to current ML techniques.

The GRU was able to identify DDoS and incursion attacks across the board. In addition, a feasibility test is conducted by determining the typical rate of flows per second that can be examined and classified by the detecting techniques. The test is conducted using real IP traffic data obtained from the State University of Londrina. Based on the findings, GRU seems to be a workable strategy. The suggested technique achieves average values of 99.94% and 97.09% on the CICDDoS2019 and CICIDS2018 datasets, respectively, for accuracy, recall, precision, and f-measure. Offline datasets analysis has been performed, and the publication does not include calculations for detection or training timeframes.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

6. Testing and Evaluation Methods

Datasets are a crucial component of evaluating the effectiveness of proposed systems, and in this section, they have been presented in detail along with related and more recent types.

6.1. ISCX2012 Dataset

In 2012, a ISCX2012 dataset is lunched, it is compiled full-packet network data from the seven days (11-06-2010 to 17-06-2010) of regular and malicious traffic that make up the ISCX2012 dataset. Examples of malicious traffic include internal network infiltration, distributed denial of service, brute force SSH, and HTTP denial of service. The data in this collection was generated in a simulated network setting. Unbalanced and annotated dataset (Ring et al. 2019There are two broad types of profiles included in the ISCX dataset: profiles that describe malicious activity and profiles that describe typical user behavior. There are 2,381,532 clean records and 68,792 bad ones. [1], [13].

6.2. UNSWNB15 Dataset

The Cyber Range Lab at the Australian Cyber Security Centre created it. Specifically, the argus, bro-IDS, IXIA Perfect Storm, and tcpdump tools were utilized to compile this dataset. Fuzzers, exploits, backdoors, generic assaults, shellcode, denial-of-service (DoS) attacks, worms, and analysis attacks are only some of the nine kinds of attacks that may be generated using the IXIA tool [14]. The packets travelling across the network were snatched by the tcpdump programme. It took a total of 31 hours (16 hours on 22-01-2015 and 15 hours on 17-02-2015) over the simulation period of the dataset to capture 100 GBsFrom the pcap data, the trustworthy characteristics were retrieved using Argus and bro-IDS. There are 49 different functions. In addition, twelve algorithms written in C# were created to examine the packets' movement across the network. There are 2,218,761 safe records and 321,283 risky ones within its 2,540,044 total.

6.3. CICIDS2017 Dataset

From July 3rd to 7th, 2017, the CICDS2017 dataset was created in a simulated setting. Both unidirectional and directed flows of network traffic in packet form are included in this collection. This year's CICIDS2017 data was compiled by the authors in [10] DDoS, DoS, Web Attack, Heartbleed, Infiltration, Botnet, Brute Force SSH, and Brute Force FTP are all included into its routine operation [1]. The CICFlowMeter application has taken the produced network traffic and retrieved over 80 characteristics for each flow. Data from 25 users' actions were abstracted based on the protocols HTTPS, FTP, HTTP, SSH, and email. In total, 2,273,097 clean records exist, while 557,646 negative records exist.

6.4. The CSECICDataset

In a joint effort, the Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) have compiled this report using data they gathered over the course of 10 days, from February 14 (Wednesday) to February 22 (Friday (02-03-2018).The big network was used to build this dataset, which includes seven different attack scenarios: Heartbleed, Botnet, Brute force, DoS, Web assaults, DDoS, and internal penetration [4]. To simulate network activity, the CIC Flow Meter program has gleaned eighty different characteristics.

6.5. CICDDoS 2019 Dataset

A dataset known as CICDDoS2019 (2019) was created by Sharafaldin et al. [7]. Through the use of the CICFlowMeter-V3 program, over 80 various traffic characteristics have been determined from the raw data. The CICDDoS2019 is a collection of safe and modern DDoS attacks. This dataset contains a significant number of synthetic DDoS attacks across TCP/UDP protocols, produced from actual traffic. Reflection-based attacks and exploitation-based attacks are two branches of the attack tree. Microsoft SQL, and several network Protocol else, CICDDoS 2019 dataset was collected over the course of 2 days in PCAP and flow formats for use in training and testing purposes. Twelve

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

different DDoS attacks were caught on January 12th, 2019 for use in training. These included SSDP, UDP-Lag, SNMP, MSSQL, DNS, TFTP, NetBIOS, NTP, UDP, LDAP, WebDDoS, and SYN. On March 11th, 2019, seven different attacks were captured for use in testing.

7. Discussion and Future Research Directions

This study provides a comprehensive and in-depth analysis of several methods for blocking and detecting DDoS assaults utilizing Deep learning and Machine learning algorithms that are practical at the Cloud Computing Systems. This review covers a total of 64 research publications, and 5 review articles. The review looks into the defense strategies used to identify, lessen, and/or prevent DDoS attacks. It categorizes DDoS defense techniques-based Machine learning and Deep Learning. For many different types of DDoS assault and DDoS defense strategies, the classification stresses a concrete approach and offers tables of relations. Additionally, popular testing datasets and evaluation techniques are included in this work.

Furthermore, in the previous work of Parast et al. [1], to determine the state of the field at the time, the study examined service-based cloud computing security vulnerabilities. In order to present an uniform taxonomy of security challenges across the three-layer paradigm, i.e., IaaS, PaaS, and SaaS, this paper's primary contribution is to examine the state of cloud security over the past ten years. The evaluation, however, did not address recent attacks on cloud computing, testing datasets, or defense strategies.

In the prior work of Alashhab et al., [2], This survey offers a thorough examination of the security concerns and difficulties affecting cloud service providers and their customers. In this study, a brand-new taxonomy for CC attacks, distributed denial of service (DDoS) attacks, and DDoS attack detection techniques on CC is also proposed. Additionally, it offers a qualitative contrast with the previous surveys. The survey also hopes to act as a guide and a resource for other academics who are developing fresh DDoS attack detection strategies for the Cloud Computing environment.

Agrawal and Tapaswi [3], This paper provides a thorough taxonomy of all potential cloud DDoS assault methods, along with in-depth explanations of the characterization, avoidance, detection, and mitigation techniques. The study offers a thorough analysis of the crucial performance indicators for assessing the effectiveness of various defensive solutions in a cloud context. The purpose of this survey paper is to inspire cloud security experts to create strong defenses against diverse DDoS attacks. Future research directions are presented together with the identification of the research gaps and challenges.

Khalaf et al., [4], This research study focuses on the most popular DDoS attack defense strategies that employed statistical and artificial intelligence techniques. The review also categorizes and demonstrates the attack kinds, testing characteristics, assessment techniques, and testing datasets used in the methodology of the suggested defense methods. Finally, this research offers a framework and potential areas for expansion for creating superior DDoS attack defense approach models.

Aziz et al. [5], the study provides a thorough analysis of cutting-edge methods for identifying DDoS attacks. It sought to characterize numerous DDoS attack types, including Web-based, peer-to-peer, and internet relay chat-based attacks. Additionally, the key difficulties facing efficient DDoS defensive techniques are also investigated. Finally, numerous DDoS attack detection strategies' weaknesses are emphasized.

Lata, S., & Singh [6], the study offers a cogent analysis of the benefits and drawbacks of the security techniques now in use. Additionally, it discusses the state-of-the-art of IDS, the significance of feature selection and dimensionality reduction, and security issues with each cloud service type. This study categorizes IDS techniques according to the assaults it recognizes, where they are located, and how they are configured. The study will also cover hypervisor introspection (HVI) and virtual machine introspection (VMI) methodologies. However, the three separate views that serve as the foundation for the current study's structure are cloud security concerns, the significance of feature selection, and an analysis of current IDS methodologies.

The purpose of this review is to broaden the focus and direct DDoS research in new directions. Its conclusions highlight certain unresolved research issues and make a few recommendations for additional study. However, the current study distinguishes itself from the previous study by

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

considering the limitations of the most recent related review articles which have been discussed. Table 1. Shows the comparison results of our study with the most related work.

Table 1: Comparison of our review with the most related work

Ref.	Cloud Computing	DDoS attack		Defense Methods			Dataset
		Low Rate	Hight Rate	Traditional	ML	DL	
Parast et al. [1]	✓	✓	✓	×	×	×	×
Alashhab et al., [2]	✓	✓	✓	✓	✓	×	×
Agrawal & Tapaswi [3]	✓	✓	✓	✓	×	×	×
Khalaf et al., [4]	×	×	✓	✓	✓	×	✓
Aziz et al. [5]	✓	✓	✓	×	×	×	×
Lata and Singh [6]	✓	×	×	✓	✓	×	✓
Our Study	✓	✓	✓	×	✓	✓	✓

Different algorithms based on deep learning and machine learning will be used in the future for cloud security. The datasets and research directions listed below all called for additional investigation:

- Before implementing new innovations, it is crucial to do a careful analysis of overhead. The virtualization approach, for instance, might be used to place critical functions in the ideal location.
- A collection of Artificial Intelligence datasets from many disciplines, including spam, phishing, and other security-related datasets, is known as testing datasets.
- This open-source deep learning project seeks to detect and prevent the use of dangerous file paths, registry keys, and URL addresses. It exposes both machine learning and deep learning. Datasets with sample ratings are typically found in registries for specific models or bodies of knowledge.
- To our knowledge, no survey during 2014 to 2023 discussed the topics which have been covered in our study.
- There are still many difficulties that can be investigated in the future.

8. Conclusion

The most challenging issues in cloud computing were studied in this study, in particular, security threats and attacks. To solve the security issues in cloud computing, a variety of machine learning techniques, including SVD, Naive Bayes, ANNs, SVM, K-NN and K-Means were examined. Also, the most effective deep learning techniques have been presented such as DNN, CNN, LSTM and GRU. Also, the study covers the Sophisticated types of Flooding Attacks and the testing dataset. Furthermore, the study examined and evaluated the offered methods, noting both their advantages and disadvantages. Subsequently, the study contributes in the development of sophisticated and efficient DDoS attack defense techniques. Additionally, ongoing updates and improvements are required for the classifications of the linked DDoS attack aspects in order to counter new and complex threats. In addition, a number of research areas have been identified to be considered further in the future.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] 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.

[2] 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.

[3] Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769-3795.

[4] 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.

[5] Naeemullah Khan, Ismael Khaleel, & Elika Daghighi. (2021). Improved feature selection method for features reduction in intrusion detection systems . Mesopotamian Journal of CyberSecurity, 2021, 9–15. https://doi.org/10.58496/MJCS/2021/003

[6] 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.

[7] Elzamly, A., & Hussin, B. (2016). Classification of critical cloud computing security issues for banking organizations: A cloud Delphi study. International Journal of Grid and Distributed Computing, 9(8), 137-158.

[8] 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.

[9] El-Boghdadi, H., & Rabie, A. (2019). Resource scheduling for offline cloud computing using deep reinforcement learning. *Int. J. Comput. Sci. Netw*, *19*, 342-356.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Zardari, M. A., Jung, L. T., & Zakaria, N. (2014, June). K-NN classifier for data confidentiality in cloud computing. In *2014 International Conference on Computer and Information Sciences (ICCOINS)* (pp. 1-6). ieee.

[15] Shamshirband, 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).

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

[16] Park, J., & Lee, D. H. (2018). Privacy preserving k-nearest neighbor for medical diagnosis in e-health cloud. *Journal of healthcare engineering*, *2018*.

[17] Kour, H., & Gondhi, N. (2020). Machine learning techniques: a survey. In *Innovative Data Communication Technologies and Application: ICIDCA 2019* (pp. 266-275). Springer International Publishing.

[18] 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.

[19] 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).

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] Wan, J., Yang, J., Wang, Z., & Hua, Q. (2018). Artificial intelligence for cloud-assisted smart factory. *IEEE Access*, *6*, 55419-55430.

[26] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, *107*(8), 1608-1631.

[27] Zou, Y., Zhao, Z., Shi, S., Wang, L., Peng, Y., Ping, Y., & Wang, B. (2020). Highly secure privacy-preserving outsourced k-means clustering under multiple keys in cloud computing. *Security and Communication Networks*, *2020*, 1-11.

[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] Zhao, X., & Zhang, W. (2016, July). An anomaly intrusion detection method based on improved k-means of cloud computing. In *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)* (pp. 284-288). IEEE.

[30] Khilar, P. M., Chaudhari, V., & Swain, R. R. (2019). Trust-based access control in cloud computing using machine learning. *Cloud Computing for Geospatial Big Data Analytics: Intelligent Edge, Fog and Mist Computing*, 55-79.

[31] Feng, J., Yang, L. T., Dai, G., Wang, W., & Zou, D. (2018). A secure high-order Lanczos-based orthogonal tensor SVD for big data reduction in cloud environment. *IEEE Transactions on Big Data*, *5*(3), 355-367.

[32] Kumar, R. S. S., Wicker, A., & Swann, M. (2017, November). Practical machine learning for cloud intrusion detection: challenges and the way forward. In *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security* (pp. 81-90).

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023

[33] 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.

[34] 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.

[35] 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.

Doi : https://doi.org/10.54216/FPA.110103
Received: December 04, 2022 Accepted: April 03, 2023