IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
University of Kut Journal
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
Vol. 10 , Issue 2 , December 2025

Advancement in Detection and Mitigation Techniques of DDoS Attacks against Cloud Computing Environment

Omer S Mahdi [1] , Abdulbasit ALAzzawi [2]

Abstract

This research covers a detailed survey of the Distributed Denial of Service (DDoS) attack cases in the context of cloud computing, describing their evolution in light of the past, current, and future trends, as well as the related technologies used in detection and mitigation approaches. It highlights the contradictory nature of cloud computing services to be both a for resource scalability and flexibility and a hurmful, as any DDoS attack can wreak havoc on it. The literature has been synthesized over the past decade, from 2012 to 2024, to identify the main advances in detection techniques, starting with traditional signature-based methods and ending with AI-based innovative approaches, such as machine learning and deep learning algorithms. The paper deals with the DDoS challenges, including the evolution of attack vectors, scalability limit of detection systems, integration of DDoS with cloud services, false positives or negatives, and resource limitations. Future research and practice call for the adoption of AI and machine learning techniques, a mixture of manual and automatic detection approaches, strong collaborations, regular system updates, and user education and awareness.

Keywords: DDoS, Cloud Computing, Deep Learning, Machine Learning, Distributed Denial of Service

Affiliation of Authors
[1, 2] College of Science, University of Diyala, Iraq, Diyala, 32000

[1]scicompms222316@uodiyala.edu.iq
[2] dr.abdulbasit@uodiyala.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Dec. 2025

التقدم في تقنيات الكشف والتخفيف من هجمات DDoS ضد بيئة الحوسبة السحابية

عمر سلام مهدي [1] ، عبد الباسط العزاوي [2]

المستخلص

يغطي هذا البحث دراسة تفصيلية لحالات هجوم رفض الخدمة الموزعة (DDoS) في سياق الحوسبة السحابية، مع وصف تطورها في ضوء الاتجاهات الماضية والحالية والمستقبلية، بالإضافة إلى التقنيات ذات الصلة المستخدمة في الكشف والتخفيف من آثارها. إنه يسلط الضوء على الطبيعة المتناقضة لخدمات الحوسبة السحابية لتكون نعمة لقابلية التوسع في الموارد والمرونة ولعنة، حيث أن أي هجوم DDoS يمكن أن يلحق الضرر بها. وقد تم تجميع الدراسات على مدى العقد الماضي، من عام 2012 إلى عام 2024، لتحديد التطورات الرئيسية في تقنيات الكشف، بدءاً من الأساليب التقليدية القائمة على التوقيع وانتهاءً بالأساليب المبتكرة القائمة على الذكاء الاصطناعي، مثل التعلم الآلي وخوارزميات التعلم العميق. تتناول هذه الورقة تحديات DDoS، بما في ذلك تطور نواقل الهجوم، وحدود قابلية التوسع لأنظمة الكشف، وتكامل DDoS مع الخدمات السحابية، والإيجابيات أو السلبيات الكاذبة، وقيود الموارد. تدعو الأبحاث والممارسات المستقبلية إلى اعتماد تقنيات الذكاء الاصطناعي والتعلم الآلي، ومزيج من أساليب الكشف اليدوي والآلي، والتعاون القوي، وتحديثات النظام المنتظمة، وتعليم المستخدم وتوعيته.

الكلمات المفتاحية: هجمات الحرمان من الخدمة الموزعة DDoS، الحوسبة السحابية، التعلم العميق، التعلم الآلي، رفض الخدمة الموزعة

انتساب الباحثين
[1، 2] كلية العلوم، جامعة ديالى، العراق، ديالى، 32000

[1]scicompms222316@uodiyala.edu.iq
[2] dr.abdulbasit@uodiyala.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر: كانون الاول 2025

Introduction

Cloud computing is the availability of computer resources over the internet, such as physical or virtual servers, data storage, networking features, application development tools, software, and AI-driven analysis tools. This strategy offers Internet users more scalability and flexibility than

traditional on-premises infrastructure [1].

Early in the 1960s, "Dr. Joseph Carl Robnett Licklider," an American computer scientist and psychologist known as the "father of cloud computing," presented the first concepts of global networking in a series of memos describing an Intergalactic Computer Network[2]. This marked the beginning of cloud computing technology. However, modern cloud infrastructure for businesses did not appear until the early 2000s.

The three primary types of cloud computing are public cloud, private cloud, and hybrid cloud. Within these deployment models, there are four main services categorized as follows:

1- Infrastructure-as-a-Service, or IaaS, offers online access to basic computer resources such as networking, storage, and physical and virtual servers.
2- Platform-as-a-Service PaaS: it offers a platform for running, developing, and managing applications on-demand that includes hardware, the entire software stack, infrastructure, and development tools. This eliminates the need for an installed platform's expensive, complicated, and rigid maintenance.
3- Software-as-a-Service SaaS: Application software hosted in the cloud is also called cloud-based or cloud applications.
4- Serverless computing: it is a cloud computing model that allows developers to concentrate all of their time and energy on the code and business logic unique to their project by giving the cloud provider full control over all back-end infrastructure management tasks, including provisioning, scaling, scheduling, and patching, an example of a serverless system is Function-as-a-Service or FaaS. Application code "functions" can be run by developers in response to particular events.

Cloud computing is growing as the standard platform for distributing large data pools with various user-friendly features.

Ensuring the security and availability of data, resources, and services is still a research challenge despite the rapidly growing popularity of cloud services.

The proliferation of cloud computing as a central component of modern digital infrastructure presents a double-edged sword: scalability, flexibility, and efficiency are the main advantages of this technology, but it also raises the level of threats and vulnerabilities, in particular to Distributed Denial of Service (DDoS) attacks. By taking advantage of the decentralized cloud infrastructure, these attacks have continued to grow in complexity, magnitude, and frequency, employing multifaceted attacks that are challenging to identify and stop. The problem lies not only in the direct impact of these attacks—disrupting services and causing significant downtime—but also in the subtler, more insidious effects:

Eroding user trust, imposing hefty financial losses, and potentially compromising sensitive data.

Many traditional DDoS attack detection algorithms have been designed for more classical network environments. They do not perform well in the cloud as the resources are combined and replenished constantly, and service elasticity is a factor. This limitation is further compounded by the characteristics of cloud platforms, which share the resources where the attack of one customer impacts other customers and is used in contrast to non-cloud platforms. Also, the kind of cloud capabilities that come in handy when applications

need to handle real-time surge traffic (scalability) can also benefit an attacker by helping them exploit auto-scaling and use the auto-scaling capabilities to augment the size of their attacks[3].

Hence, the development in DDoS attack detection puts it to the test and calls for revamping and innovation in detection techniques. This needs the creation of adaptive and intelligent systems capable of the instant separation of benevolent and harmful traffic in real-time mode with constantly changing conditions of cloud computing. These platforms should tackle not only the distinctive problems of cloud-based architecture but also see through the future of DDoS attack methods. The problematization statement indicates the importance of research and development to enhance the capacity of Cloud environments to fight off the ongoing menace of DDoS attacks.

The main objective of this research can be summarized as:

1. Explore the advancement of detection and mitigation techniques regarding DDoS attacks on cloud computing environments.
2. Give a broad understanding of the history of DDoS attacks.
3. Chronologically summarize related research articles by comparing their underlying architecture, datasets, detection and mitigation techniques, and accuracy.

Then this work is organized as follows: section 2 discusses our research methodology, the history of DDoS attacks and their types provided in section 3; in section four we explore different detection and mitigation techniques in the context of DDoS in cloud computing, compare selected articles based on their underlying architecture, datasets, detection and mitigation techniques, and accuracy provided In a tabular way in section 5, sections 6 and 7 discussed the challenges related to DDoS in cloud computing ,and conclusion, respectively, followed by the references.

1. Methodology

The Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols have adhered to identify pertinent and noteworthy papers about our study area. Three protocols were used to complete this study: searching, inclusion and exclusion, and the final reviewing and data extraction [4].

2.1 Searching Protocol

We start by searching trusted online libraries and databases such as ScienceDirect, IEEE Xplore MDPI, using search terms related to our research area such as "DDoS attacks," "DDoS attacks detection," "DDoS attacks detection technique," "DDoS attacks detection technique in cloud computing," DDoS attacks mitigation on cloud" and so on. We also used advanced search techniques (AND, OR) combining search terms like "DDoS," cloud computing," "Deep learning," and "Machine learning." We downloaded 189 articles in this phase.

2.2 Inclusion and Exclusion Protocol

We included relevant English peer-reviewed articles for our inclusion and exclusion criteria. Meanwhile, non-English, non-peer-reviewed, and non-relevant to our research were excluded. Forty-three articles were excluded in this phase. We considered articles published in (2012-2024), publication type (journal or conference), publishing house, and cite score during preliminary screening. We verified the themes of the searched articles against our survey theme by extending this screening process to the abstract composition level. Ultimately, we selected the top

40 articles for additional analysis, 14 of which were relevant papers but didn't provide a novel solution (i.e., review papers). Papers were selected based on the focus, especially on DDoS detection in a cloud computing environment, the uniqueness of the proposed detection technique, and the reported design outcomes in most cases. In particular, the studies which described their detection accuracy were emphasized. Therefore, the methodologies employed by different studies could be evaluated in a direct comparison.

2.3 Reviewing and Data Extraction

As the last step in our process, we thoroughly examined a variety of contextual factors before performing a thorough analysis of the selected publications. We began by arranging the summary in accordance with the context, goal, source of evidence, eligibility criteria, databases, model algorithms, findings, and conclusion of the abstract section. After that, we moved on to the paper's in-depth illustration, considering the previously mentioned aspects along with a few more details, including computational complexity, the possibility of real-time deployment, limitations, research gaps, and prospects.

3- DDoS Attack history

A distributed denial of service (DDoS) attack is a malicious attempt to stop regular traffic from reaching a targeted server, service, or network by flooding the target or the infrastructure around it with a deluge of Internet traffic.

DDoS attacks are conducted via networks of computers linked to the Internet. Computers and other devices, including Internet of Things devices, are part of these networks. These devices have been compromised with malware, which enables an attacker to remotely manipulate them. These standalone devices are known as bots (or zombies), and a botnet is an assembly of bots. An attacker can control an attack by remotely instructing each bot in the botnet once it has been set up. Each bot that is sent to the IP address of a target when a victim's server or network is targeted by a botnet may overload the server or network, preventing regular traffic from reaching which make it challenging to distinguish between attack and legal traffic because every bot is an Internet device.

Cloud computing has been increasingly prevalent in commercial technologies and academic study in recent years, one of the security risks that compromises availability is DDoS. DDoS is one of the top nine risk factors to a cloud computing environment, according to Cloud Security Alliance[5]. In a cloud environment, 14% of all attacks are DoS attacks. DDoS attacks are a serious security concern that has long been a subject of attention for researchers. According to, the term “Denial of Service (DoS)” was first used by Gligor in the context of operating systems, but it has subsequently gained widespread use. A Distributed Denial of Service (DoS) attack is a concerted attempt to harm a victim using several computers (DDoS)[6].

The first recorded distributed denial of service attack was in 1996 when a SYN flood took down Panix, one of the oldest ISPs, offline for many days. Since then, countless DDoS attacks have occurred as shown in Figure (1).

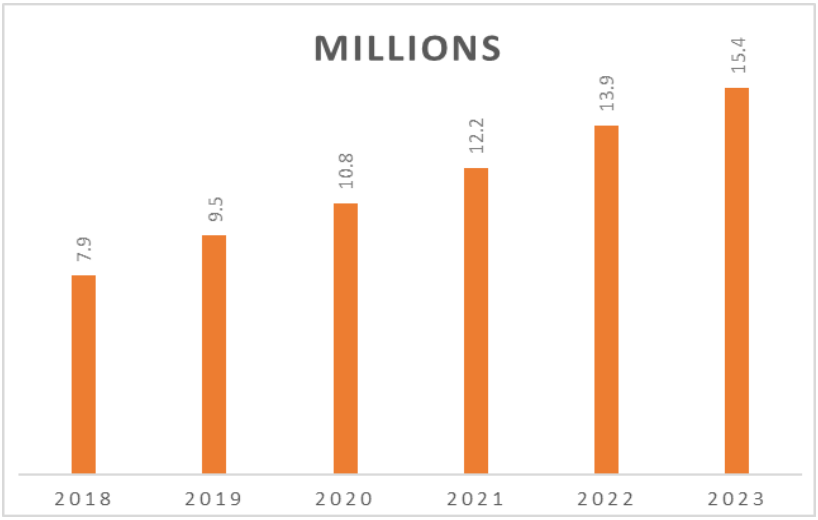

Figure (1): No. of DDoS attacks in millions

Nevertheless, more than just the quantity of DDoS attacks are happening these days. Attackers are building ever-larger botnets and hijacking device armies to produce DDoS attacks. DDoS attacks are becoming larger in scope in tandem with the growth of botnets[7].

Microsoft stopped what is thought to be the biggest DDoS attack in history in November 2021, directed against an Azure client with a throughput of 3.45 Tbps and a packet rate of 340 million PPS.. With a peak of 46 million requests per second (rps), Google claimed to have stopped the "biggest" DDoS attack ever recorded.

The attack was directed at a user who had used Google Cloud Armor, a network protection service, for 69 minutes with HTTPS security protocol and authentication. Five thousand two hundred fifty-six source IPs from 132 different countries contributed to the attack, which means that more than 5,000 distinct IP addresses were registered for the attack[8].

In May 2023, the US government seized 13 domains linked to 'booter' sites that offer DDoS-attacks-for-hire services. These sites allow customers to pay malicious actors to launch DDoS attacks against the victim of their choice by overwhelming their servers with traffic[9].

The domain seizure revealed that "hundreds of thousands of registered users have used these services to launch millions of attacks against millions of victims," including financial institutions, school districts, government websites, and universities as shown in Table (1).

Table (1): Most famous DDoS attacks

Year	Details
1996	A SYN flood DDoS attack took Panix offline for a few days.
1998	DDoS tools were developed in their first iteration. Nevertheless, Smurf amplification and point-to-point DoS attacks persisted even though DDoS tools were not often used.
1999	At the University of Minnesota, a single machine connected to a trinoo network was flooded, leaving the network inoperable for over two days. Additionally, Shaft was used to detect one of the large strikes.

2000	When 15-year-old Michael Calce, also known as "Mafiaboy," started "Project Rivolta," it resulted in removing the top search engine website and Yahoo as the next target. This incident served as a warning to everyone, demonstrating how quickly a single child may take down popular websites throughout the globe.
2001	From Mbps to Gbps, the onslaught was progressively intensified. The 3 Gbps DDoS attack had a considerable impact on the business Efnet.
2002	Several name servers became unavailable within a few days as a result of the congestion that the attackers caused. Although all inquiries are answered by servers, many legitimate queries were not able to reach certain root name servers.
2003	Using Mydoom, block the SCO collecting website's operation. A sizable number of PCs were infected to get the data to the target server.
2004	Attackers attacked online payment processing companies like 2Checkout and Authorize-IT. It was then discovered that the attackers had threatened and coerced them into taking down their websites.
2005	Attackers demanding 40K Euros to halt a DDoS attack on the gambling website "jaxx.de"
2006	Michelle Malkin's blog was the target of DDoS attacks. Over a week, there were constant attacks.
2007	During the riots, Russian government websites were severely targeted by DDoS attacks. Many were prevented from accessing IP addresses outside Estonia for a few days.
2008	A website belonging to a well-known European-associated press was attacked. The attacker controls the server for an hour or ninety minutes, which is the longest time the website has been down.
2009	Many institutions were impacted, including the president of the nation, a bank, the largest daily newspaper in Asia, and numerous North American websites. A botnet of around 1.6 million machines is used to carry out this attack.
2010	Operation Payback: A DDoS attack was launched against the Master website. Numerous services, including Visa, Master Card, and PayPal, ceased to support WikiLeaks.
2011	North Korea was the target of an anonymous DDoS attack. "LOIC" is a well-known DDoS tool that Anonymous and other online attackers employ to flood websites with requests and continuously interfere with the target server.
2012	Many attacks on US banks presume to use the DDoS tool.
2013	Spamhaus attack, the DDoS attack, essentially overburges the victim's servers by flooding them with information. It can interfere with the victim's business or knock its site offline
2014	With over 100 measures over 100 GB/sec reported, it was one of the most massive DDoS attacks ever.
2015	attackers launched one of the largest coordinated attacks against Proton mail. After a few days, the attack hit 80 Gbps of traffic.
2016	Attackers are aiming for the French web host OVH with 1 Tbps. The IoT botnet's source code becomes public within a few days and is named the year's "marquee" attack.
2018	GitHub was the target of one of the biggest verified memcached DDoS attacks ever recorded.

	Sending packets at a rate of 126.9 million per second, this attack hit 1.3 Tbps.
2020	According to AWS's report on the mitigation of a massive DDoS attack, connection-less Lightweight Directory Access Protocol (CLDAP) web servers were taken over by hackers.
2021	Microsoft stopped a DDoS attack aimed at an Azure user with a 340 million PPS packet rate and 3.45 Tbps throughput.
2022	For 69 minutes, Google prevented a DDoS attack that peaked at 46 million requests per second (rps) using the HTTPS authentication and security protocol.
2023	The US government took over thirteen domains connected to "booter" sites. Hundreds of registered users have utilized these services to launch millions of attacks against millions of victims.

3.1 DDoS Attack Types

DDoS attacks in the cloud can be categorized into several types based on the attack vector used or the part of the network infrastructure they target. Here are some of the common types of DDoS attacks encountered in cloud computing[10]:

3.1.1Volume-based Attacks:

These attacks aim to saturate the bandwidth of the targeted site or service, including:

1) ICMP (Ping) Flood: Leveraging the Internet Control Message Protocol to overwhelm the target with ping requests.
2) UDP Flood: Flooding the target with User Datagram Protocol UDP packets to saturate the bandwidth.

3.1.2 Protocol Attacks:

These attacks target resources like firewalls and load balancers by exploiting weaknesses in the layer where internet protocol communication occurs:

1) SYN Flood: Exploiting the TCP handshake process by sending a flood of TCP/SYN packets, often with a “spoofed” sender address.
2) Ping of Death: Exploiting vulnerabilities in older systems where packets larger than the maximum allowed size cause overflow and system crashes.

3.1.3 Application Layer Attacks:

Targeting the web application layer, these are more sophisticated and difficult to detect because they mimic legitimate user traffic. Examples include:

1) HTTP Flood: Sending overwhelmingly HTTP requests to the web server.
2) Slow loris: Holding as many connections to the target web server open for as long as possible with minimal traffic, which can eventually overwhelm the server.

3.1.4 Amplification Attacks:

the attacker sending small queries to a third party that then responds with a much larger reply; the response is directed towards the targeted IP address. Common amplification attacks are:

1) DNS Amplification: DNS response traffic is flooded at a target by using publicly accessible DNS servers.
2) NTP Amplification: Exploiting public Network Time Protocol servers to flood a target with UDP traffic.
3) NoneXistent Name Server Attack (NXNSAttack) In late May 2020, cybersecurity researchers disclosed an attack called NXNSAttack, which relies on a vulnerability in the Domain Name System (DNS) as shown in Figure (2).

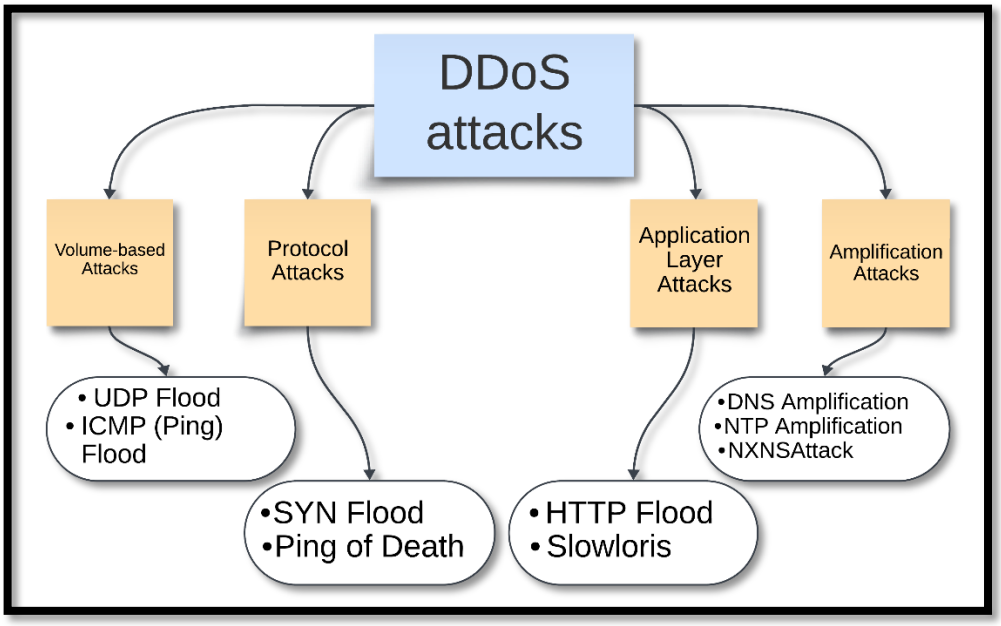

Figure (2): DDoS attack types

3.2 DDoS Detection Methodologies

Intrusion Detection Methodologies

1) Signature-based Detection: By monitoring events and seeing patterns that correspond to the signatures of known assaults, signature-based ID systems are able to identify intrusions. An attack signature outlines the steps needed to carry out the attacks, along with the sequence in which they must be completed. Additionally, it only identifies attacks whose signatures have been kept on record in a database[11]. Regular updates of the signatures are necessary for efficiency. New threats against the hosts are found regularly, much like new threats are frequently released, necessitating signature changes. This approach is effective only when applied to the set behavioral pattern. They cannot counter attacks made by humans or worms that can change their behavior on their own[11].

They suggested a security service known as a "filtering tree," which functions like a service broker inside a service-oriented architecture (SOA) model. It works by transforming customer requests into XML tree form and filtering messages at different stages by first comparing the client IP of the request with previously stored suspicious IP in Traceback. Next, Cloud Defender is used to detect DDoS attacks, including HTTP DDoS, Forcible parsing DDoS, and XML DDoS, and a virtual Cloud Defender will defend against these kinds of attacks[12].

proposed solution for detecting Distributed Denial of Service (DDoS) attacks in Eucalyptus private Cloud by evaluating two virtual machines, Snort(an open-source network intrusion detection system) Network Intrusion and Detection System; they simulate various DDoS attacks and analyze the effectiveness of the IDS setup applying data fusion methodology based on the Dempster-Shafer Theory to enhance the accuracy of attack detection and reduce false positives. Their findings highlight the potential of integrated IDS in cloud computing environments for improving DDoS detection and mitigation, as their methods show 97.33% accuracy in detecting DDoS attacks[13].

proposed a modified confidence-based Filtering method (CBF), which is investigated for a cloud

computing environment based on correlation patterns to detect and mitigate DDoS attacks on the Cloud. They demonstrate that this modification introduces nominal additional bandwidth and increases the processing speed of the victim-initiated server.

2) Anomaly-based Detection: The AD's capacity to identify new attacks has drawn the attention of numerous academics. Identifying network behavior serves as the foundation for detection. The predefined behavior and the network behavior conform. After that, it is approved or rejected, which causes the anomaly detection event. The network administrators' specifications can be used to prepare for or teach accepted network behavior. The primary benefit of AD over signature-based engines is its ability to identify new attacks without signatures if they deviate from typical traffic patterns[14].

proposed a system that combines intrusion detection techniques, merging entropy-based systems with anomaly detection to provide multilevel distributed denial of service by first allowing the user to pass through the router in the network site, incorporating a detection algorithm to identify legitimate users.It then passes through a router installed in a cloud site to incorporate a confirmation algorithm that looks for a threshold value; if the value is exceeded, the user is deemed appropriate; if not, an attacker has been discovered in the environment[15].

presented a DDoS attack detection and mitigation (DaMask-D and DaMask-M) architecture that combines a highly customizable network monitoring system to facilitate attack detection with a versatile control framework for quick and targeted attack response. They have also suggested an attack detection method based on graphic models that can address the issue of dataset shift. Based on real-world network traffic, the simulation results demonstrate that the attack detection system can properly report various threats with an accuracy of 89.3%, and the architecture can effectively and efficiently manage the security concerns provided by the new network paradigm[16].

4. AI-based Techniques

several artificial intelligence-based approaches and methods are mentioned below which researchers use in order to identify Distributed Denial of Service attacks on cloud computing, for example, machine learning, Artificial Neural Networks, and Deep Learning algorithms[17].

5. Machin Learning

In recent years, machine learning (ML) has permeated most scientific areas, it comprises a wide range of modeling tools and algorithms used for a wide variety of data processing tasks. Iin the context of DDoS attacks detection machine learning algorithms has proved its ability t detect various DDoS, Naive Bayes, Decision tree, K-Mean Clustering, C4.5, Support Vector Machines, k-nearest Neighbors, and Random Forest; are among the used algorithms[18].

Naïve Bayes algorithm NB is a Bayesian probabilistic machine learning model that computes the likelihood an input falls into a specific class based on the assumption that features are independent of one another.

Decision tree DT is among the most popular and widely used classification algorithms that make predictions using a “decision tree” which represent decisions and their potential outcomes that

resembles a tree, operates by recursively dividing the data into subsets according to the most important attribute at each tree node[19].

Random Forest RF is A popular machine-learning approach that aggregates the output of several decision trees to produce a single outcome. Its versatility, ease of use, and ability to handle both regression and classification problems have driven its popularity.

Support Vector Machines SVM is the most popular method for machine learning tasks to solve both classification and regression tasks; SVMs are especially well-suited Binary classification tasks, which divide a data set's items into two groups[20].

A work by was accomplished in the owncloud environment. Employing an intrusion detection system to create a new dataset and Tor Hammer as an attacking tool. This work uses various machine learning algorithms: SVM, Naïve Bayes, and Random Forest. All algorithms considered, the SVM algorithm reached the best accuracy, while Random Forest and Naïve Bayes reached 97.6% and 98.0%, respectively[21].

Comparing the efficiency of two machine learning algorithms, they discussed that regarding the fact that a million packets are sent towards the destination end by DDoS attacks, they decided to target just one cloud-based website. After the attack is confirmed, the website is taken offline. They performed pre-processing and a "discretize" filter analysis on the data that had been trained using the most popular tool, Weka. Within a single platform, they compared using two different algorithms. After extensive analysis, they concluded that naïve Bayes outperforms random forest[22].

suggested two methods. The NSL-KDD dataset is the dataset's source; the first employs a filter method called Learning Vector Quantization (LVQ), and the second uses a dimensionality reduction method called Principal Component Analysis (PCA). The features that were chosen from each strategy are classified using Naïve Bayes (NB), Support Vector Machine (SVM), and Decision Tree (DT), and the outcomes are compared concerning how well they can detect DDoS attacks. The findings indicate that the LVQ-based DT approach outperforms the others in terms of attack classification. Where the accuracy of each model comes as follows:

LVQ-NB: 91.97%, LVQ-SVM: 92.88%, LVQ-DT: 98.74%, PCA-NB: 87.21%, PCA-SVM: 98.47%, PCA-SVM: 98.47%, PCA- DT: 98.60 %[23].

strengthened the system's defenses against denial-of-service attacks by introducing the DDOS attack and a countermeasure. They discussed that many hosts are accustomed to delivering millions or even trillions of packets in an attempt to cause a distributed denial of service attack against cloud-based websites. They used machine learning algorithms, such as Random Forest and Naive Bayes, for detection and mitigation, concluding that the NB algorithm outperforms RF with 97.05% accuracy[24].

6. Deep Learning

The limitations of traditional DDoS attack detection methods are overcome by deep learning algorithms, which produce good results. These algorithms are highly suitable for identifying DDoS attacks in cloud environments because they can automatically discover intricate patterns and relationships in data.in this section, we will provide a broad understanding of deep learning from the simplest concepts (ANN) to the most complex ones (hybrid) and how it is used in

detecting DDoS attacks in cloud computing[25].

Artificial Neural Networks (ANN) are brain-inspired algorithms used to foresee problems and model complex patterns, artificial neural networks, or ANNs, are the simplest type of deep learning technique[26].

Backpropagation Artificial Neural Networks BP-ANN: Backpropagation It is the process of adjusting a neural net's weights in accordance with the error rate—or loss—obtained in the preceding epoch (i.e. iteration.) Lower error rates are guaranteed by carefully calibrating the weights, which also increases the model's generalizability and reliability. Multilayer perceptron MLP Multilayer perceptron Represent the simplest form of neural network as it contains three fully connected layer input, hidden, and output layer, MLP typically consist of few hidden layer (below six), as the network gets bigger the term Deep neural Network DNN introduced

Convolutional Neural Networks CNNs: CNNs are frequently used for image processing but can also be used for DDoS detection in network traffic analysis as Their effectiveness in spotting patterns suggestive of DDoS attacks stems from their ability to automatically and adaptively learn spatial hierarchies of characteristics from network traffic data[27].

Recurrent Neural Networks (RNNs): particularly useful for DDoS detection since they can handle data sequences such as packets or network traffic flows and retain lengthy dependencies, especially when equipped with Long Short-Term Memory (LSTM) units[28].

Deep Belief Networks (DBNs): a class of deep neural networks composed of multiple layers of stochastic, latent variables that can learn to probabilistically reconstruct the inputs, making them useful for feature extraction and anomaly detection in network traffic data.

Autoencoders: an approach to neural networks where the input is first encoded into a lower-dimensional space and subsequently decoded back, By learning a representation of typical traffic and spotting deviations, autoencoders can be used for unsupervised learning, which aids in detecting anomalies in network traffic[29].

Hybrid Models: Combining different types of neural networks, such as CNNs with RNNs, to leverage the strengths of each in processing and analyzing network traffic. Hybrid models can capture spatial features (through CNNs) and temporal dependencies (through RNNs or LSTMs) in network traffic, enhancing the detection of complex DDoS attack patterns[29].

outlined the usage of a back propagation neural network equipped with a trained model named Cloud Protector to identify and block such attack traffic. They obtained 91% and 88% results for training and testing datasets, respectively. The outcomes demonstrate that the suggested approach can quickly identify most attack messages[30].

Compared the use of different machine learning algorithms (DT, KNN, NB) with the Deep Neural Network model, their result showed that the DNN model outperforms machine learning algorithm in the context of the accuracy of detecting Distributed Denial of Service attacks on the cloud-based networks as the DNN model reach proximally 96% accuracy[31].

recommended using a deep neural network (DNN) as a deep learning model to identify DDoS attacks on a sample of packets taken from network traffic. This is because the DNN model can operate rapidly and accurately even on small samples, thanks to its self-updating layers that incorporate feature extraction and classification processes. The outcome demonstrates that the DNN model has a

99.99 percent success rate in detecting DDoS attacks and a 94.57% accuracy rate in classifying the different types of attacks. They show that the deep learning model may be utilized effectively to counter DDoS attacks, as evidenced by the high accuracy values obtained[32].

The author addressed a novel application layer DDoS attacks by examining the properties of incoming packets, such as the size of HTTP frame packets, the number of IP addresses sent, the number of ports that are constantly mapped, and the number of IP addresses that use proxy IP. They examined client behavior in public attacks using CTU-13, real weblogs from the company, standard datasets, and experimentally constructed datasets from DDoS attack tools like Slow Lairs, Hulk, Golden Eyes, and Xerex. They assessed the efficacy of metrics-based attack detection using MLP[28]. According to simulation data, the suggested MLP classification algorithm detects DDoS attacks with a 98.99 percent accuracy rate. They claim that the effectiveness of the method they suggested yielded the lowest number of false positives compared to several machine learning algorithms[17].

Deep learning algorithm, in general, proposed a new approach to extracting various sequence patterns from the recorded data and examining the high-level characteristics of DDoS attacks, especially for LSTM since they can handle data sequences compared the use of the three different deep learning algorithms namely Convolutional Neural Networks, Long Short-Term Memory[33], and Multilayer perceptron on two datasets KDD Cup, NSL-KDD and real-time data the result came as

KDD Cup-MLP: 82%, KDD Cup-CNN:97.63%, KDD Cup-LSTM: 99.09%,

NSL-KDD -MLP:73.32%, NSL-KDD -CNN:88%, NSL-KDD -LSTM:93.29%

Real-data- MLP:69.32, Real-data- CNN:91%, Real-data- LSTM:95.66

These results demonstrate that the LSTM outperformed the MLP and CNN models on all datasets.

Even more compared the LSTM model with Artificial neural network and convolutional neural network by testing it on datasets collected by them, the LSTM model outperformed both algorithms with 98% accuracy while CNN and ANN reached 97% and 85% respectively[34].

Also designed a deep learning-based model to protect a Fog network from DDoS attacks. They chose LSTM to train on the Hogzilla dataset and tested on real-time DDoS attacks, showing 98.88% accuracy on the testing data set[35].

To our knowledge introduced the first hybrid model tackling the problem of DDoS attack detection in a cloud computing environment, combining an artificial bee colony with a back propagation neural network. The minimal mean square error is used by the Artificial Bee Colony to determine the weights and thresholds. The Back Propagation Artificial Neural Network is also initialized using these weights and thresholds. They demonstrate that this approach increases speed and accuracy without providing numerical values[36].

They designed a hybrid model with optimized Autoencoder and DNN architecture to classify DDoS attacks. First, they build a naïve-AE- DNN model as a baseline model by randomly tuning the hyperparameter values. An optimized AE and DNN model was produced by further refining this baseline model. Sparsity, unit norm, orthogonality, and hyperparameter optimization via Grid search are some enhancements made to the basic AE that

have produced optimized AE that has shown promise in generating useful latent representation to improve classification results. They illustrate that this approach outperformed other state-of-the-art approaches for DDoS detection over the NSL-KDD dataset by giving an accuracy of 98.43% and 98.92% For CICIDS 2017[37].

Hybrid Taylor-Elephant Herd Optimization based Deep Belief Network (TEHO-DBN), constructed by as they modified the Elephant Herd Optimization (EHO) with the Taylor series and the Deep Belief Network (DBN) is trained for the detection of DDoS attacks using this method. The simulation result showed that the proposed hybrid classifier had improved performance with a maximum accuracy of 83% and 89.6% detection rate with 5.6 seconds computational time[38].

Discussed using a hybrid model consisting of a deep learning algorithm with a machine learning algorithm. They presented two hybrid models: the first consists of Deep Belief Networks combined with Decision Tree DBN-DT, and the second is a combination of Deep Belief Networks and Support Vector Machines DBN-SVM applied to DDoS attack detection in a cloud environment; the two models tested on CICDDoS2019 dataset yield accuracy of 99.75% and 98.5% respectively[39].

Another hybrid model proposed by combines a Deep Belief Network with the Gated Recurrent Unit (DBN-GRU), with hyperparameters tuned and optimized using the Probability of Fitness-based Billiards-Inspired Optimization (PF-BIO) algorithm[40]. The proposed model achieves an accuracy of 97.05% in detecting DDoS attacks[41].

Radial Basis Function (RBF) networks, a type of ANN commonly used for function approximation, pattern recognition, and classification tasks, combined RBF with LSTM To improve the overall security of cloud computing infrastructures to detect and mitigate DDoS attacks. With the CICDDoS2019 dataset, the accuracy is tested to be about 99.95%[42].

tackled the detection of DDoS attacks by training Deep Stacked Autoencoder DSA with their proposed optimization algorithm named GHLBO, which is a combination of Gradient Descent and Hybrid leader-based optimization algorithm HLBO, the proposed DSA-GHLBO model tested on two datasets BOT-IoT and NSL-KDD the accuracy was 91.7% and 91.4% with 2.676 sec computational time[39].

Deep Defend framework was introduced by as a unique solution for detecting and mitigating DDoS in cloud computing environments. Integration of advanced machine learning and deep learning techniques is proposed, which makes it possible to quickly and accurately identify possible attacks[43]. They used CNN-LSTM-Transformer for entropy projection, genetic algorithms for data pre-processing optimization, and AutoCNN-DT for real-time attack prediction, which significantly enhanced the efficiency of the DDoS detection process. Furthermore, decreasing detection times has been made possible by the CNN+DT model's integration of an auto encoder (AE)[44].

7. DDoS Attack Mitigation Techniques

On top of detection, creating efficient mitigation solutions is critical to help reduce the impact of DDoS attacks on cloud systems. Traffic filtering, rate limitation, and IP blocking are a few of the often employed DDoS attack mitigation strategies. However, these traditional models might need to be revised to address advanced DDoS attacks in cloud environments[45]. The mitigation of DDoS attacks has also been investigated with deep learning algorithms Through the development of

more focused mitigation techniques, as these methods can adapt to new attack patterns[46].

Employed a method to filter the requested message at several stages. First, the request client IP was compared to a suspicious IP previously stored in Traceback. Next, cloud Defender was used to detect DDoS attacks on HTTP, DDoS attacks using coercive parsing, and DDoS attacks using XML. Cloud Defender first detects attacks by first recognizing suspicious messages[47].

investigated the effectiveness of a cloud trace back (CTB) model utilizing a back propagation neural network to combat Distributed Denial of Service (DDoS) attacks and discovered that the model works well against such attacks[12].

Using the open-source Eucalyptus platform, a private cloud model was implemented by. The three nodes were equipped with virtual machines-based intrusion detection systems (VMs-based IDS) and a MySQL database used to collect data. The front-end server was installed and configured with graphical interfaces for monitoring alerts. Reviewing every signal the VM-based intrusion detection system has collected following a string of DDoS attacks launched against it[33].

An Entropy System with an Anomaly detection System for providing multilevel Distributed Denial of Service (DDoS) was used to detect DDoS attacks, and a third-party monitoring system was involved When an attack happens in the environment, it sends a notification message to the client and advisory report to Cloud Service Provider (CSP)[13].

provide a DDoS attack mitigation architecture (DaMask-M) that combines a highly configurable network monitoring system to detect attacks and a customizable control framework to enable targeted and quick attack response [13]. While and adopted a monitoring approach (OpenStack's firewall and raw socket programming monitoring network, Packet traceback approach based on third-party monitoring, respectively) for mitigating DDoS proposed a novel Source-based DDoS defense mechanism to mitigate DDoS attacks in fog environments and cloud environments using a software-defined network (SDN), which must have the SDN controller implement the DDoS defender module in order to identify unusual DDoS attack activity at the network/transport level[16].

They have presented the "DeepDefend" framework as a cutting-edge method for identifying and mitigating DDoS attacks in cloud computing. They claimed that the incorporation of cutting-edge deep learning and machine learning techniques makes a remarkable framework as its goal is to stop DDoS attacks by anticipating entropy and spotting possible dangers instantly, allowing for quick mitigation measures[17].

hile other researchers focus solely on detecting DDoS attacks, early and accurate detection is a crucial step in enhancing cloud securit.[34] .

8. Performance Comparison

In this section, we will provide an in-depth analysis of the selected papers based on the dataset they used, the detection technique, the mitigation technique, and the best accuracy. The tabular comparison illustrated in as shown in Table (2).

9. Dataset

In machine\deep learning model training, choosing the right dataset is a crucial step as each data can fit or not specific model architecture besides considering the number of classes and the overall quality of the chosen dataset as the number of classes defines the model generalization against different DDoS attacks.

Some papers should have mentioned how the data

is collected or used log data collected using tools like SNORT or OpenStack, especially for the papers that used traditional detection techniques.

The KDD Cup dataset and CICDDoS are the most used datasets according to the selected works. Many researchers mentioned using these datasets; in Table (2), we only mentioned the dataset with which the chosen model performs better. as shown in Figure (3) provides a visualization of the chosen datasets.

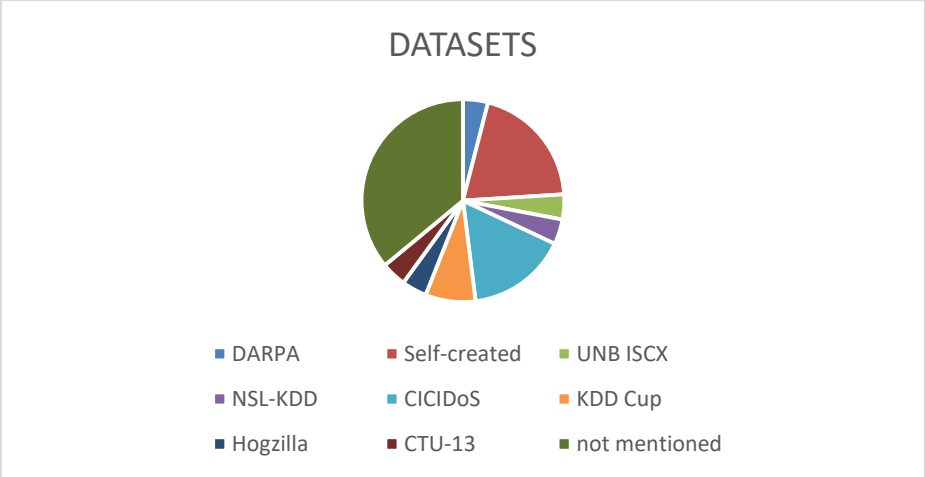

Figure (3): Datasets

10. Detection and Mitigation Techniques

Detecting DDoS attacks is a crucial step in cloud security, which encourages researchers around the globe to develop and investigate every detection technique that can be used to enhance cloud computing security, from traditional statistical and preanalytical ways to advanced AI techniques. According to our search, the first involves AI for detecting DDoS attacks in the cloud using back-propagating ANN with cloud traceback mitigation in 2012. since then, many machine learning algorithms such as Naïve Bayes, Random Forest, and SVM have been used for the same purpose Also, deep learning algorithms have proven their ability in many use cases; researchers have not only used a single deep learning algorithm but also combined multiple algorithms to take the advantages of every strength point of different algorithm as most of the works used a hybrid model. Especially for articles that used deep learning algorithms focused on detecting DDoS attacks without providing mitigation techniques, the strength of these techniques lies in the early detection and the system's ability to classify traffic and potentially initiate responses to identified attacks.

11. Accuracy

In this review, we analyzed advancements in DDoS attack detection techniques across 26 studies, considering only accuracy as a comparison measure, where accuracy is a measure of how the proposed model will perform, given by equation (1).

$$\boldsymbol{Accuracy = \frac{TP+TN}{TP+FP+TN+FN} x100\%} \quad \textbf{(1)}$$

Referring to the accuracies in Table 2, a substantial range in detection accuracy from 83% to 99.99% revealed. The highest accuracy reported by using a Deep Neural Network (DNN) on the CICDDoS dataset, demonstrating the effectiveness of deep learning approaches in accurately identifying DDoS attacks, while hyberd model showed a high accuracy levels on average of

97.68% except for, the lowest accuracy observed using Hybrid TEHO-DBN on the KDD Cup dataset underscores the challenges in detection accuracy potentially due to dataset complexity or methodological limitations [37].

In context of machine learning Random Forest algorithm reached the best accuracy (99.76%). These results provide an example of DNN model usage and hybrid schemes for detection boosting [48] which implies the importance of algorithm evolvement and dataset selection for effective detection as shown in Figure (4).

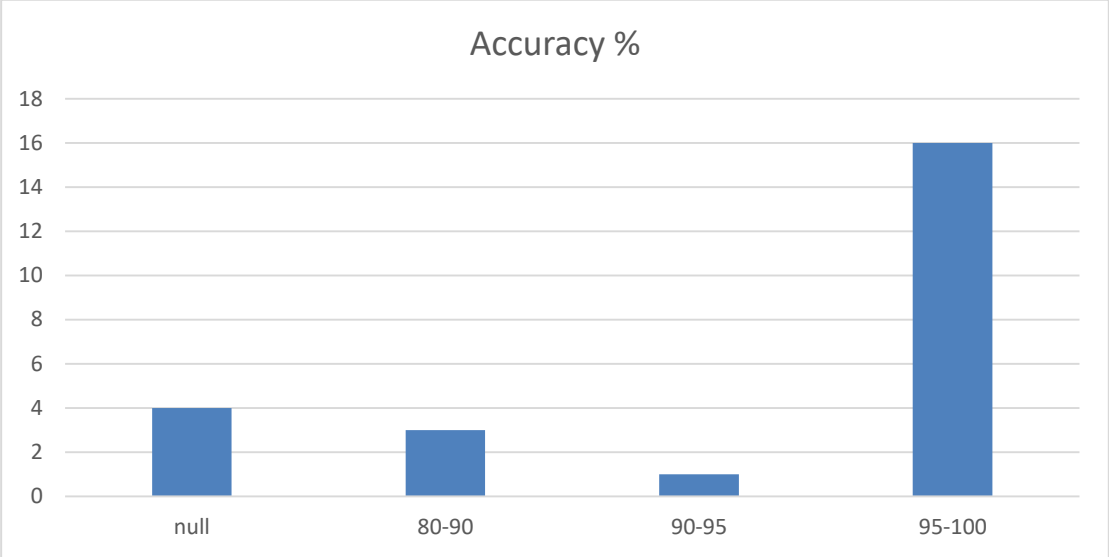

Figure (4): Accuracy rates

Table (2): is a detailed illustration of the selected papers

REFERENCE	DATASET	DETECTION TECHNIQUE	MITIGATION TECHNIQUE	ACCURACY
[12]	-	Signature-based	IP TRACEBACK	-
[33]	DARPA	BP-ANN	Cloud Trace Back (CTB)	88%
[16]	-	Anomaly detection	Third-party monitoring	-
[13]	Self-created dataset	Signature-based	Alert monitoring	97.33%
[14]	-	Signature-based	CBF Packet Filtering	-
[18]	UNB ISCX	anomaly detection module (DaMask-D)	attack reaction module (DaMask-M)	89.30%
[35]	-	ABC-BP-ANN	-	-
[22]	Self-created dataset	SVM	-	99.7%

[23]	Self-created dataset	Naïve Bayes, Random Forest	-	-
[34]	OpenStack generated	DNN	monitoring network	96%
[49]	-	‘‘Cloud Warrior” mechanism	on based PTB third-party	97.4%
[24]	NSL-KDD	LVQ-DT	-	98.74%
[38]	CICIDoS	SAE-DNN Hybrid	-	98.92%
[37]	KDD Cup	Hybrid TEHO-DBN	-	83%
[50]	KDD Cup	LSTM	-	99.09%
[44]	CICDDoS	DBN-DT Hybrid	-	99.75%
[48]	-	Random Forest	-	99.76%
[36]	CICDDoS	DNN	-	99.99%
[42]	Hogzilla Dataset	LSTM	SDN controller	98.88%
[47]	CICDDoS	-RBF Hybrid LSTM	-	99.95%
[41]	Self-created dataset	LST	-	98%
[39]	CTU-13 dataset	MLP	-	98.99%
[40]	-	Hybrid DBN-GRU	hybrid learning-based classifier	97.05%
[51]	-	DSA- GHLBO	-	91.7%
[43]	CIDDS	CNN-LSTM-Transformer	DeepDefend framework	-
[25]	-	Naive Bayes	NB and RF	97.05%

12. Challenges and Recommendation

12.1 Challenges

1) DDoS Evolution: the fast evolution of DDoS attack techniques remains a considerable issue as attackers continuously designing new strategies to bypass the existing security measures, which makes it challenging to overcome all DDoS attacks.
2) Scalability: With the rapid expansion of cloud computing systems, ensuring that DDoS detection and mitigation strategies can scale effectively to handle large volumes of data and high network traffic is challenging.
3) Integration: Integrating advanced DDoS detection and protection mechanisms with existing cloud services without altering

performance or user experience is a complex task.

4) FP and FN: Minimizing false positives where legitimate traffic is identified as malicious and false negatives where malicious traffic is not discovered in detection systems remains a critical challenge, affecting the reliability of DDoS defenses.
5) Resource Limitations: Certain DDoS mitigation solutions need a lot of resources, which might result in a decrease in cloud service availability, which can affect system performance and user experience in general.

12.2 Recommendation

1) Adoption of AI: Implementing AI and machine learning algorithms can enhance both the accuracy and efficiency of DDoS detection systems by learning from past attacks and the ability to adapt to new threats.
2) Hybrid Detection Approaches: leveraging the strengths of more than one algorithm, which can lead to better detection for both previously known and new DDoS attacks to overcome new DDoS strategies.
3) Enhanced Collaboration: Businesses, cybersecurity groups, and cloud service providers should work together more closely to share best practices and threat intelligence in order to strengthen defenses against DDoS attacks.
4) Regular System Updates: Security audits and routine detection and mitigation system updates can help find vulnerabilities and make sure defenses are resilient against new DDoS attack.
5) User Awareness: Reducing attacks that take advantage of human behavior or insecure equipment can be achieved in large part by educating users about the dangers of DDoS attacks and encouraging best practices for security.

13. Contribution

Iin this paper we tried to offer in-depth analysis of DDoS attack history, types, and technology evolution meant for detection and mitigation in a special interest to cloud computing. by comparing the processes from outdated forms to intelligent AIs so as to provide a clear distinction of diverse approaches in terms of the relative performance on various models, datasets and scenarios. This paper puts these issues in the context of information security and reveals how evolving attack vectors, scalability, integration of cloud services, and the trade-offs between detection accuracy and resource limitations are the main issues with information security. Propositions comprise the following: technological adoption of AI and machine learning, a combination of multiple systematic detection methods, elimination of communication barriers, implementation of timely system updates and audits, and constant user awareness.

Finally, the paper provides a good insight into DDoS attacks in the cloud, revealing how significant these attacks have triggered the research and developments. It recommends an all-round approach that integrates world-class technologies, collaboration, and education to secure cloud computing infrastructures in the face of emerging DDoS threats.

14. Conclusion

Our detailed analysis of the progress in DDoS detection and mitigation techniques in cloud computing environments underlines the urgent need to keep improving the security measures alongside the growing complexity of DDoS

attacks. Additionally, this analysis reveals that there has been a considerable "move" toward the use of AI and machine learning algorithms to enhance both accuracy and efficiency; as our research shows, technological advancement is not the exception but also the rule that reveals the current challenges raised by the dynamism of DDoS attacks, such as scalability, integration, and newly emerging mechanism.

15. References

[1] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The characteristics of cloud computing," in 2010 39th International Conference on Parallel Processing Workshops, IEEE, 2010, pp. 275–279.

[2] J. C. R. Licklider, "Intergalactic computer network," ARPA. http://imiller. utsc. utoronto. ca/pub2/licklider_intergalactic_1963. pdf, 1963.

[3] U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi, and N. Albaqami, "Cloud security threats and solutions: A survey," Wireless Personal Communications, vol. 128, no. 1, pp. 387–413, 2023.

[4] A. C. Tricco et al., "PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation," Annals of internal medicine, vol. 169, no. 7, pp. 467–473, 2018.

[5] "CSA Warns Providers of 'The Notorious Nine' Top Threats." Accessed: Apr. 01, 2024. [Online]. Available: https://cloudsecurityalliance.org/press-releases/2013/02/25/ca-warns-providers-of-the-notorious-nine-cloud-computing-top-threats-in-2013

[6] K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica, "Taming IP packet flooding attacks," ACM SIGCOMM Computer Communication Review, vol. 34, no. 1, pp. 45–50, 2004.

[7] K. E. Braathen and S. Salte, "Threat to information security: the system vulnerability and denial of service attacks." Høgskolen i Agder, 2004.

[8] A. Toh, "Azure DDoS protection—2021 Q3 and Q4 DDoS attack trends." Microsoft, 2022.

[9] A. S. Olufikayo and W. Sakpere, "INTRUSION DETECTION IN CLOUD NETWORK ENVIRONMENT: A MULTILAYER PERCEPTRON MODEL".

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

[11] P. Szynkiewicz, "Signature-Based Detection of Botnet DDoS Attacks," in Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools, Springer, 2022, pp. 120–135.

[12] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE, 2012, pp. 1–5.

[13] A. M. Lonea, D. E. Popescu, O. Prostean, and H. Tianfield, "Evaluation of experiments on detecting distributed denial of service (DDoS) attacks in Eucalyptus private cloud," in Soft Computing Applications: Proceedings of the 5th International Workshop Soft Computing Applications (SOFA), Springer, 2013, pp. 367–379.

[14] P. Negi, A. Mishra, and B. B. Gupta, "Enhanced CBF packet filtering method to

detect DDoS attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[15] M. Nooribakhsh and M. Mollamotalebi, "A review on statistical approaches for anomaly detection in DDoS attacks," Information Security Journal: A Global Perspective, vol. 29, no. 3, pp. 118–133, 2020.

[16] A. S. Navaz, V. Sangeetha, and C. Prabhadevi, "Entropy based anomaly detection system to prevent DDoS attacks in cloud," arXiv preprint arXiv:1308.6745, 2013.

[17] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," Computer Networks, vol. 81, pp. 308–319, 2015.

[18] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," Computer Networks, vol. 81, pp. 308–319, 2015, doi: 10.1016/j.comnet.2015.02.026.

[19] X. Wu et al., "Top 10 algorithms in data mining," Knowledge and information systems, vol. 14, pp. 1–37, 2008.

[20] A. Liaw and M. Wiener, "Classification and regression by randomForest," R news, vol. 2, no. 3, pp. 18–22, 2002.

[21] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in Proceedings of the fifth annual workshop on Computational learning theory, 1992, pp. 144–152.

[22] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," in 2019 Amity International conference on artificial intelligence (AICAI), IEEE, 2019, pp. 870–875.

[23] A. Amjad, T. Alyas, U. Farooq, and M. A. Tariq, "Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm," EAI Endorsed Transactions on Scalable Information Systems, vol. 6, no. 23, pp. e7–e7, 2019.

[24] C. Bagyalakshmi and E. S. Samundeeswari, "DDoS attack classification on cloud environment using machine learning techniques with different feature selection methods," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 5, 2020.

[25] Y. Shang, "Prevention and detection of DDOS attack in virtual cloud computing environment using Naive Bayes algorithm of machine learning," Measurement: Sensors, vol. 31, p. 100991, 2024.

[26] J. Zupan, "Introduction to artificial neural network (ANN) methods: what they are and how to use them," Acta Chimica Slovenica, vol. 41, p. 327, 1994.

[27] S. E. Dreyfus, "Artificial neural networks, back propagation, and the Kelley-Bryson gradient procedure," Journal of guidance, control, and dynamics, vol. 13, no. 5, pp. 926–928, 1990.

[28] H. Taud and J. F. Mas, "Multilayer perceptron (MLP)," Geomatic approaches for modeling land change scenarios, pp. 451–455, 2018.

[29] N. Ketkar, J. Moolayil, N. Ketkar, and J. Moolayil, "Convolutional neural networks," Deep Learning with Python: Learn Best Practices of Deep Learning Models with PyTorch, pp. 197–242, 2021.

[30] L. R. Medsker and L. C. Jain, "Recurrent neural networks," Design and Applications, vol. 5, no. 64–67, p. 2, 2001.

[31] G. E. Hinton, "Deep belief networks," Scholarpedia, vol. 4, no. 5, p. 5947, 2009.

[32] D. Bank, N. Koenigstein, and R. Giryes, "Autoencoders," Machine learning for data science handbook: data mining and knowledge discovery handbook, pp. 353–374, 2023.

[33] B. Joshi, A. S. Vijayan, and B. K. Joshi, "Securing cloud computing environment against DDoS attacks," in 2012 International Conference on Computer Communication and Informatics, IEEE, 2012, pp. 1–5.

[34] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud," Procedia Computer Science, vol. 167, pp. 2297–2307, 2020.

[35] U. Ali, K. K. Dewangan, and D. K. Dewangan, "Distributed denial of service attack detection using ant bee colony and artificial neural network in cloud computing," in Nature Inspired Computing: Proceedings of CSI 2015, Springer, 2018, pp. 165–175.

[36] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," Expert Systems with Applications, vol. 169, p. 114520, 2021.

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

[38] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud," IEEE Access, vol. 8, pp. 181916–181929, 2020.

[39] S. Ahmed et al., "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," Future Internet, vol. 15, no. 2, p. 76, 2023.

[40] A. A. Samsu Aliar and M. Agoramoorthy, "An Automated Detection of DDoS Attack in Cloud Using Optimized Weighted Fused Features and Hybrid DBN-GRU Architecture," Cybernetics and Systems, pp. 1–42, 2022.

[41] E. Deniz and S. Serttaş, "Deep learning-based distributed denial of service detection system in the cloud network," Journal of Scientific Reports-A, no. 055, pp. 16–33, 2023.

[42] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 3, pp. 825–831, 2022.

[43] M. Ouhssini, K. Afdel, E. Agherrabi, M. Akouhar, and A. Abarda, "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing," Journal of King Saud University-Computer and Information Sciences, p. 101938, 2024.

[44] İ. İbrahim and S. Kurnaz, "A new distributed denial-of-service detection system in cloud environment by using deep belief networks," Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, vol. 63, no. 1, pp. 17–24, 2021.

[45] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," IEEE Access, vol. 5, pp. 6036–6048, 2017.

[46] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud," in 2018 IEEE international conference on big data and smart computing (bigcomp), IEEE, 2018, pp. 251–256.

[47] M. Amitha and M. Srivenkatesh, "DDoS Attack Detection in Cloud Computing Using Deep Learning Algorithms," International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 4, pp. 82–90, 2023.

[48] A. Mishra, B. B. Gupta, D. Peraković, F. J. G. Peñalvo, and C.-H. Hsu, "Classification based machine learning for detection of ddos attack in cloud computing," in 2021 ieee international conference on consumer electronics (icce), IEEE, 2021, pp. 1–4.

[49] R. Saxena and S. Dey, "DDoS attack prevention using collaborative approach for cloud computing," Cluster Computing, vol. 23, pp. 1329–1344, 2020.

[50] A. V Kachavimath and D. G. Narayan, "A deep learning-based framework for distributed denial-of-service attacks detection in cloud environment," in Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1, Springer, 2021, pp. 605–618.

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