Egyptian Informatics Journal 27 (2024) 100517

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Review Article

Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches

Mohamed Ouhssini [a,*], Karim Afdel [a], Mohamed Akouhar [b], Elhafed Agherrabi [c], Abdallah Abarda [d]

[a] Lab SIV, Department of Computer Science, University IBN Zohr, Agadir, Morocco
[b] Lab Partial Differential Equations, Algebra and Spectral Geometry, University IBN Tofail, Kenitra, 14000, Morocco
[c] LabIRF-SIC, Department of Mathematics, Faculty of Science, Ibn Zohr University, Agadir, Morocco
[d] Laboratory of Mathematical Modeling and Economic Calculations, Hassan First University Settat, Settat, Morocco

ARTICLE INFO

Keywords:
DDoS attacks
Cloud environments
Effective strategies
Systematic review
Cloud security
Defense mechanisms
Machine learning
Security measures
Deep learning

ABSTRACT

This comprehensive study examines cutting-edge strategies for combating Distributed Denial of Service (DDoS) attacks in cloud environments, addressing a critical gap in recent literature. Through a systematic review of the latest advancements, we propose a framework for identifying, preventing, and mitigating DDoS threats specifically tailored to cloud infrastructures. Our research highlights the urgent need for robust defense mechanisms to enhance cloud security, minimize service disruptions, and safeguard against data breaches. By analyzing the strengths and limitations of current models, we underscore the importance of continued innovation in this rapidly evolving field. This study provides essential insights for academics and industry professionals aiming to enhance the resilience of cloud infrastructure against the ongoing and adaptive menace of DDoS attacks.

Contents

[*] Corresponding author.
E-mail address: mohamed.ouhssini@gmail.com (M. Ouhssini).

https://doi.org/10.1016/j.eij.2024.100517
Received 19 March 2024; Received in revised form 23 July 2024; Accepted 30 July 2024
Available online 26 August 2024

1. Introduction

Cloud computing has emerged as a pivotal component in contemporary IT infrastructure, offering significant advantages including scalability, adaptability, and cost-effectiveness through its pay-per-use model. The widespread adoption of cloud-based services has simultaneously made them more susceptible to cybersecurity risks, with DDoS attacks emerging as a particularly serious threat [1,2]. DDoS attacks are defined by their ability to flood target systems with an excessive volume of traffic from multiple distributed sources, leading to potential system failures and significant operational disruptions [3]. These attacks present serious threats to the core principles of information security — availability, integrity, and confidentiality — particularly in cloud services.

The consequences of a successful DDoS attack are diverse and can be highly detrimental. Economically, organizations may face substantial financial losses due to service disruptions and the costs associated with incident response and system recovery [4,5]. Additionally, DDoS attacks can act as a gateway to data breaches, potentially compromising sensitive information and exposing organizations to significant legal and regulatory liabilities. A major concern is the potential for long-term reputational damage; successful attacks can erode user trust and harm an organization's market position by highlighting vulnerabilities in service reliability and security [6,7]. These varied impacts highlight the critical need for robust DDoS mitigation strategies in cloud environments.

DDoS attacks leverage the anonymity afforded by the internet to circumvent firewalls and intrusion detection systems, rendering them exceptionally resistant to mitigation efforts. These attacks are systematically orchestrated by an attacker who utilizes a network of compromised devices, commonly termed as bots [8] (See Fig. 1). By mobilizing these bots, the attacker inundates the target server with a deluge of fabricated requests, ultimately causing it to fail. To maintain control over the bots, the attacker relies on a central server known as the Command and Control (C&C) server [9,10]. Acting as an intermediary, the C&C server facilitates the transmission of instructions from the attacker to the bots, directing them to initiate the attack by dispatching harmful data packets towards the designated target server.

DDoS attacks can be categorized into three main types: volumetric, protocol, and application layer attacks. Volumetric attacks overwhelm the target's network capacity by flooding it with traffic. Protocol attacks exploit vulnerabilities in network and transport layer protocols to deplete server resources. Application layer attacks focus on exhausting the resources of specific applications by targeting their vulnerabilities [12,13].

The landscape of DDoS attacks is evolving in concerning ways, according to recent data. Although attacks are generally becoming shorter in duration, they are simultaneously growing more intense and sophisticated. A notable milestone was reached in the latter half of 2023 when the peak intensity of DDoS attacks surged to an unprecedented 1.6 Tbps, effectively doubling the previous high of 800 Gbps. This dramatic increase in attack strength represents a significant escalation in the potential for digital disruption and damage. Furthermore, the data highlights the prevalence of UDP flood attacks, which account for 62% of all DDoS incidents, indicating this method's popularity among malicious actors [14].

Moreover, the landscape of DDoS threats is constantly evolving due to the increasing utilization of artificial intelligence (AI) and the widespread adoption of Internet of Things (IoT) devices. AI-powered attacks present a particularly troublesome problem, as they can mimic legitimate network traffic, making detection and mitigation more challenging. The surge in IoT malware, which saw a 37% increase during the first half of 2023, indicates a rise in potential avenues for cyberattacks. This issue is further exacerbated by the extensive addressing capabilities of IPv6 [15].

Businesses face significant financial consequences due to DDoS attacks, with costs varying greatly depending on the size of the business. Small-to-medium-sized businesses can expect an average cost of 52,000 USD per DDoS attack incident, while enterprises may face an average cost of 444,000 USD [16].

The escalating threat of DDoS attacks necessitates innovative and adaptable detection methods that enhance service availability, efficiency, and accuracy while minimizing overhead, boosting flexibility, reducing recovery time, and maintaining a low false positive rate. Although advancements in networking technology are beneficial, they introduce new challenges concerning trust, privacy, availability, and security. To safeguard the availability of networking resources, it is crucial to implement mitigation strategies that include multi-level validation and the identification of compromised elements such as applications, flow rules, and controllers. These strategies are essential components of a robust DDoS defense mechanism.

Current methodologies for detecting, preventing, and mitigating DDoS attacks in cloud environments are limited, necessitating the development of more effective strategies. This study addresses this urgent need by highlighting a significant gap in the literature, which stems from a lack of recent comprehensive reviews on the subject. The research aims to fill this gap by proposing a systematic review that provides a precise framework for identifying, preventing, and mitigating DDoS threats, with a primary focus on enhancing cloud security and minimizing the risks of service downtime and data breaches.

The research focuses on recent advancements in DDoS defense, specifically examining papers published between 2020 and 2024. The core objective is to provide an in-depth review of defense mechanisms designed for cloud infrastructures to combat DDoS attacks. It also encourages future investigations to explore deploying state-of-the-art machine learning techniques and integrating proposed systems with existing security measures, aiming to significantly bolster cloud security.

This study offers insights into the effectiveness of using Machine Learning (ML) and Deep Learning (DL) methodologies, along with other recent techniques, for detecting, preventing, and mitigating DDoS attacks in cloud environments. It discusses the advantages and challenges of various proposed models, emphasizing the need for further studies and advancements in this area.

Furthermore, the lack of recent article reviews on DDoS attack detection, prevention, and mitigation in cloud environments underscores the relevance and timely contribution of this research. The following

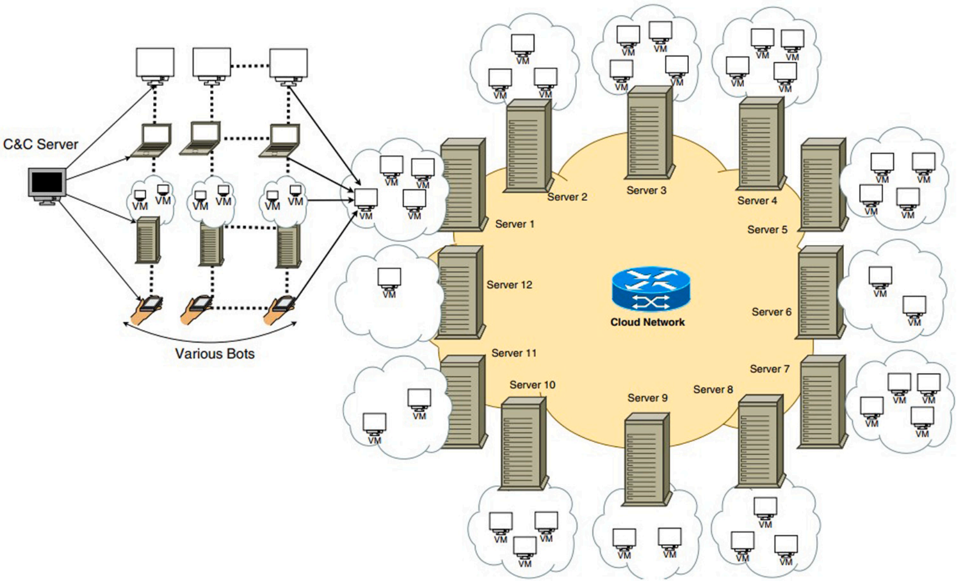

Fig. 1. A DDoS attack scenario in cloud infrastructure [11].

sections will explore the key findings and contributions of this study in the realm of DDoS attack detection in the cloud, with a particular focus on the use of ML and DL techniques. This endeavor aims to provide a comprehensive understanding of this crucial aspect of network security, highlighting the critical role of advanced technologies in safeguarding modern cloud-based services and addressing a significant gap in current scholarly discourse.

This paper is organized as follows: Section 2 examines the DDoS threat landscape in cloud computing, covering attack types, recent statistics, and impacts. Section 3 details the systematic literature review methodology. Section 4 summarizes key findings on detection, prevention, and mitigation strategies. Sections 5 and 6 analyze deep learning and traditional machine learning techniques for DDoS defense, respectively. Section 7 explores alternative defense approaches. Section 8 identifies research gaps and future directions. Section 9 concludes the paper, summarizing main findings and implications of this systematic review on cloud-based DDoS defense.

2. Navigating the DDoS threat landscape in cloud computing: Types, statistics, and consequences

DDoS attacks in cloud environments present significant risks to the availability and performance of cloud services, affecting both providers and users alike. This section delves into recent statistics, different attack types, and the consequences of DDoS attacks.

2.1. Recent statistics about DDoS attacks

Recent statistics on DDoS attacks show a significant rise in activity. In the last quarter of 2023, Cloudflare's systems blocked over 5.2 million HTTP DDoS attacks, most of which ended within 10 min and peaked below 500 megabits per second [17]. The report also indicates a 117% year-over-year increase in network-layer DDoS attacks, especially targeting retail, shipping, and public relations websites during Black Friday and the holiday season [18]. Additionally, Kaspersky reported nearly 57,116 DDoS attacks in 2024, showing a 67% rise in ransom DDoS attacks [19].

The summary Table 1 of the largest DDoS attacks spanning from 2018 to 2023 highlights the growing scope and complexity of cyber threats over time. It shows a progression from large volumetric attacks, peaking with the 1.35 Tbps attack on GitHub in 2018, to more sophisticated and multi-faceted attacks targeting various sectors like cloud services and the technology industry. The evolution of these attacks is evident in their increasing scale, such as the 2.3 Tbps attack on Amazon AWS in 2020, and the diverse tactics used by attackers. The table also reveals a rising trend in the frequency and intensity of attacks, with significant figures like 800 Gbps and 8.7 million requests per second reported in 2023, underscoring the continuous advancement of DDoS attack capabilities and the ongoing challenge for cybersecurity defense.

Table 1
The largest DDoS attacks recorded (2018–2023).

Year	Size	Type	Target
2018	1.35 Tbps	Volumetric	GitHub
2018	11.2 Gbps	Volumetric	Cloud services
2020	2.3 Tbps	Volumetric	Amazon AWS
2020	500 Gbps	Volumetric	Technology sector
2021	38 Gbps	Multi-vector	Technology sector
2022	26 million requests/s	–	–
2023	Up to 800 Gbps	–	–
2023	8.7 million requests/s	Network-layer	Cloudflare

2.2. Types of DDoS attacks

DDoS attacks can be broadly categorized into several types, each targeting different components of the cloud infrastructure:

1. **Volume-based Attacks:** These aim to saturate the bandwidth of the target, using techniques like UDP floods, ICMP floods, and other spoofed packet floods [20].
2. **Protocol Attacks:** These target network layer or transport layer protocols to consume server resources or the resources of intermediate communication equipment, such as firewalls and load balancers [21].
3. **Application Layer Attacks:** Focused on web applications, these are more sophisticated, aiming to exhaust the resources of the application servers [22].

Notably, the Economic Denial of Sustainability (EDoS) attack is a subclass that specifically targets the cloud's billing model, aiming to inflate the costs by abusing the auto-scaling feature of cloud services [23].

2.3. Direct and indirect impacts of DDoS attacks

Direct Impacts:

1. **Service Disruption:** The most immediate impact is the unavailability of services for legitimate users, which can lead to significant downtime [24].
2. **Financial Losses:** For businesses relying on cloud services, downtime can result in substantial financial losses due to interrupted operations and lost business opportunities [25].
3. **Resource Exhaustion:** DDoS attacks consume vast amounts of resources, leading to degraded performance for legitimate users and increased operational costs for cloud service providers [26].

Indirect Impacts:

1. **Reputation Damage:** Frequent or high-profile attacks can damage the reputation of businesses, eroding customer trust and potentially leading to a loss of customers [27].
2. **Increased Operational Costs:** Organizations may need to invest in advanced security measures and infrastructure upgrades to defend against DDoS attacks, increasing operational costs [28].
3. **Legal and Regulatory Implications:** Businesses may face legal and regulatory repercussions if they fail to protect user data and ensure service availability [29].

In summary, a multi-layered approach to security is essential for protecting against DDoS attacks in cloud computing environments. By implementing network layer protection, application layer protection, traffic management, monitoring and analytics, and incident response planning, businesses can effectively detect and mitigate DDoS attacks and minimize the impact on their operations.

3. A methodical approach to conducting a systematic literature review

A Systematic Literature Review (SLR) is a structured method for examining research questions by analyzing existing studies. This approach, as outlined by [30], forms the basis of our study on detecting, preventing, and mitigating DDoS attacks in cloud computing. We focus on recent techniques like deep learning and machine learning, reviewing research from 2020 to 2024. The SLR method is valuable because it systematically gathers research articles to identify gaps in current knowledge, guiding future research.

This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. These steps include:

1. Searching literature using relevant databases and keywords
2. Selecting studies based on specific criteria to ensure quality
3. Extracting data on key findings, limitations, and methods
4. Synthesizing data to summarize insights

The process concludes with theoretical and practical recommendations based on the reviewed literature. Fig. 2 shows the survey protocol, illustrating the SLR process and providing a solid foundation for advancing cloud security knowledge.

3.1. Research questions

This systematic review addresses critical questions regarding the defense against DDoS attacks within cloud computing environments. The questions are categorized into several key research areas:

RQ1: What are the most efficient and effective strategies for detecting, preventing, and mitigating DDoS attacks in cloud environments, considering factors such as performance, cost, and security?

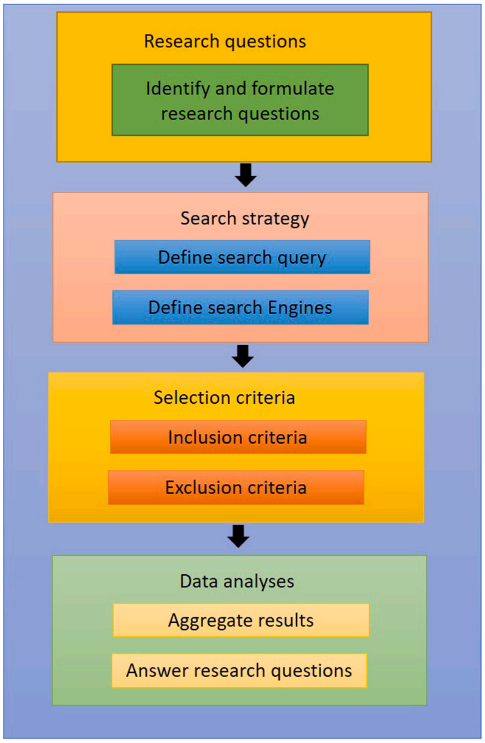

Fig. 2. SLR process.

RQ2: How can cutting-edge technologies like deep learning, blockchain, and machine learning be utilized to enhance the detection, prevention, and mitigation of DDoS attacks in cloud systems?

RQ3: What are the challenges and solutions in achieving real-time detection and mitigation of DDoS attacks in cloud computing, focusing on minimizing false positives and adapting swiftly to evolving attack strategies?

RQ4: In what ways can DDoS defense mechanisms in the cloud be designed to efficiently scale and flexibly adapt to the dynamic nature of cloud resources and the diversity of services offered?

RQ5: What are the primary research gaps in the current literature on DDoS defense in cloud computing, and what future research directions could address these gaps and improve detection, prevention, and mitigation strategies?

Furthermore, the review extends to understand the foundational aspects of current research through additional questions:

RQ6: How are the studies distributed based on countries of origin, journals, publishers, and years of publication?

RQ7: What datasets are commonly used for evaluating existing models in cloud systems?

RQ8: What tools and network simulations are utilized in current studies?

RQ9: Which evaluation metrics and parameters are employed to assess the performance of existing studies?

3.2. Search strategy

In order to gather a comprehensive set of papers related to the topic of DDoS attacks and their detection, prevention, and mitigation in the context of cloud computing, a rigorous search was conducted across several prominent online bibliographic databases. These databases included ScienceDirect, Springer, ACM, IEEE, Google Scholar, and Scopus.

To be precise, the search resulted in the following number of papers:

- ScienceDirect: A total of **1602** papers were obtained from this database.
- Springer: A substantial number of **2850** papers were gathered from Springer.
- Google Scholar: An impressive **17 300** papers were sourced from Google Scholar.
- ACM Library: A total of **575** papers were obtained from the ACM Library.
- IEEE: A total of **776** papers were sourced from IEEE.
- Scopus: A total of **523** papers were gathered from Scopus.

The search query used for this purpose was as follows:

(“DDoS attacks” OR “Distributed Denial of Service attacks” AND (detection OR prevention OR mitigation) AND (cloud OR “cloud computing”)).

This query ensured that the search results were focused on papers that discussed DDoS attacks and their detection, prevention, and mitigation in the context of cloud computing.

3.3. Selection criteria for literature review

In our meticulous selection process, we focused on identifying and evaluating scholarly papers from reputable peer-reviewed journals and conference proceedings. Our interest was specifically in works that address the detection, prevention, and mitigation of DDoS attacks within cloud computing environments. This selection was guided by a set of inclusion and exclusion criteria, meticulously designed to ensure the relevance and quality of the sourced literature.

Inclusion criteria

- **Innovative Approaches:** We prioritized articles that introduced novel methods for detecting, preventing, and mitigating DDoS attacks in cloud settings. These contributions are vital for advancing the field and offering new perspectives on tackling DDoS threats.
- **Relevance to Research Questions:** The study must directly contribute to answering our predefined research questions, ensuring that each selected piece of literature adds value to our investigation and understanding of DDoS challenges in cloud environments.
- **Extension of Previous Work:** We sought out studies that build upon or significantly extend existing research in the field. This criterion helps in piecing together the evolving landscape of DDoS defense mechanisms and their efficacy.
- **Publication Window:** We restricted our review to articles published within the 2020–2024 timeframe, with a focus on the last two years. This specific timeframe guarantees that our review highlights the most recent trends, technologies, and methodologies in combating DDoS attacks, ensuring the information is up-to-date and relevant.

Exclusion criteria

- **Language Limitation:** Articles published in languages other than English were excluded to ensure the clarity and accessibility of the information reviewed.
- **Irrelevance to the Topic:** Any articles that did not specifically address DDoS attacks detection, prevention, and mitigation in cloud computing were excluded to maintain the focus and coherence of our literature review.

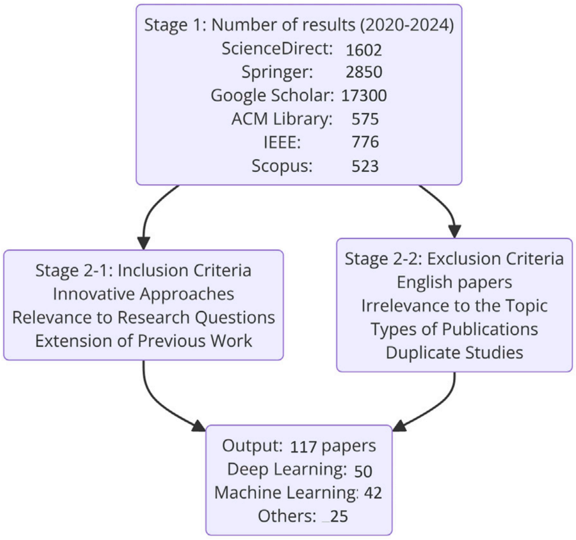

Fig. 3. The process of selection.

- **Certain Types of Publications:** We excluded review articles, editorials, discussion pieces, and data articles, as these often do not present original research findings or are not directly relevant to our investigative scope.
- **Lack of Comprehensive Information:** Articles that failed to provide a sufficient depth of information, either in terms of methodology, results, or discussion, were excluded. This ensures that our review is based on comprehensive and detailed studies.
- **Duplicate Studies:** To avoid redundancy, we excluded studies that were duplicates or offered no new insights compared to previously included research.

Research findings

Upon the completion of our extensive and detailed research process, we identified a total of 117 pertinent papers across various techniques and methodologies aimed at addressing DDoS challenges in cloud environments. These include:

- **Deep Learning Techniques:** We gathered 50 papers that explore deep learning applications for enhancing DDoS attack detection, prevention, and mitigation. These studies highlight the growing importance of advanced AI techniques in cybersecurity.
- **Machine Learning Approaches:** A collection of 42 papers was identified, focusing on machine learning strategies to combat DDoS threats. These works underline the adaptability and effectiveness of machine learning in identifying and countering DDoS incidents.
- **Other Recent Techniques:** Additionally, we found 25 papers discussing various recent methodologies beyond the conventional machine and deep learning approaches. These papers contribute to a broader understanding of the evolving toolkit available for DDoS defense in cloud computing environments.

Fig. 3 provides a succinct overview of the paper selection process, which comprises several stages:

Stage 1: This stage entails retrieving the initial set of search results from various academic databases spanning the years 2020 to 2024. The databases utilized for this search encompass ScienceDirect, Springer, Google Scholar, ACM Library, IEEE, and Scopus.

Stage 2: Stage 2 is further divided into two parts, namely inclusion and exclusion criteria.

Inclusion Criteria: The inclusion criteria prioritize papers that employ innovative approaches, demonstrate relevance to the research questions, and extend upon previous studies.

Exclusion Criteria: The exclusion criteria serve to filter out papers that are not written in English, are irrelevant to the investigated topic, represent undesired types of publications, or duplicate existing studies.

The output of this selection process comprises a total of 117 papers, which are categorized into three groups: Deep Learning (50 papers), Machine Learning (42 papers), and Others (25 papers).

The flowchart illustrates a rigorous paper selection process for the literature review. Initially, titles and abstracts are carefully scrutinized against predetermined criteria, with a focus on contemporary approaches. Papers that pass this initial screening undergo a thorough examination of their full content. This methodical approach ensures the identification of the most relevant and up-to-date literature in the field. This exhaustive review methodology has yielded two significant outcomes. Firstly, it has provided an in-depth exploration of the current landscape of DDoS attack mitigation strategies in cloud environments. Secondly, it has underscored the evolving and complex nature of research in this domain. The process reveals a field characterized by rapid advancements and multifaceted challenges, reflecting the ongoing arms race between cybersecurity professionals and malicious actors in the cloud computing space.

3.4. Data extraction

In this phase of our investigation, we systematically identified and meticulously extracted a comprehensive set of key variables that are crucial for addressing our research inquiries. These variables encompass a wide range of aspects related to scholarly publications, including but not limited to the year of publication, the datasets utilized, the methodologies or computational techniques employed, the advantages or unique strengths of the research approach, the results or findings obtained, identified research gaps or areas necessitating further exploration, the type of publication (whether it is an article or a conference paper), the journal in which the research is published, the publisher, the country of origin, and the tools for simulation and programming languages used. The comprehensive list of variables and their descriptions are outlined in Table 2

The comprehensive list of variables and their descriptions are outlined below

Table 2
The information gleaned from the reviewed sources and their accompanying explanations.

Variable	Description
Publication year	The specific year in which the research was made public and published.
Dataset used	The particular dataset(s) that were utilized in the research, either for the purpose of analysis or testing.
Techniques employed	The methodologies or computational techniques that were applied in the research.
Advantages	The benefits or strengths of the research approach, including any innovative aspects that were incorporated.
Results obtained	The outcomes or findings that were derived from the research.
Research gaps	Any limitations or areas that require further research, as recognized by the study.
Type of publication	The research categorized based on whether it was published as an article or a conference paper.
Journal	The specific journal in which the research was published.
Publisher	The publisher responsible for publishing the research.
Country	The country of origin or location of the research.
Tools of simulation	The specific tools that were used for the purpose of simulation in the research.
Programming languages	The programming languages that were utilized in the research.

3.5. Data reporting

In our analysis, we undertook a comprehensive examination of the literature, utilizing tables, charts, and figures to illustrate the findings in a detailed manner. We focused on various key aspects, Publication Year, Dataset Used, Techniques Employed, Advantages, Results Obtained, Research Gaps, Type of Publication, Journal, Publisher, Country, Tools of Simulation, and Programming Languages used. Each variable offers insight into different dimensions of the research, including the years and datasets involved, the methodologies and outcomes of the studies, their strengths, and areas requiring further investigation.

By integrating quantitative and qualitative data in a coherent manner, our analysis provides a holistic overview of the current state of research in the field. It highlights trends, identifies gaps, and suggests opportunities for future work, offering a structured perspective on the progression and focal points of contemporary studies. This approach not only illuminates the landscape of current research but also sets the stage for subsequent analysis and discussion, pinpointing avenues for advancement and innovation.

4. Key findings from relevant research

From Table 3 detailing research overview in the context of DDoS attacks in the cloud, several deep insights can be extracted related to trends, methodologies, geographical contributions, and technology preferences. This analysis will explore these dimensions to provide a comprehensive understanding of the current state and directions in DDoS research in cloud computing environments.

4.1. Geographical distribution and contributions

Fig. 4 presents a comparative analysis of global research papers on DDoS attack defense systems in cloud computing, categorized by country. This graph provides insights into the level of engagement and focus of different countries on addressing DDoS threats within cloud computing environments.

India's Prominence: A significant proportion of the research originates from India, indicating a strong research interest and expertise in the area of DDoS defense mechanisms within the cloud computing landscape in this country. This could be due to the growing digital infrastructure and the corresponding need to secure it against cyber threats.

Global Interest: Besides India, there is noticeable research output from countries like China, Turkey, Malaysia, Saudi Arabia, Vietnam, and several collaborations between countries (e.g., Finland, UK, Iran, Algeria). This variety illustrates the global concern and research interest in combating DDoS attacks in cloud environments, emphasizing the universal challenge of ensuring cybersecurity.

4.2. Research trends and methodologies

In Fig. 5, we illustrate the distribution of papers according to the techniques employed, specifically: machine learning (42 papers), deep learning (50 papers), and other methods (25 papers).

Deep Learning Dominance: Most studies utilize deep learning techniques, demonstrating the current leading-edge approach in identifying, analyzing, and alleviating DDoS attacks. This tendency suggests

Table 3
Studies overview.

Num	Ref	Year	Type	Journal	Publisher	Country	Method	Tools	Programming language
1	[31]	2024	Article	Expert Systems With Applications	Elsevier	India	Deep learning	N/A	Python
2	[32]	2024	Article	Computers and Security	Elsevier	India	Deep learning	Mininet	Python
3	[33]	2024	Article	Journal of King Saud University - Computer and Information Sciences	Elsevier	Morocco	Deep learning	N/A	Python
4	[34]	2024	Article	Computers and Security	Elsevier	Turkey	Deep learning	N/A	Python
5	[35]	2024	Article	Expert Systems	Wiley	Colombia	Deep learning	N/A	Python
6	[36]	2023	Article	International Journal of Computer Network and Information	MECS Press	India	Deep learning	N/A	N/A
7	[37]	2023	Article	International Journal of Intelligent Systems and Applications in Engineering	Ismail Saritas	India	Deep learning	N/A	N/A
8	[38]	2023	Article	Measurement: Sensors	Elsevier	India	Deep learning	N/A	Matlab
9	[39]	2023	Article	Systems	MDPI	Malaysia, Saudi Arabia	Deep learning	N/A	N/A
10	[40]	2023	Article	Knowledge-Based Systems	Elsevier	India	Deep learning	N/A	N/A
11	[41]	2024	Article	Computers and Security	Elsevier	India, Vietnam	Deep learning	Mininet	Python
12	[42]	2023	Article	IEEE Transactions on Dependable and Secure Computing	IEEE	Finland, UK, Iran, Algeria	Deep learning	Kubernetes, Openstack	Python
13	[43]	2023	Article	Computer Systems Science and Engineering	Tech Science Press	India	Deep learning	N/A	N/A
14	[44]	2023	Article	International Journal of Intelligent Systems	Hindawi	India	Deep learning	N/A	Matlab
15	[45]	2023	Article	Computers, Materials and Continua	Tech Science Press	Jordan, Saudi Arabia	Deep learning	N/A	Python
16	[46]	2023	Article	Computer Systems Science and Engineering	Tech Science Press	India	Deep learning	Apache spark	Python
17	[47]	2023	Article	IEEE Transactions on Cybernetics	IEEE	Vietnam, Australia	Deep learning	N/A	Python
18	[48]	2021	Article	Wireless Personal Communications	Springer	India	Deep learning	N/A	Matlab
19	[49]	2023	Article	Computer Communications	Elsevier	India	Deep learning	N/A	N/A
20	[50]	2024	Article	Computers and Security	Elsevier	India	Deep learning	N/A	Python
21	[51]	2022	Article	Simulation Modeling Practice and Theory	Elsevier	Kuwait, Jordan, Kazakhstan	Deep learning	N/A	Matlab
22	[52]	2022	Article	Journal of King Saud University - Computer and Information Sciences	Elsevier	India	Deep learning	Owncloud, Mininet, HPing-3	Python
23	[53]	2022	Article	Concurrency and Computation: Practice and Experience	Wiley	India	Deep learning	Qemu, HPing-3, IPTraf, Vnstat, Top command, Netstat	N/A
24	[54]	2022	Article	Journal of Sensors	Hindawi	Korea	Deep learning	N/A	N/A
25	[55]	2022	Article	IEEE Access	IEEE	Sweden, Singapore	Deep learning	N/A	N/A
26	[56]	2023	Article	Cybernetics and Systems: An International Journal	Taylor and Francis	India	Deep learning	N/A	Python
27	[57]	2022	Article	Computers and Security	Elsevier	Turkey	Deep learning	N/A	Python

(continued on next page)

Table 3 (*continued*).

28	[58]	2020	Conference Paper	Procedia Computer Science, International Conference on Computational Intelligence and Data Science	Elsevier	India	Deep learning	Openstack	N/A
29	[59]	2021	Article	Future Generation Computer Systems	Elsevier	Brazil, Spain	Deep learning	Mininet, Scapy	Python
30	[60]	2023	Article	Multimedia Tools and Applications	Springer	India, Saudi Arabia	Deep learning	N/A	N/A
31	[61]	2023	Article	Wireless Personal Communications	Springer	India	Deep learning	Owncloud, Mininet, HPing-3	Python
32	[62]	2023	Article	International Journal of Intelligent Systems	Hindawi	India, Maldives	Deep learning	N/A	Matlab
33	[63]	2024	Article	Computers and Security	Elsevier	China	Deep learning	NetLogo	N/A
34	[64]	2024	Article	Computers and Security	Elsevier	China, Singapore	Deep learning	N/A	N/A
35	[65]	2022	Article	International Journal of Intelligent Systems and Applications in Engineering	Ismail Saritas	India	Deep learning	Openstack	N/A
36	[66]	2023	Article	International Journal of Computer Network and Information Security	MECS Press	India	Deep learning	N/A	N/A
37	[67]	2023	Article	Materials Today: Proceedings	Elsevier	India	Deep learning	N/A	Python
38	[68]	2024	Article	Scientific Reports	Nature Publishing Group	China	Deep learning	N/A	Python
39	[69]	2023	Article	Majlesi Journal of Electrical Engineering	Islamic Azad University	India	Deep learning	N/A	Python
40	[70]	2023	Conference paper	2023 International Conference on System Computation Automation and Networking	IEEE	India	Deep learning	N/A	Python
41	[71]	2020	Article	IEEE Access	IEEE	India	Deep learning	N/A	N/A
42	[72]	2023	Article	IEEE Access	IEEE	China	Deep learning	N/A	Python
43	[73]	2024	Conference paper	5th International Conference on Industry 4.0 and Smart Manufacturing	Elsevier	India	Deep learning	N/A	Python
44	[74]	2024	Article	Computers and Electrical Engineering	Elsevier	India, Thailand	Deep learning	N/A	Python
45	[75]	2024	Article	Journal of Network and Computer Applications	Elsevier	UK	Deep learning	N/A	N/A
46	[76]	2024	Article	Nature Publishing	Scientific Reports	India, Saudi Arabia, Tunisia	Deep learning	N/A	N/A
47	[77]	2024	Article	Nature Publishing	Scientific Reports	China	Deep learning	N/A	N/A
48	[78]	2024	Article	Journal of Adaptive Control and Signal Processing	Wiley	India	Deep learning	N/A	N/A
49	[79]	2024	Article	Applied Sciences	MDPI	Saudi Arabia	Deep learning	N/A	N/A
50	[80]	2024	Article	Multimedia Tools and Applications	Springer	India	Deep learning	N/A	N/A
51	[81]	2024	Article	Measurement: Sensors	Elsevier	China	Machine learning	N/A	Python
52	[82]	2024	Article	Cyber Security and Applications	Elsevier	India, Taiwan, China	Machine learning	NS2	N/A
53	[83]	2022	Article	Computers and Electrical Engineering	Elsevier	India, Jordan	Machine learning	N/A	N/A
54	[84]	2020	Article	Journal of Information Security and Applications	Elsevier	India	Machine learning	N/A	Matlab

(*continued on next page*)

Table 3 (*continued*).

55	[85]	2023	Article	International Journal of Computer Network and Information Security	MECS Press	India	Machine learning	N/A	N/A
56	[86]	2023	Article	EAI Endorsed Transactions on Scalable Information Systems	European Alliance for Innovation	India	Machine learning	N/A	Python
57	[87]	2023	Article	International Journal of Advanced Computer Science and Applications	Science and Information Organization	India	Machine learning	N/A	Python
58	[88]	2023	Article	Journal of Discrete Mathematical Sciences and Cryptography	Taylor and Francis	India, USA	Machine learning	N/A	Python
59	[89]	2023	Article	International Journal of Intelligent Engineering and Systems	Intelligent Networks and Systems Society	India	Machine learning	N/A	Python
60	[90]	2023	Article	International Journal of Electrical and Computer Engineering Systems	Intelligent Networks and Systems Society	Egypt	Machine learning	N/A	Python
61	[91]	2022	Article	Computer Networks	Elsevier	India	Machine learning	N/A	Matlab
62	[92]	2022	Article	Array	Elsevier	Azerbaijan	Machine learning	N/A	Python
63	[93]	2022	Article	Concurrency and Computation: Practice and Experience	Wiley	India	Machine learning	N/A	Matlab
64	[94]	2024	Article	Measurement: Sensors	Elsevier	Bangladesh	Machine learning	N/A	Python
65	[95]	2022	Article	Journal of King Saud University – Computer and Information Sciences	Elsevier	India	Machine learning	N/A	Matlab
66	[96]	2022	Article	IJ Computer Network and Information Security	MECS Press	China	Machine learning	N/A	Python
67	[97]	2022	Article	Symmetry	MDPI	Saudi Arabia, Pakistan	Machine learning	N/A	Python
68	[98]	2022	Article	Journal of Cyber Security and Mobility	River Publishers	Saudi Arabia	Machine learning	Weka	Java
69	[99]	2022	Article	International Journal of Advanced Computer Science and Applications	Science and Information Organization	India	Machine learning	N/A	N/A
70	[100]	2022	Article	Computational Intelligence and Neuroscience	Hindawi	India	Machine learning	N/A	Python
71	[101]	2024	Article	Measurement: Sensors	Elsevier	China	Machine learning	N/A	Matlab
72	[102]	2022	Article	Mobile Information Systems	Hindawi	Iran	Machine learning	Mininet	Python
73	[103]	2022	Article	IEEE Access	IEEE	China	Machine learning	Mininet	N/A
74	[104]	2021	Article	Journal of Parallel and Distributed Computing	Elsevier	India	Machine learning	N/A	N/A
75	[105]	2021	Article	Computers and Security	Elsevier	India	Machine learning	N/A	Matlab
76	[106]	2022	Article	Turkish Journal of Electrical Engineering and Computer Sciences	Turkiye Klinikleri	India	Machine learning	N/A	Matlab
77	[107]	2021	Article	Security and Communication Networks	Hindawi	China	Machine learning	N/A	N/A
78	[108]	2021	Article	International Journal of Advances in Intelligent Informatics	Universitas Ahmad Dahlan	Iraq	Machine learning	N/A	Python
79	[109]	2023	Article	Mobile Networks and Applications	Springer	India, Ireland	Machine learning	N/A	Python
80	[110]	2024	Article	Algorithms	MDPI	USA	Machine learning	N/A	Python
81	[111]	2024	Article	Electronics	MDPI	USA	Machine learning	N/A	N/A

(*continued on next page*)

Table 3 (*continued*).

82	[112]	2023	Article	IEEE transactions on network science and engineering	IEEE	China	Machine learning	N/A	N/A
83	[113]	2021	Article	International Journal of Communication Networks and Information Security	Institute of Information Technology, Kohat University of Science and Technology	Brasil	Machine learning	Azure	N/A
84	[114]	2021	Article	Journal of Network and Systems Management	Springer	Brasil	Machine learning	N/A	Python
85	[115]	2021	Article	Journal of Telecommunications and Information Technology	National Institute of Telecommunications	India	Machine learning	Openstack, Spark	Python
86	[116]	2022	Article	Concurrency and Computation: Practice and Experience	Wiley	India	Machine learning	N/A	Python
87	[117]	2023	Article	Wireless Personal Communications	Springer	India	Machine learning	Mininet	Python
88	[118]	2024	Article	Cyber Security and Applications	Elsevier	India	Machine learning	Mininet	Python
89	[119]	2023	Article	IEEE Access	IEEE	Egypt	Machine learning	N/A	N/A
90	[120]	2020	Article	IEEE Access	IEEE	Turkey	Machine learning	N/A	N/A
91	[121]	2024	Article	Journal of Cloud Computing	Springer	India	Machine learning	N/A	Python
92	[122]	2024	Article	Multimedia Tools and Applications	Springer	India, Jordan	Machine learning	N/A	Python
93	[123]	2023	Article	Journal of Parallel and Distributed Computing	Elsevier	Iran	Others	CLoudSim	N/A
94	[124]	2023	Article	Journal of Cyber Security and Mobility	River Publishers	Palastine	Others	NS2	Matlab, Python
95	[125]	2023	Article	Applied Sciences	MDPI	Malaysia	Others	Kubernetes	Python
96	[126]	2023	Article	Journal of Information Security and Applications	Elsevier	India	Others	N/A	N/A
97	[127]	2023	Article	Intelligent Automation and Soft Computing	Tech Science Press	India	Others	N/A	N/A
98	[128]	2023	Article	International Journal of Safety and Security Engineering	International Information and Engineering Technology Association	India	Others	N/A	N/A
99	[129]	2022	Article	International Journal of Safety and Security Engineering	International Information and Engineering Technology Association	Indonesia	Others	GNS3, VirtualBox	N/A
100	[130]	2022	Article	Computer Communications	Elsevier	Pakistan	Others	Openstack, POX	Python, Java
101	[131]	2022	Article	IEEE Transactions on Industrial Informatics	IEEE	Nepal, India	Others	AWS EC2	N/A
102	[132]	2022	Article	International Journal of Advanced Computer Science and Applications	Science and Information Organization	India	Others	N/A	N/A
103	[133]	2021	Article	International Journal of Computer Networks and Applications	EverScience Publications	India	Others	Oracle VM VirtualBox, Low Orbit Ion Cannon, Packet Storm	Python
104	[134]	2020	Article	Evolutionary Intelligence	Springer	India	Others	CloudSim	N/A
105	[135]	2021	Article	Telecommunication Systems	Springer	India	Others	Mininet, POX	Python
106	[136]	2021	Article	Wireless Personal Communications	Springer	India	Others	Vnstat, TOP command	N/A

(*continued on next page*)

Table 3 (*continued*).

107	[137]	2021	Article	Journal of Network and Systems Management	Springer	India	Others	AWS EC2, Mininet, FlowVisor, OpenDayLight	N/A
108	[138]	2020	Article	Mobile Networks and Applications	Springer	Malaysia	Others	Mininet, HPing-3	N/A
109	[139]	2021	Article	Future Generation Computer Systems	Elsevier	India, Taiwan, Australia	Others	N/A	Matlab
110	[140]	2021	Article	Computers and Security	Elsevier	China	Others	N/A	Matlab
111	[141]	2023	Article	Multimedia Tools and Applications	Springer	India, Malaysia	Others	OPNET, ndnSIM	N/A
112	[142]	2023	Article	Journal of Network and Systems Management	Springer	India	Others	Openstack, BoNeSi	N/A
113	[143]	2023	Conference paper	2023 4th IEEE Global Conference for Advancement in Technology	IEEE	India	Others	N/A	N/A
114	[144]	2023	Conference paper	International Conference on Sustainable Communication Networks and Application 2023	IEEE	India	Others	N/A	N/A
115	[145]	2023	Article	IEEE Access	IEEE	Pakistan, Germany, Taiwan, Hungary	Others	N/A	N/A
116	[146]	2023	Conference paper	The 20th International Joint Conference on Computer Science and Software Engineering	IEEE	Thailand	Others	Google GCP	N/A
117	[147]	2024	Article	Journal of Network and Computer Applications	Elsevier	India	Others	Oracle virtual Box	N/A

the complexity and sophistication of recent DDoS threats, which demand advanced analytical capabilities to identify relevant patterns and anomalies, thereby facilitating the necessary countermeasures.

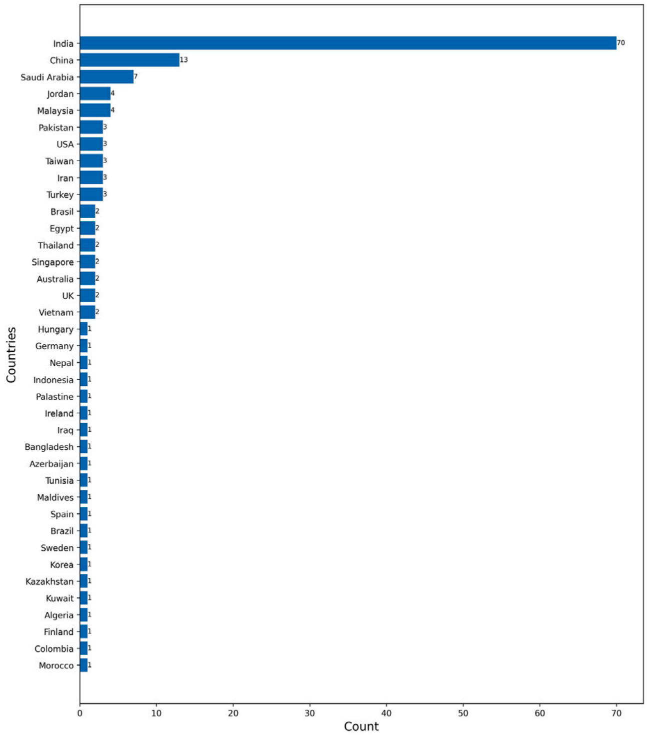

Fig. 4. Comparative analysis of global research papers on DDoS attack defense systems in cloud computing by country.

Machine Learning Applications: Indeed, machine learning techniques are also implemented, highlighting the broader utilization of AI technologies to tackle cybersecurity challenges. These methods likely encompass a diverse range, from traditional statistical techniques to cutting-edge methods . Consequently, this spectrum of approaches provides a wide array of detection and response mechanisms, further bolstering cybersecurity capabilities.

Fig. 5 illustrates the distribution of papers across various programming languages. According to the data from Table 3, 51 papers did not specify any information regarding the programming languages used.

Tools and Programming Languages: Python emerges as the predominant programming language, suggesting its popularity and effectiveness in implementing deep learning and machine learning algorithms. Other tools and languages mentioned, such as Matlab, Mininet, and Kubernetes, indicate a diverse set of technologies used for simulations, network emulations, and orchestrating containerized applications, respectively. This diversity points to the multifaceted nature of research methodologies, from theoretical models to practical implementations (see Fig. 6).

4.3. Publication venues and type

Leading Publishers: Research is predominantly published in journals associated with well-known publishers like Elsevier, IEEE, Springer, and Wiley. This indicates the quality and rigorous peer review process behind the research contributions in this field (See Fig. 7).

Types of Contributions: The majority of the contributions are in the form of articles, complemented by a smaller number of conference papers. Articles typically present comprehensive research findings and in-depth analysis, whereas conference papers tend to introduce novel ideas and preliminary results. This diverse mix of article types demonstrates a well-balanced approach. It promotes both in-depth research investigations and the prompt sharing of new ideas and concepts. This strategy ensures a comprehensive coverage of the field, combining

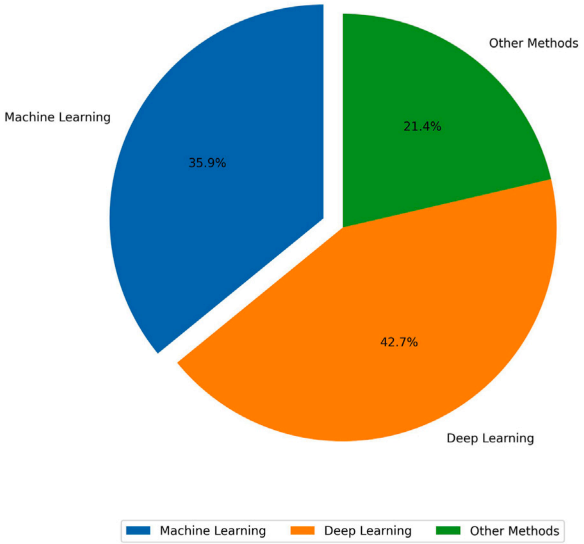

Fig. 5. Paper distribution by employed techniques.

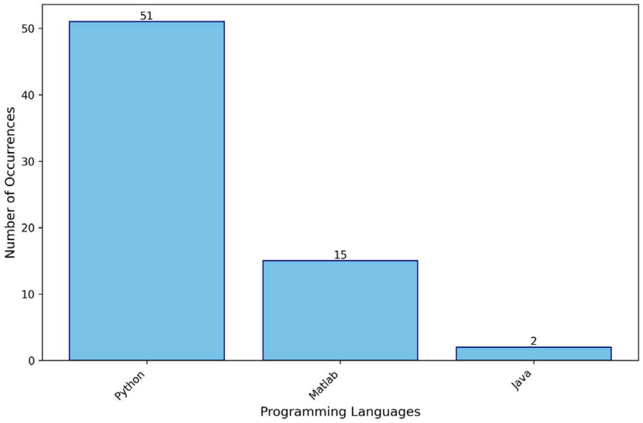

Fig. 6. Paper distribution by programming languages.

thorough academic exploration with the agility to address emerging trend (See Fig. 8).

4.4. Yearly distribution

In order to address the most recent trends and advancements, we have chosen to primarily focus on papers published in the last two years, 2023 and 2024. The literature from this period indicates either an increasing or persistent interest in these fields, likely propelled by continuous technological progress and the ongoing demand for novel solutions to newly arising issues within computer science, especially within the realms of security and data analysis. By concentrating on the most recent literature, we aim to capture the latest developments, cutting-edge techniques, and state-of-the-art approaches, ensuring that our analysis and solutions are aligned with the current landscape and poised to tackle the most pressing issues effectively (See Fig. 9).

The analysis reveals a dynamic and globally distributed research effort focusing on leveraging advanced AI techniques, particularly deep learning, to address DDoS attacks in cloud environments. The widespread use of Python and diverse tools for simulation and orchestration highlight the practical and experimental nature of this research. Moreover, the geographical distribution of the research underscores the global recognition of DDoS attacks as a critical threat to cloud computing's security and reliability, necessitating a global response.

5. In-depth insights from research papers utilizing deep learning techniques

This section offers an in-depth review of contemporary research aimed at enhancing the detection and countermeasures of DDoS attacks within diverse computing contexts such as cloud, fog, and software-defined networking (SDN), utilizing deep learning methods.

5.1. Advancing cloud cybersecurity with deep learning techniques

The study [31] presents a novel approach for predicting DDoS attacks in cloud environments using honey badger optimization for feature selection and a Bi-LSTM classifier. It highlights the effectiveness of this model by comparing it with traditional methods, showing superior accuracy with public datasets CICIDS2018-AWS, CICIDS2017 and CICDoS2016. The study emphasizes the importance of advanced preprocessing and optimization techniques in improving detection capabilities. However, it points out the need for further research on enhancing detection speed and reducing false positives, without specifying direct mitigation strategies.

The study [32] proposes a real-time IoT-DDoS mitigation framework utilizing fog computing and software-defined networking to enhance security in cyber–physical systems. It leverages a multi-stage Stack-Ensemble model and a comprehensive dataset combining public (InSDN, BoT-IoT and UNSW-Sydney) and simulated data for accurate DDoS attack detection. The framework significantly reduces feature count while maintaining high detection accuracy, emphasizing the efficiency of fog computing in attack mitigation. However, the need for further improvements in reducing false positives and enhancing real-time detection capabilities.

The study [33] introduces "DeepDefend", a real-time DDoS attack detection and prevention framework in cloud environments. It leverages advanced deep learning techniques, such as CNN-LSTM-Transformer networks, to predict network traffic entropy. DeepDefend incorporates a genetic algorithm for optimal feature selection, enhancing its effectiveness in distinguishing between normal and attack traffic. Tested on the CIDDS-001 dataset, DeepDefend demonstrates high accuracy in entropy forecasting and DDoS detection. The study emphasizes the combination of time series analysis, genetic algorithms, and deep learning for robust DDoS protection in cloud computing. Further validation is needed for scalability and effectiveness against various types and scales of attacks.

The study [34] introduces LSTM-CLOUD, an LSTM-based detection and defense system for DDoS attacks in public cloud networks. The system focuses on signature-based detection and achieved a remarkable 99.83% accuracy rate on the CICDDoS2019 dataset. LSTM-CLOUD consists of detection and defense modules that leverage deep learning techniques for real-time anomaly identification and automated mitigation strategies. The study's contributions include a high-performance LSTM model and its application in network traffic characterization, aiming to effectively mitigate DDoS attacks. However, further validation and exploration are necessary to evaluate the scalability and effectiveness of the system against different types and scales of attacks.

The study [35] introduces a cloud-based deep learning architecture for DDoS cyber-attack prediction. It utilizes a large public dataset (CICIDS2017) and employs deep neural networks to accurately detect and predict DDoS attacks. The key findings showcase the effectiveness of deep learning in mitigating such attacks, especially in high-speed data traffic environments. The study discusses strategies for prevention and mitigation. A limitation is the use of an unbalanced dataset, and further research could explore techniques to improve overall performance.

The study [36] presents a novel technique for detecting DDoS attacks in cloud environments, combining Gaussian Kernel Density algorithms and deep learning for improved accuracy. It uses public datasets (NSL-KDD and CICIDS2017) for validation, demonstrating effectiveness over traditional methods. The approach mainly involves

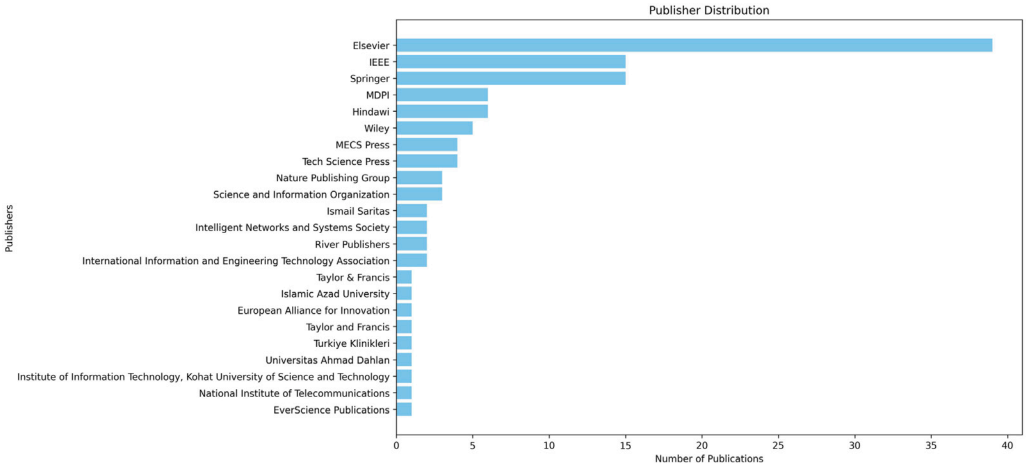

Fig. 7. Paper distribution by the publishers.

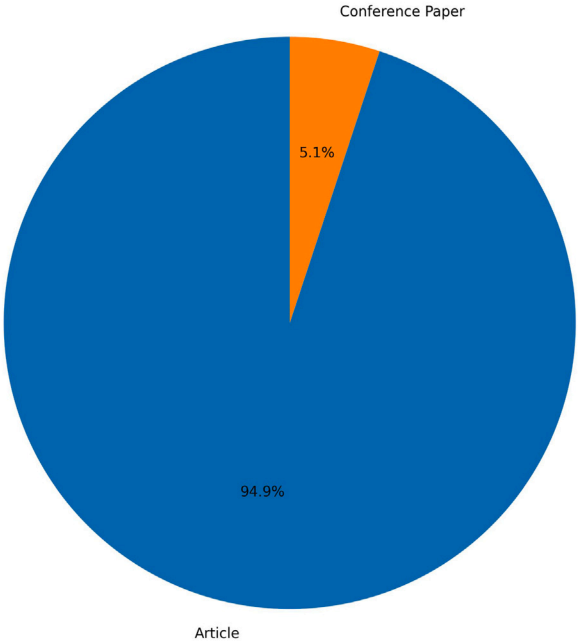

Fig. 8. Paper distribution by type.

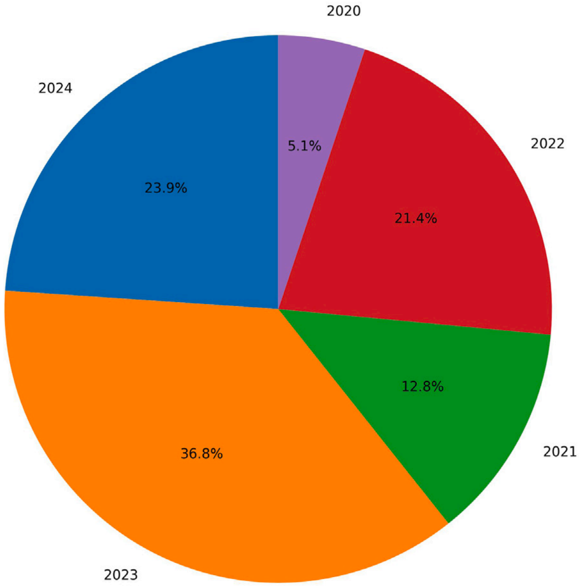

Fig. 9. Paper distribution by the year.

’Filtering’ as a mitigation strategy. Despite its effectiveness, it faces limitations like high computational demands, suggesting future research could focus on optimizing these algorithms for efficiency and better performance.

The study [37] proposes a hybrid model of Radial Basis Function (RBF) and LSTM networks for detecting and mitigating DDoS attacks in cloud computing. It utilizes deep learning algorithms and evaluates the model using the CICDDoS2019 dataset. The findings demonstrate the effectiveness of the hybrid model in identifying DDoS attacks. However, potential areas for further research could include the evaluation of the proposed method on different datasets to assess its generalizability.

The study [38] introduces the LRDADF, an innovative AI-enabled framework designed to detect and mitigate low-rate DDoS attacks in cloud computing environments. The framework incorporates a hybrid detection algorithm and a dynamic mitigation strategy, which falls under the category of ‘Redirection’. The effectiveness of the framework is demonstrated through rigorous testing using a public dataset (CICDDoS2019). However, to further enhance the framework’s capabilities, future research could focus on evaluating its performance using real-world datasets and exploring additional techniques for detection and mitigation.

The study [39] presents a method for detecting DDoS attacks using deep learning in SDN environments. It utilizes a public dataset (DDOS attack SDN) for evaluation, applying data preprocessing, feature selection, and RNNs, achieving high detection accuracy and low false positives. The research suggests potential for future studies in applying the model to real-world data and exploring its effectiveness across various network configurations.

The study [40] presents a novel approach for DDoS attack detection in cloud environments using a hybrid model that combines fractional calculus with Anti Corona Virus Optimization (ACVO) and a Deep Neuro-Fuzzy Network (DNFN). It leverages public datasets for evaluation, demonstrating high accuracy in identifying attacks. Key strategies include feature fusion and data augmentation. Limitations point to scalability and real-time processing needs, suggesting future research could focus on optimization for real-world deployment and computational efficiency enhancement.

The study [41] introduces a DNN model for DDoS attack detection in SDN settings, showcasing high accuracy using public (InSDN, CICIDS2018, Kaggle DDoS) and simulated data. It underscores the model's advantage over conventional techniques without detailing specific prevention strategies. Acknowledging the model's complexity, it calls for future work to improve real-time performance and the model's response to new DDoS threats.

The study [42] presents "FortisEDoS", a framework that utilizes deep transfer learning for detecting Economical Denial of Sustainability (EDoS) attacks in 5G network slices. The framework introduces CG-GRU, a novel model combining graph and recurrent neural networks, which is optimized using transfer learning techniques. The study employs simulated data to evaluate the framework's performance, demonstrating high detection rates and computational efficiency. It suggests future research directions, including adaptive thresholding and integration of advanced deep learning models. The study acknowledges limitations in simulating attack scenarios and emphasizes the need for real-world validation, without explicitly discussing specific mitigation strategies.

The study [43] presents a DDoS detection method for cloud environments, leveraging an Adaptive Butterfly Optimization Algorithm (ABOA) for feature selection and a Deep Neural Network (DNN) for classification. It uses public datasets NSL-KDD and CICIDS2017, showing a high accuracy of up to 99.05%. The approach is noted for its potential in cloud security, with suggestions for future research focusing on scalability and adaptability, particularly in software-defined networks.

The study [44] introduces a new algorithm to detect DDoS attacks in cloud environments, combining deep learning and optimization techniques. It utilizes public datasets (BOT-IoT and NSL-KDD), achieving high accuracy in detection. The study focuses on improving cybersecurity through advanced algorithms but suggests further exploration in real-time detection and feature selection for future research.

The study [45] presents an efficient Intrusion Detection System (IDS) for cloud computing, specifically targeting DDoS attacks. The IDS incorporates ensemble feature selection and a hybrid deep learning model that combines CNN and LSTM. By utilizing the publicly available CICIDS 2017 dataset, the proposed IDS achieves remarkable performance in terms of accuracy and precision. The integration of feature selection and deep learning in the methodology is a notable contribution to enhancing cloud security. However, it is worth noting that the study's limitations lie in the dataset's lack of diversity, suggesting the need for future research focusing on real-time data and more diverse datasets.

The study [46] introduces a hybrid model combining Deep Belief Networks and LSTM optimized by Particle Swarm Optimization for DDoS attack detection, using the NSL-KDD dataset. It outperforms traditional models in accuracy, precision, recall, and F-measure. The study suggests its potential for improving cybersecurity in cloud computing but notes the need for further efficiency optimization and real-time data testing as areas for future research.

This study [47] explores the use of Deep Generative Learning Models, specifically Conditional Denoising Adversarial Autoencoders (CDAAE) and a hybrid model (CDAAE-KNN), to improve Cloud Intrusion Detection Systems (IDS) in detecting Distributed Denial of Service (DDoS) attacks. The research utilizes three public IDS datasets: CICIDS 2017, NSL-KDD, and UNSW-NB15, to prove that these models increase detection accuracy through the generation of synthetic malicious samples. The study emphasizes the effectiveness of deep learning in managing dataset imbalances and suggests potential areas for further research. These include examining the scalability and performance of the proposed models in large-scale cloud environments and investigating additional methods for addressing imbalanced datasets in cloud IDSs.

The study [48] introduces a novel method combining Whale Optimization Algorithm (WOA) for feature selection and Deep Neural Network (DNN) for DDoS attack detection in cloud storage, using the public CIC-IDS 2017 dataset. It emphasizes the technique's high detection accuracy and the use of homomorphic encryption to secure data. The study's limitations are its reliance on the CIC-IDS 2017 dataset, which may not capture all DDoS attack types or real-world scenarios, and the challenges in detecting new attacks.

The study [49] introduces a hybrid intrusion detection system (IDS) for web and cloud environments, combining modified manta-ray foraging optimization (MMFO) and teacher learning-based deep recurrent neural network (TL-DRNN). It excels in accuracy and efficiency using public datasets (DARPA LLS DDoS-1.0, CICIDS-2017, and CSIC-2010) for validation. The study highlights the system's effectiveness in reducing false positives and negatives, with potential improvements suggested for scalability and real-time detection. Further research could explore adapting the system to newer and more varied attack types.

This study [50] presents a new method for identifying and addressing DDoS attacks in Software Defined Networking (SDN) systems, using Balanced Random Sampling (BRS) and Convolutional Neural Networks (CNNs). A significant focus is placed on utilizing public datasets, particularly the CICDDoS2019 dataset, for training and verifying the model's effectiveness. The primary contributions are: a precise DDoS detection system, a mitigation system utilizing filtering, rate limiting, and iptables rules for blocking fraudulent IPs, and an original monitoring system. The study boasts impressive detection accuracy rates of over 99.99% for binary classification. However, limitations include the possibility of false positives and the necessity for additional validation in real-world scenarios. Future research could examine the scalability of the proposed solutions and their efficacy against changing DDoS attack tactics.

The study [51] presents a neural network model designed to improve security against DDoS attacks in containerized cloud computing environments. The model, tested with the CICDDoS 2019 public dataset, boasts a 97.07% detection accuracy. It effectively distinguishes between benign and malicious traffic while minimizing computational cost. However, future studies should focus on further optimizing computational efficiency and exploring comprehensive defense strategies, such as traffic filtering or blocking, to enhance cloud security.

This study [52] proposes a deep learning framework to tackle DDoS attacks in fog and cloud computing systems, using software-defined networking (SDN) to implement a defense mechanism that incorporates 'Filtering' and 'Blocking' techniques at the source. The framework is evaluated using the ISCX 2012 dataset and simulated attacks created with HPing-3, resulting in a 98.88% accuracy rate in differentiating between legitimate and malicious traffic. However, the necessity for continuous model training to keep up with new attack patterns highlights the need for future research on increasing model resilience and addressing additional attack vectors in cloud computing.

The article [53] presents a new method that combines Deep Belief Networks and Support Vector Machines to detect DDoS and EDoS attacks in cloud environments, resulting in high detection accuracy. The method was trained using simulated traffic and resource utilization data, demonstrating its effectiveness in identifying attacks, particularly in its high precision rate of 99.708%. The approach is similar to 'Filtering' for attack mitigation. However, there are potential limitations in the form of possible decreased accuracy in specific environments and the need for large data samples, indicating a need for further research on model enhancement and expanding the applicability of the dataset.

This study [54] presents a hybrid Intrusion Detection System (IDS) that combines optimization algorithms and Long Short-Term Memory (LSTM) for detecting Distributed Denial of Service (DDoS) attacks. The proposed model utilizes Harris Hawks Optimization and Particle Swarm Optimization for optimizing features. The IDS, trained using simulated data, demonstrates improved accuracy and efficiency in identifying DDoS attacks. However, there are opportunities for further improvement in parameter optimization and exploration of additional hybrid approaches to enhance adaptability and performance in detecting DDoS threats.

The study [55] introduces a reinforced transformer learning method for detecting VSI-DDoS attacks in edge clouds, demonstrating high accuracy through testing on real and benchmark datasets (CIC-DDoS2019 and UNSW- NB15). It merges transformers with deep reinforcement learning to prioritize context-driven information. A significant limitation is its lack of discussion on prevention or mitigation strategies for such attacks, in addition to the need for model generalization improvements. Future research directions include enhancing the model's adaptability to diverse attack scenarios.

The article [56] proposes a method for identifying DDoS attacks in cloud environments using an optimized DBN-GRU model with weighted features and public datasets, including CICIDS 2017, NSL-KDD, and KDDcup99, for evaluation. The study obtains a detection accuracy of 97.05%, demonstrating the effectiveness of the proposed model. Future research directions include enhancing the model's scalability and adaptability to emerging attack patterns.

The study [57] introduces deep learning models (DNN, CNN, LSTM) for DDoS attack detection, utilizing the CIC-DDoS2019 dataset. It highlights preprocessing techniques and the superior performance of the CNN model, pointing towards deep learning's potential in cybersecurity. Future research directions include exploring diverse datasets and real-world scenarios.

The study [58] presents a DDoS detection system for private clouds based on OpenStack. Simulations are used to generate data, and the effectiveness of Decision Tree, KNN, Naive Bayes, and DNN algorithms is evaluated. The study finds that the DNN algorithm is the most effective. The system combines an OpenStack firewall with raw socket programming to target bandwidth and connection flooding attacks, aiming to enhance cloud security. Future research is suggested to optimize DDoS detection and explore potential integration with Hadoop for improved performance. The limitations of current OpenStack firewalls in handling DDoS attacks highlight the need for dedicated detection modules.

This study [59] presents a novel approach for identifying and combating DDoS attacks in SDN environments using a Generative Adversarial Network (GAN) for real-time anomaly detection. The method utilizes adversarial training and IP flow analysis, along with both emulated data and the CICDDoS 2019 public dataset. The proposed defense mechanism has demonstrated improved detection accuracy and speed. However, future research could focus on further exploration of deep learning techniques and testing in diverse settings to build upon its success.

The study [60] introduces the MMEDRL-ADM technique for DDoS attack detection and mitigation in cloud-based SDN environments, combining metaheuristic optimization with multi-layer ensemble deep reinforcement learning. It employs the African buffalo optimization algorithm for feature selection and the improved grasshopper optimization algorithm for hyperparameter tuning. Tested on a benchmark dataset, this approach demonstrates superior performance over existing models, suggesting its effectiveness in real-time DDoS threat mitigation. Future research endeavors might concentrate on the extended investigation of deep learning methodologies and their application in a variety of contexts, with the aim of augmenting their proven efficacy.

This study [61] presents a DDoS attack mitigation system for cloud and fog computing environments, which utilizes Software-Defined Networking (SDN) technology for network management. The system uses Deep Reinforcement Learning (DRL) and Long Short-Term Memory (LSTM) for real-time packet classification as either malicious or legitimate. The proposed scheme has been tested using both real and simulated DDoS attack packets, achieving a high accuracy rate of 98.88%. In future work, the integration of DRL with Autoencoders will be explored to further improve DDoS attack detection. The dataset used for this study includes both real and simulated attack scenarios, with the Hogzilla dataset serving as the primary source of data.

This study [62] presents a deep learning framework that utilizes the Gradient Hybrid Leader Optimization (GHLBO) algorithm to identify DDoS attacks in cloud environments. The framework incorporates a Deep Stacked Autoencoder (DSA) for effective detection, further enhanced by the implementation of feature fusion and data augmentation techniques. The proposed framework demonstrates high detection accuracy, indicating its potential for use in various network configurations. Future research could focus on optimizing the algorithm and expanding its applicability to diverse contexts.

This study [63] presents EDM_TOS, a groundbreaking approach to minimizing edge DDoS attacks through risk-evaluated task offloading in edge and cloud computing. Equipped with a distinctive risk assessment mechanism and algorithms, it significantly improves security. The evaluation is based on five datasets (CICDDoS2019, CICIDS2018, CIC-IDS2017, UNSW NB15, and ISCX-IDS-2012), highlighting its exceptional performance compared to existing solutions. Future research could concentrate on developing more effective risk assessment and offloading strategies in various computing environments.

The study [64] introduces a novel method for mitigating DDoS attacks by identifying attack patterns and categorizing them into specific families using community detection techniques. It focuses on analyzing real-world DDoS traffic data to optimize defense mechanisms and enhance filtering responses. The study demonstrates the potential of this approach in improving the effectiveness of DDoS mitigation strategies. Future research could further refine this technique for broader applicability across various network settings.

The research [65] proposes a cloud-based DDoS attack detection method using machine learning architectures, focusing on ResNet-101 based KELM for feature extraction and classification. It processes input data through dimensionality reduction and noise removal techniques. The study utilized CICIDS 2017 and CICDDoS 2019 datasets from public sources, achieving a data delivery ratio of 92%, a transaction rate of 82%, validation accuracy of 89%, training accuracy of 96%, and an end-to-end delay of 56%. This innovative approach underscores the potential of utilizing deep learning architectures for enhancing cloud security against DDoS attacks. For improved credibility, it is highly recommended to validate the approach by utilizing real-world data.

The study [66] introduces the HGSO-WIB-ReLU framework for efficient DDoS attack detection, emphasizing low-rate attack identification unachievable by existing statistical and machine learning methods. Utilizing the BUET-DDoS2020, CIC DoS Attacks, and Low Rate DDoS datasets, it incorporates a novel weight initialization approach in CNN architecture to address gradient vanishing, enhanced by the Henry Gas Solubility Optimization (HGSO) method for optimizing hyperparameters. Achieving high accuracy across datasets, it demonstrates the effectiveness of combining chaos theory with machine learning for security applications, it is highly recommended to validate the approach by utilizing real-world data.

The study [67] introduces a novel Deep Learning Binary Fruit Fly Algorithm (DL-BFFA) to detect SYN flood attacks in TCP/IP networks, demonstrating a significant enhancement in detection accuracy (99.96%) using the KDD Cup dataset. This approach integrates deep learning with an innovative binary fruit fly optimization for precise SYN flood attack prediction. The methodology emphasizes optimizing neural network parameters for superior performance. Nonetheless, it is strongly advised to verify the method across various network configurations.

The study [68] introduces the MSCBL-ADN model to detect low-rate DDoS attacks, leveraging the ISCX-2016-SlowDos dataset. It uniquely integrates CNNs and Bi-LSTM for feature extraction and classification, surpassing traditional methods in both precision and speed. The study suggests the potential of attention networks and advanced attack categorization for future research, emphasizing its contribution to network security. However, it acknowledges limitations such as the exclusive focus on low-rate DDoS attacks and the necessity for validation across diverse datasets.

The study [69] introduces an innovative approach for detecting DDoS attacks in cloud environments, emphasizing the integration of ensemble feature selection with RNN-based classification to enhance accuracy and minimize false positives. Utilizing the public CICDDoS2019 dataset, the study validates the effectiveness of the Ensemble-RNN (ERNN) framework. Future research directions include exploring diverse datasets and real-world scenarios.

The study [70] proposes an approach using deep learning techniques for the detection of DDoS attacks in cloud environments. It combines ML decision tree and LSTM methods to improve accuracy. The study utilizes a public dataset and validates the efficacy of the proposed model. Although prevention and mitigation strategies are not explicitly discussed, further research could focus on exploring these areas.

The study [71] presents a hybrid model that integrates a stacked sparse AutoEncoder with a Deep Neural Network (DNN) for efficient DDoS attack detection in cloud computing environments. It utilizes Hyperband for hyperparameter optimization and is evaluated using the CICIDS2017 and NSL-KDD public datasets, demonstrating effectiveness in distinguishing between benign and DDoS traffic. Future research directions include exploring diverse datasets and real-world scenarios.

The study [72] introduces a novel DDoS attack detection method integrating a CNN-BiLSTM mechanism with an attention mechanism, aimed at addressing challenges such as high dimensionality and feature redundancy in network traffic data. By employing the random forest algorithm alongside Pearson correlation analysis for feature selection, and leveraging one-dimensional CNNs and BiLSTM networks for spatial and temporal feature extraction, the model significantly enhances detection accuracy and efficiency. The use of public datasets from CIC for evaluation underscores the method's robustness, showcasing superior performance in terms of accuracy, precision, recall, and F1 scores. Future research directions include enhancing real-time network traffic analysis capabilities and further improving the model's performance.

The study [73] presents a deep learning approach for network intrusion detection in cloud environments. Key contributions include data preprocessing, feature selection using random forest to identify 17 important features from 80, and a CNN model for attack detection and classification. Using the CSE-CICIDS2018 dataset, the model achieved 97.07% testing accuracy with high precision, recall, and F1-scores. Limitations include potential overfitting and focus on detection rather than prevention. Future research could explore generalizability, real-time detection, integrated mitigation strategies, and performance in various cloud architectures.

The paper [74] proposes deep neural network techniques for intrusion detection in cloud-based online music education, including fuzzy logic feature selection, a chronological salp swarm algorithm for DBN optimization, and an integrated GRU-CNN architecture. Key findings show models achieved 97%–98% accuracy, music-specific features outperformed standard one. Limitations include high computational requirements, need for continual retraining, and reduced interpretability.

The paper [75] presents DAERF, a hybrid deep learning approach for intrusion detection in Software Defined Networks (SDN). DAERF combines a Deep Autoencoder with a Random Forest classifier, achieving over 98% detection accuracy. The authors propose a three-layer adaptive framework for attack mitigation, incorporating entropy-based detection, DAERF in the control layer, and proactive service monitoring. Evaluated on the CICIDS2017 and NSL-KDD datasets, DAERF_IDS achieves 98.16% accuracy with a 1.85% false positive rate, outperforming previous methods. The approach shows minimal overhead on SDN controllers and uses native SDN traffic statistics as features. While effective, future work could explore more diverse datasets and real-world deployment.

The paper [76] introduces a novel federated learning approach for detecting next-generation malware in IoT environments using deep neural networks. The proposed framework enables secure collaboration across diverse IoT domains to build effective attack detection models on cloud–edge terminals. Key contributions include a distributed collaborative framework, a secure server aggregation mechanism, and a specialized deep neural network for network traffic classification. Using the BoT-IoT dataset, the model outperforms centralized and localized deep learning approaches across five IoT domains, achieving high attack detection rates while preserving privacy and minimizing communication costs. The study focuses on detection rather than prevention, with potential limitations in large-scale deployments and data imbalance. Future research could address scalability, resource management.

The study [77] presents MSCBL-ADN, a novel model combining multi-scale CNN and bidirectional LSTM for detecting LDDoS attacks. The approach enhances accuracy and reduces detection time by integrating spatial feature extraction with temporal relationship analysis, using an arbitration network for feature re-weighting and a dense connection network for classification. Evaluated on the ISCX-2016-SlowDos dataset, the model significantly outperforms state-of-the-art alternatives in accuracy and time performance. The study categorizes prevention strategies under Filtering and Redirection. The study's limitations include potential overfitting on the augmented dataset. Future work could explore attention mechanisms to further reduce detection time and address classification errors between attack types.

The study [78] proposes an ensemble model combining SVM, RF, NN, LSTM, and DRN classifiers, optimized by the TUDMA algorithm, for effective DDoS attack detection. Utilizing public datasets APA-DDoS and DDoS Botnet attacks, the study achieves a high accuracy of 95.34%. The methodology focuses on 'Detection', incorporating advanced data pre-processing and feature extraction techniques. Limitations include the need for real-time application. Future research could develop real-time detection and mitigation systems to enhance cloud security.

The paper [79] proposes a deep learning approach using convolutional neural networks (CNNs) for intrusion detection in cloud computing environments. The researchers utilize the public CSE-CICIDS2018 dataset, which contains a variety of cyberattack scenarios. The model incorporates multiple stages including data preprocessing, SMOTE balancing, feature selection using Pearson correlation, and model training/testing. Key contributions include achieving over 98.67% accuracy in detecting and classifying network intrusions, and demonstrating the model's effectiveness in a cloud environment. The paper focuses on detection rather than specific prevention strategies. Limitations include the need for real-time deployment testing and resilience against adversarial attacks. Future research could explore optimization strategies like genetic algorithms and integrating CNNs with other neural networks for enhanced performance.

The paper [80] proposes the FSS-DHODLAD technique for anomaly detection in cloud environments. The technique utilizes the Grasshopper Optimization Algorithm (GOA) for feature selection and the Attention Convolutional Bidirectional Long Short-Term Memory (AC-BLSTM) system for anomaly classification. The Deer Hunting Optimizer (DHO) further enhances performance by tuning the AC-BLSTM's hyperparameters. Experiments conducted on the CSE-CICIDS 2018 dataset, a public dataset, demonstrate the superior performance of FSS-DHODLAD compared to other state-of-the-art methods. Limitations include the dependency on benchmark dataset. Future research could explore integrating outlier detection methods to enhance the FSS-DHODLAD system's detection rate.

Table 4 presents a comprehensive examination of diverse deep learning methodologies employed to identify, thwart, and mitigate DDoS attacks, with a particular focus on cloud environments. Upon careful analysis of the data, we can extract the following key insights concerning the application of deep learning techniques in detecting, preventing, and mitigation DDoS attacks within cloud infrastructures:

Table 4
Deep learning approaches to combatting DDoS attacks in cloud environments: techniques, effectiveness, and future prospects.

N	Ref	Year	Datasets	Techniques	Advantages	Results	Prev/Miti	Research gap
1	[31]	2024	CICIDS2018, CICIDS2017, CICDoS2016	Honey badger optimization, Bi-LSTM	Superior accuracy, advanced preprocessing	Accuracy: 97% Sensitivity: 95% Specificity: 90% Error rate: 3% Precision: 94% F1 score: 87% FPR : 5% Kappa: 88%	No	Detection speed, false positives
2	[32]	2024	InSDN, BOT-IoT, UNSW-Sydney, simulated data	Stack-Ensemble model, fog computing	Reduced feature count, high accuracy	Accuracy: 99.99%	Yes	False positives, real-time detection
3	[33]	2024	CIDDS-001	CNN-LSTM-Transformer networks, genetic algorithm	High accuracy in real time detection	Accuracy: 99.97% Precision: 99.97% Recall: 99.97% F1 score: 99.97% Detection time: 5.18 s	Yes	Scalability, diverse attacks
4	[34]	2022	CICDDoS2019	Deep learning, signature-based detection	High accuracy, real-time anomaly identification	Accuracy: 99.83% Detection time: 3.02 s	Yes	Scalability, diverse attacks
5	[35]	2024	CICIDS2017	Deep neural networks	Effective in high-speed data traffic	Accuracy: 98.86% Precision: 98.92% F1 score: 99% Recall: 98.86%	Yes	Unbalanced dataset
6	[36]	2023	NSL-KDD, CICIDS2017	Gaussian Kernel Density, deep learning	Improved accuracy	Accuracy: 99.05% Precision: 97% F1 score: 96% Recall: 96%	Yes	Computational demands
7	[37]	2023	CICDDoS2019	RBF, LSTM networks	Effectiveness in identifying attacks	Accuracy: 99.05% Precision: 97% F1 score: 96% Recall: 96%	Yes	Generalizability
8	[38]	2023	CICDDoS2019	Hybrid detection algorithm, dynamic mitigation	Rigorous testing effectiveness	Detection rate: 95.32% False positive rate: 0.57%	Yes	Real-world data
9	[39]	2023	DDOS attack SDN	RNNs	High detection accuracy	Accuracy: 94.19% Precision: 92.15% F1 score: 94.27% PFR: 8.15%	No	Real-world data, network configurations
10	[40]	2023	NSL-KDD	Fractional calculus, ACVO, DNFN	High accuracy	Accuracy: 93.04% Precision: 87.45% TPR:90.88% TNR: 92.93%	Yes	Scalability, real-time processing
11	[41]	2024	InSDN, CICIDS2018, Kaggle DDoS, simulated data	Deep learning	Advantage over conventional techniques	Accuracy: 100%	No	Real-time performance
12	[42]	2024	Simulated data	CG-GRU, deep transfer learning	High detection rates, computational efficiency	Precision: 77.63% F1 score: 83.67% Recall: 91.11%	No	Adaptive thresholding, advanced models
13	[43]	2023	NSL-KDD, CICIDS2017	ABOA, DNN	High accuracy	99.05% accuracy	No	Scalability, adaptability
14	[44]	2023	BOT-IoT, NSL-KDD	Deep learning, optimization techniques	High detection accuracy	Accuracy: 91.70% TPR: 90.90% TNR: 90.90%	No	Real-time detection, feature selection
15	[45]	2023	CICIDS2017	Ensemble feature selection, CNN, LSTM	High accuracy and precision	Accuracy: 97.90% Precision: 98.30% F1 score: 98.10% Recall: 97.90%	Yes	Real-time data, diverse datasets
16	[46]	2023	NSL-KDD	Deep Belief Networks, LSTM, Particle Swarm Optimization	Superior metrics	Accuracy: 91.00% Precision: 95.00% F1 score: 94.00% Recall: 92.00%	No	Efficiency optimization, real-time data
17	[47]	2023	CICIDS2017, NSL-KDD, UNSW-NB15	Deep Generative learning Models, CDAAE, CDAAE-KNN	Increase in detection accuracy	AUC score: 97.50%	No	Scalability, imbalanced datasets

(*continued on next page*)

Table 4 (*continued*).

18	[48]	2021	CICIDS2017	WOA, DNN, homomorphic encryption	High detection accuracy	95.35% accuracy	No	New attack detection, dataset comprehensiveness
19	[49]	2023	DARPA LLS DDoS-1.0, CICIDS2017, CSIC-2010	MMFO, TL-DRNN	Reducing false positives and negatives	99.13% f1-score	Yes	Scalability, real-time detection
20	[50]	2024	CICDDoS2019	BRS, CNNs, filtering, rate limiting, iptables	Impressive detection accuracy	100% accuracy	Yes	False positives, real-world validation
21	[51]	2022	CICDDoS2019	DNN	High detection accuracy, low computational cost	97.07% accuracy	No	Computational efficiency, defense strategies
22	[52]	2022	ISCX 2012, Simulated data	Deep learning, SDN, filtering, blocking	High accuracy	98.88% accuracy	Yes	Model generalization
23	[53]	2022	Simulated data	Deep Belief Networks, SVMs	High precision rate	Accuracy: 99.78% TPR: 99.32% TNR: 99.67%	Yes	Accuracy in specific environments, data samples
24	[54]	2022	Simulated data	Harris Hawks Optimization, Particle Swarm Optimization, LSTM	Improved accuracy and efficiency	Accuracy: 98.53% Sensitivity: 99.09% Specificity: 97.80% Precision: 98.32% F1 score: 98.70% Inference time: 200.22 s	Yes	Applicability to diverse contexts
25	[55]	2022	CICDDoS2019, UNSW- NB15	Transformers, deep reinforcement learning	High accuracy	Accuracy: 99.25% AUC score: 98.70%	No	Model generalization
26	[56]	2023	CICIDS2017, NSL-KDD, KDDcup99	DBN-GRU, weighted features	High effectiveness	97.05% accuracy	No	Scalability, emerging attack patterns
27	[57]	2022	CICDDoS2019	DNN, CNN, LSTM	Superior performance of CNN model	99.99% accuracy	No	Diverse datasets, real-world scenarios
28	[58]	2021	Simulated data, KDD Cup	Decision Tree, KNN, Naive Bayes, DNN	Effective DNN algorithm	Precision: 98.00% F1 score: 99.00% Recall: 0.98%	Yes	DDoS detection optimization, Hadoop integration
29	[59]	2021	CICDDoS2019, Simulated data	GAN, adversarial training, IP flow analysis	Improved detection accuracy and speed	Accuracy: 94.38% Precision: 96.32% F1 score: 91.02% Recall: 86.25%	Yes	Deep learning techniques, diverse settings
30	[60]	2023	DDoS attack SDN	Metaheuristic optimization, multi-layer ensemble deep reinforcement learning	Superior performance	Accuracy: 98.19% Precision: 97.84% F1 score: 91.02% Recall: 98.19% AUC score: 98.19% Detection time: 1.07 s	Yes	Deep learning techniques, diverse settings
31	[61]	2023	Hogzilla, simulated data	DRL, LSTM, SDN	High accuracy rate, real-time packet classification	98.88% accuracy	Yes	DRL with Autoencoders integration
32	[62]	2023	NSL-KDD, BOT-IoT	GHLBO, Deep Stacked Autoencoder	High detection accuracy	Accuracy: 91.70% TPR: 90.90% TNR: 90.90% Detection time: 2.67 s	Yes	Algorithm optimization, diverse contexts
33	[63]	2024	CICDDoS2019, CICIDS2018, CICIDS2017, UNSW -NB15, and ISCX-IDS-2012	Risk assessment mechanism	High detection accuracy	Accuracy: 95.00% FPR: 3%	Yes	Applicability to diverse contexts
34	[64]	2024	Simulated data	Community detection	Improved effectiveness of filtering responses	Accuracy: 99.71% F1-score: 99.65%	Yes	Applicability to diverse contexts

(*continued on next page*)

Table 4 (*continued*).

35	[65]	2022	CICIDS2017, CICDDoS2019	ResNet-101 based KELM	High data delivery ratio, validation accuracy	Accuracy: 96.00%	No	Real-world data validation
36	[65]	2022	BUET-DDoS2020, CICIDS2017, CICDDoS2019	HGSO, chaos theory, CNN	High accuracy, innovative approach	Accuracy: 99.83%	No	Real-world data validation
37	[67]	2021	KDD Cup	Deep learning Binary Fruit Fly Algorithm	High detection accuracy	Accuracy: 99.96%	No	Real-world data validation
38	[68]	2024	ISCX-2016	CNN and BI-LSTM	High accuracy, innovative approach	Accuracy: 96.74% Precision: 96.77% F1 score: 96.74% Detection time: 5.38 s	No	Real-world data validation
39	[69]	2023	CICDDoS2019	Ensemble-RNN	High detection accuracy	Accuracy: 99.6% Precision: 99.7% Recall: 99.6%	No	Applicability to diverse contexts
40	[70]	2023	CICDDoS2019	LSTM-DT	Improved accuracy	Accuracy: 99.7% Precision: 99.22% F1 score: 99.7% Recall: 99.7%	No	Real-world data validation
41	[71]	2020	CICIDS2017, NSL-KDD	DNN, AE	High detection accuracy	Accuracy: 98.92% Precision: 99.8% F1 score: 98.57% Recall: 97.12%	No	Real-world data validation
42	[72]	2023	CICISDC2017, CICDDoS2019	CNN-LSTM-ATT	Improved accuracy	Accuracy: 95.67% Precision: 95.87% F1 score: 95.86% Recall: 95.9%	No	Real-time
43	[73]	2024	CICIDS2018	CNN	High detection accuracy	Accuracy: 97.07% Precision: 98.11% F1 score: 97.51% Recall: 96.93%	No	Applicability to diverse contexts
44	[74]	2024	CICIDS2017, NSL-KDD	GRU-CNN	High accuracy	Accuracy: 98.89% Precision: 97.30% F1 score: 98.60% Recall: 98.80%	No	High computational requirements
45	[75]	2024	CICIDS2017, NSL-KDD	Deep Autoencoder, Random Forest	High accuracy	Accuracy: 98.00% Precision: 98.89% F1 score: 98.92% Recall: 98.96%	Yes	Real-world data validation
46	[76]	2024	BoT-IoT	Federated learning, deep neural networks	High attack detection rates	Accuracy: 99.90% Precision: 99.90% F1 score: 99.90% Recall: 99.90%	No	Scalability, resource management
47	[77]	2024	ISCX-2016	Multi-scale CNN, bidirectional LSTM	High accuracy, reduced detection time	Accuracy: 96.74% Precision: 96.77% Recall: 96.74%	Yes	Applicability to diverse contexts
48	[78]	2024	APA-DDoS	SVM, RF, NN, LSTM, DRN, TUDMA	High detection accuracy	Accuracy: 95.80% Sensitivity: 97.3% Specificity: 96.6% Precision: 93.5% F1 score: 95.30%	No	Applicability to diverse contexts
49	[79]	2024	CICIDS2018	CNN, SMOTE, Pearson correlation	High accuracy	Accuracy: 100% Precision: 100% F1 score: 100% Recall: 100%	No	Applicability to diverse contexts
50	[80]	2024	CICIDS2018	Attention Convolutional BLSTM	High accuracy	Accuracy: 98.80% Precision: 98.09% F1 score: 97.91% Recall: 97.97%	No	Real-world data validation

1. **Detection Accuracy:** Most of the studies reported high detection accuracy rates, with some achieving up to 100% accuracy using advanced deep learning models like CNN-LSTM, Transformers, Ensemble models, and optimized techniques like genetic algorithms, metaheuristics, and ensemble feature selection. However, real-world data validation and generalization to diverse attack scenarios are still challenges.
2. **Techniques:** A wide range of deep learning techniques have been explored, including Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNNs), Deep Belief Networks (DBNs), Autoencoders (AEs), Transformers, Generative Adversarial Networks (GANs), and ensemble models. These techniques have shown promising results in terms of detection accuracy, precision, recall, and F1-scores.
3. **Datasets:** Numerous datasets have been utilized for training and testing the deep learning models, such as CICDDoS2019, CICIDS2017, CICIDS2018, NSL-KDD, UNSW-NB15, ISCX-IDS-2012,

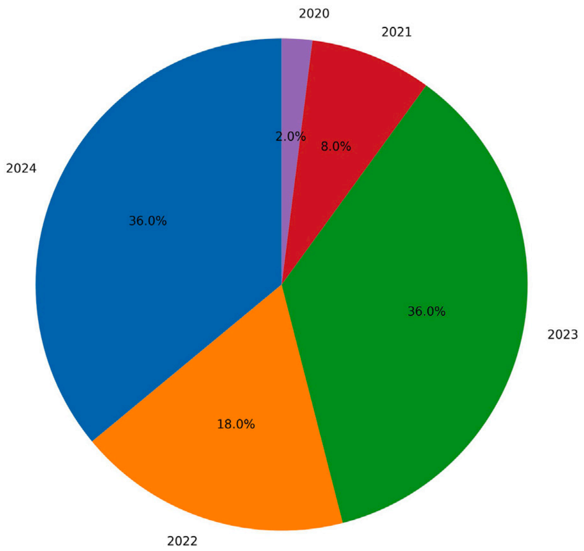

Fig. 10. The distribution of papers by years.

and simulated data. However, some studies highlight the need for more comprehensive and diverse datasets to improve generalization and real-world applicability.

4. **Prevention and Mitigation:** Several studies have focused on prevention and mitigation strategies, including filtering, blocking, rate limiting, software-defined networking (SDN), risk assessment mechanisms, and community detection techniques. These approaches aim to mitigate the impact of DDoS attacks and enhance network resilience.
5. **Research Gaps:** Despite the promising results, several research gaps have been identified, including:
   - Real-time detection and processing capabilities
   - Scalability and adaptability to handle large-scale and diverse attack scenarios
   - Reducing false positives and false negatives
   - Integrating deep learning with other techniques (e.g., homomorphic encryption, dynamic mitigation)
   - Optimizing computational efficiency and resource utilization
   - Validating models on real-world data and diverse network configurations
6. **Future Prospects:** The studies suggest potential future directions, such as adaptive thresholding, advanced model architectures (e.g., integrating Autoencoders with Deep Reinforcement Learning), optimization techniques (e.g., metaheuristics, chaos theory), and ensemble approaches. Additionally, exploring deep learning in conjunction with emerging technologies like fog computing, blockchain, and software-defined networking (SDN) could enhance DDoS attack prevention and mitigation capabilities in the cloud.

5.2. Some insights from deep learning studies for ddos attack detection, prevention and mitigation in the cloud

Fig. 10 illustrates the temporal distribution of research papers applying deep learning to DDoS attack defense in cloud environments from 2020 to 2024. The data reveals a significant upward trend in deep learning adoption for this purpose. The most recent years, 2023 and 2024, show the highest proportion, with 36.0% of papers each year focusing on deep learning methodologies. This represents a substantial increase from 2022, which accounted for 18.0% of papers. The earlier years demonstrate the initial stages of adoption, with 2021 representing 8.0% and 2020 only 2.0% of the papers. This distribution clearly indicates a rapid growth in the application of deep learning techniques for cloud-based DDoS defense strategies over the five-year period, suggesting an increasing recognition of deep learning's potential in addressing complex cybersecurity challenges in cloud computing environments.

Fig. 11 depicts the frequency distribution of datasets used in deep learning research papers for network security. CICIDS2017 emerges as the most prevalent, followed by CICDDOS2019 and NSL-KDD, highlighting their significance in the field. Notably, "simulated data" also features prominently, indicating researchers' frequent use of custom-generated datasets to address specific scenarios not covered by public datasets. This distribution underscores both the reliance on established benchmarks and the need for tailored data solutions in contemporary network security research.

The presence of "simulated data" as a category indicates a considerable number of studies opt to create and use their custom datasets tailored to the specific requirements of their experiments. This could be due to a variety of reasons, such as the need for data that matches specific conditions not met by public datasets, or the desire to test algorithms in a controlled environment where all variables are known and can be manipulated.

Further down the line, datasets like BOT-IOT, ISCX2012, and ISCX2016 show moderate use, with a range of other datasets like UNSW-Sydney, CIDDSS001, Kaggle DDoS, DARPA LLS DDOS 1.0, CSIC-2010, and BUET-DDoS2020 being utilized to a lesser extent. Each dataset's frequency of use could reflect its relevance, quality, or suitability for deep learning applications.

Fig. 12 presents the metrics used in deep learning research papers to evaluate model performance. The most commonly used metric, as shown by the tallest bar, is accuracy, indicating that the majority of papers prioritize overall correctness in their model evaluations. Precision, F1 Score, and Recall are also frequently utilized, suggesting a concern for not only the correctness of the positive predictions (precision) but also the balance between precision and recall (F1 Score) and the ability to identify all positive samples (recall).

The middle section of the chart, with notably lower bars, includes metrics like detection time and false positive rate, emphasizing the importance of timeliness and the avoidance of incorrect positive predictions in model assessment. The area under the curve (AUC) score is another significant metric used, reflecting the model's ability to distinguish between classes.

Towards the right end of the chart, metrics such as true positive rate, sensitivity, true negative rate, and error rate are less frequently reported in papers, but are still relevant to understanding specific aspects of model performance. The least used metrics shown are kappa and detection rate, which may suggest that they are less relevant.

The section reveals a significant advancement in the use of deep learning for DDoS attack detection, prevention, and mitigation, with a clear focus on improving accuracy, efficiency, and real-time capabilities. However, challenges such as scalability, computational demands, and the need for real-world validation point towards areas requiring further research and development. Future work in this field will likely explore more advanced deep learning models, optimization techniques, and hybrid approaches to address these challenges, ensuring that DDoS defense mechanisms can keep pace with the increasing complexity and frequency of attacks.

6. Advancements and challenges in traditional machine learning for defending against ddos attacks in the cloud

This section provides an overview of various studies that explore the application of machine learning techniques for detecting and mitigating DDoS attacks in cloud network environments.

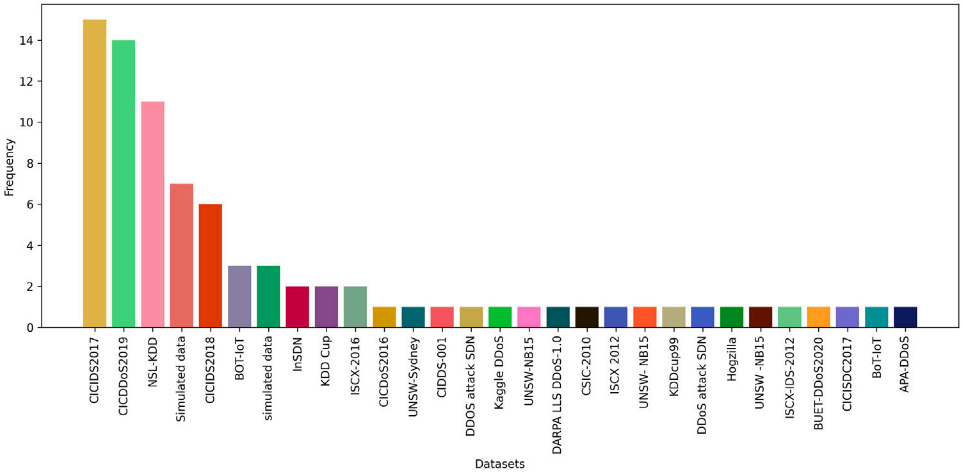

Fig. 11. Comparative analysis of dataset utilization.

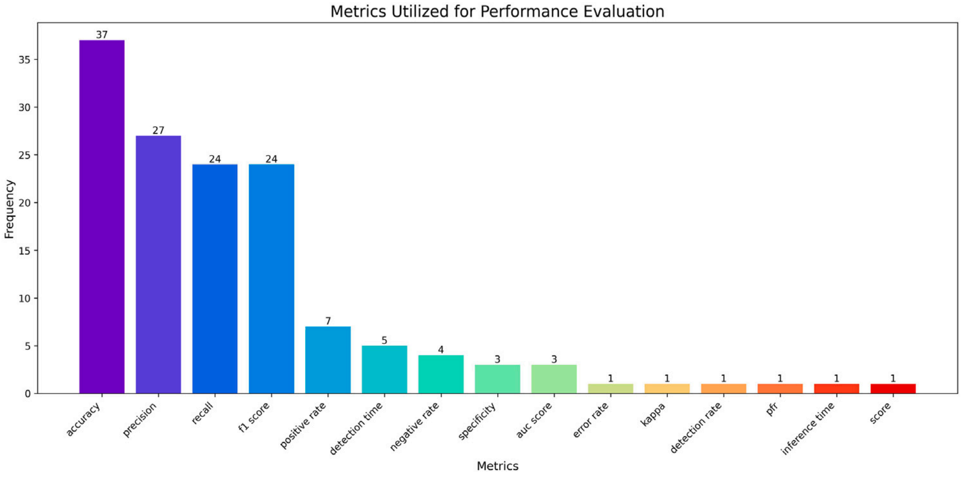

Fig. 12. Metrics utilized for performance evaluation in deep learning research papers.

6.1. Exploring machine learning techniques for DDoS attack detection in cloud computing environments

The main objective of the study [81] is to explore the application of the Naive Bayes algorithm for the detection of DDoS attacks in cloud computing. The study demonstrates the effectiveness of this algorithm by using simulated data. A comparison is made between Naive Bayes and the Random Forest algorithm, with Naive Bayes outperforming in terms of accuracy in identifying DDoS traffic. The study emphasizes the significance of machine learning in enhancing cybersecurity, especially in the preprocessing and analysis of data to distinguish between normal and malicious network traffic. However, it should be noted that the study has limitations, such as relying on simulated data. The future research directions, including real-time detection and the exploration of other machine learning techniques.

The study [82] introduces a novel approach to identify Distributed Denial of Service (DDoS) attacks in VANET (Vehicular Ad Hoc Network) Cloud by utilizing Random Forest and Decision Tree algorithms. The data used for the analysis is generated through NS2 simulations. The research highlights the exceptional accuracy of the proposed models in effectively differentiating between normal and DDoS traffic. Furthermore, it observes a noteworthy inverse correlation between energy consumption and packet delivery rate. Future research directions suggest further exploration of machine learning techniques and datasets to address evolving DDoS attack patterns.

The research [83] presents SWASTHIKA, a novel machine learning model designed to detect DDoS attacks. This model utilizes a distinctive similarity function that analyzes patterns in traffic attributes. To evaluate its performance, the researchers employed an IoT DoS/DDoS dataset from IEEE Dataport, which is accessible to the public. The results demonstrate that SWASTHIKA exhibits remarkable detection capabilities, surpassing current models by effectively identifying low and high-rate attacks. However, it is advisable to validate the model using real-world data to further improve its reliability.

This study [84] introduces a DDoS attack detection system for cloud computing using a Voting Extreme Learning Machine (V-ELM), a type of artificial neural network. It leverages two benchmark datasets, NSL-KDD and ISCX, from public sources for evaluation. The system demonstrates high accuracy, outperforming traditional backpropagation and other machine learning models. The research suggests V-ELM's effectiveness in accurately identifying DDoS attacks through majority voting among multiple ELMs. However, it is recommended further investigation into parameter optimization and real-world applicability to enhance the model's reliability and performance.

The study [85] presents the LCDT-M framework, which is designed for detecting and mitigating DDoS attacks in cloud environments based on Software-Defined Networking (SDN). The framework incorporates Greedy Feature Selection, Two Log Mean Clustering, and Decision Tree algorithms. To address the data shift problem, simulated data from the gureKddcup dataset is utilized, leading to an impressive accuracy of 99.83%. The framework demonstrates excellent capabilities in filtering malicious traffic while allowing normal traffic flow, surpassing traditional machine learning methods in terms of performance. However, it is recommended that future research explore other types of attacks beyond DDoS to ensure comprehensive network security.

The study [86] outlines a cloud DDoS attack detection model employing data fusion and machine learning classifiers, including Decision Trees, Naive Bayes, SVM, and KNN. Utilizing the publicly available CICDDoS2019 dataset, it demonstrates that the Decision Tree model outperforms others with a 99% accuracy rate. The study emphasizes leveraging machine learning to differentiate between benign and non-benign traffic, underscoring the effectiveness of data fusion in enhancing detection capabilities. Future research directions suggest further exploration of machine learning techniques and datasets to address evolving DDoS attack patterns.

The study [87] outlines the detection of cloud DDoS attacks through data fusion and machine learning classifiers, particularly emphasizing the Decision Tree model's exceptional accuracy with the CICDDoS2019 dataset, has been requested once more. This model underscores the efficacy of machine learning in distinguishing between benign and malicious traffic, and suggests the need for further investigation into these techniques to combat evolving DDoS threats as a potential avenue for future research.

The study [88] introduces DAD-CSP, a machine learning framework for DDoS detection, using Decision Tree, Naïve Bayes, and Random Forest models. It emphasizes on feature selection to enhance model training. Random Forest was found to be the most effective, achieving 92% accuracy. However, it is recommended to undertake real-world data validation to enhance the model's accuracy and reliability further.

The study [89] presents an enhanced DDoS attack detection system for cloud environments, employing a Back Propagation Neural Network optimized with Bacterial Colony Optimization (BCO-BPNN). This method aims to refine the network's performance by optimizing connection weights and biases. It is tested on public datasets: NSL-KDD, ISCXIDS2012, CIC-IDS2017, and UNSW-NB15, demonstrating superior accuracy and detection rates compared to traditional methods. The study suggests the BCO-BPNN model's effectiveness in detecting DDoS attacks. Nevertheless, it is advisable to conduct real-world data validation.

The study [90] introduces a feature selection-based method for DDoS attack prevention in cloud systems, utilizing the CICID2018 dataset for evaluation. By applying Pearson Correlation Coefficient, Random Forest Feature Importance, Mutual Information, and Chi-squared tests, the approach significantly increases detection accuracy, particularly with the combination of PCC and RFFI, achieving up to 99.27% accuracy. This underscores the importance of precise feature selection in enhancing DDoS attack detection. Further exploration into diverse datasets and the application of advanced machine learning techniques are recommended to enhance security measures.

The study [91] proposes an SVM-based DEHO classifier for DDoS attack detection in cloud computing, incorporating KPCA for optimal feature extraction. It evaluates the classifier's effectiveness using four public datasets: NSL-KDD, UNSW-NB15, ISCX ID, and CICIDS2017, demonstrating superior performance over other methods. However, validating the approach with real-world data is recommended for enhanced credibility.

The study [92] presents a DDoS attack detection system in E-government cloud environments, utilizing PCA for feature selection and clustering algorithms like DBSCAN, Agglomerative Clustering, and k-means for data analysis. The methodology is tested on the CICIDS2018, NSL-KDD, and HTTP CSIC 2010 datasets, showing high effectiveness in distinguishing between benign and attack traffic. The study emphasizes the value of feature selection and clustering for security in cloud networks. For improved credibility, it is highly recommended to validate the approach by utilizing real-world data.

The study [93] introduces a hybrid optimization-enhanced SVM for DDoS detection in IDS, leveraging a combination of Harris Hawks Optimization and Particle Swarm Optimization to fine-tune SVM parameters. Employing the NSL-KDD dataset, this approach showcases superior accuracy and efficiency in identifying DDoS threats compared to standard methods. Further exploration into diverse datasets and the application of advanced machine learning techniques are recommended to enhance security measures.

The study [94] presents an advanced DDoS attack detection model combining a novel feature selection method with an ensemble-based classifier, specifically a Random Forest classifier. Utilizing several publicly available datasets, including CIC-DDoS2019 and others, the model demonstrates exceptional detection accuracy, outperforming existing techniques across various metrics. This research underscores the effectiveness of combining hybrid feature selection with ensemble classifiers in cybersecurity, achieving nearly perfect accuracy and recall rates. It highlights the potential of this approach in real-time DDoS attack detection, suggesting further validation and exploration in diverse real-world scenarios.

The study [95] introduces a framework for attack detection and mitigation in SaaS using Deep Belief Networks optimized by a novel algorithm. It employs a unique bait strategy for mitigation, tested on public datasets (CICDDoS2019, DDoS-SDN and CICIDS2018), showcasing improved network performance. This approach highlights the effectiveness of integrating machine learning with optimization techniques for cybersecurity, suggesting further real-world application and testing.

The study [96] presents a three-level machine learning classification architecture for detecting DDoS attacks at the application layer, using XGBoost and LGBM within a CatBoost classifier framework. It employs the CICDDoS2019 dataset for validation. The architecture significantly improves detection accuracy and efficiency in both binary and multiclass classification of DDoS attacks, showcasing substantial advancements over traditional ML algorithms. For enhanced security measures, a thorough examination of diverse datasets is advised.

The study [97] proposes a DDoS attack detection method in cloud computing environments, emphasizing feature selection techniques (Mutual Information and Random Forest Feature Importance) and employing machine learning models (Random Forest, Gradient Boosting, K Nearest Neighbor, Logistic Regression, and a Weighted Voting Ensemble). Utilizing the CICIDS 2017 and CICDDoS 2019 public datasets, the study aims to minimize misclassification errors in DDoS detection. The Random Forest model, with a select set of 19 features, showcased notable accuracy. It is recommended further validation and exploration in diverse real-world scenarios.

The study [98] introduces an ensemble-based approach for DDoS attack detection in cloud computing, employing majority voting among classifiers like Naïve Bayes, Decision Trees, SVM, and K-NN. It utilizes the CICDDoS2019 dataset, highlighting a significant improvement in detection accuracy, sensitivity, and specificity. It is recommended further validation and exploration in diverse real-world scenarios.

The study [99] presents a Decision Tree Detection (DTD) model aimed at detecting DDoS attacks in SDN-based cloud environments. It employs the Greedy Feature Selection (GFS) algorithm and Decision Tree Algorithm (DTA) for enhanced attack detection accuracy, specifically targeting the data shift problem. The model is validated using the gureKddcup dataset, demonstrating significant improvements in detection rates and accuracy. It is recommended further validation and exploration in diverse real-world scenarios.

The study [100] introduces the Perplexed Bayes Classifier model for DDoS attack detection in cloud computing, demonstrating improved performance over traditional Naïve Bayes and Random Forest algorithms. Utilizing the NSL-KDD dataset for training and testing, the model achieves an accuracy of 99% with feature selection, outperforming other machine learning algorithms and nature-inspired feature selection methods like Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). To strengthen security measures, conducting an in-depth analysis of a wide range of datasets is recommended.

This study [101] focuses on utilizing the Naive Bayes algorithm for the detection and prevention of DDoS attacks in cloud computing environments. It explores various cyber-attacks against cloud services and employs both Naive Bayes and Random Forest algorithms for mitigation. The research demonstrates the application of these algorithms in enhancing system resilience against such threats, using OS like ParrotSec for simulation. It is recommended to further validate and test in a variety of real-world scenarios.

The study [102] proposes a novel machine learning (ML) approach for online detection of DNS-based Distributed Reflection Denial of Service (DRDoS) attacks in Software Defined Networking (SDN) environments. It utilizes ML algorithms to analyze DNS traffic flows, distinguishing between normal and malicious traffic. The study employs the CICIDS2017 public dataset and additional malicious traffic generated using the Scapy tool. The method demonstrates improved detection accuracy and speed compared to existing techniques, emphasizing the effectiveness of decision trees, Support Vector Machine (SVM), and Gradient Boosting Classifier (GBC) in detecting DRDoS attacks. Future work aims to explore deep learning methods and identify other types of DRDoS attacks.

The study [103] presents a source-based defense against DDoS attacks in SDN environments, utilizing sFlow and an improved Self-Organizing Map (SOM) model. This approach combines sFlow-based macro-detection to cover entire networks for DDoS attack perception, and SOM-based micro-detection for identifying attack traffic, guided by a global view from the controller. The method was validated through open data and simulated attack scenarios, showing superior detection performance over traditional methods like k-means and k-medoids. This innovative defense mechanism highlights the advantages of SDN for organizing collaborative and efficient DDoS mitigation strategies. The study acknowledges the limitations of simulating attack scenarios and stresses the importance of validating in real-world conditions.

The study [104] introduces the RMPSOM-SDNDM scheme, a novel DDoS attack prevention mechanism for SDN-based cloud computing environments, leveraging the Rival-Model Penalized Self-Organizing Map (RMPSOM). This approach emphasizes enhancing DDoS attack detection accuracy by maintaining the topological structure of data through penalizing rival models. The model achieves significant improvements in sensitivity, specificity, and accuracy rates in detecting DDoS attacks, compared to baseline mitigation strategies. It is recommended to conduct more research on the development of methods for dynamically and responsively updating network security rules.

The study [105] discusses an optimized Extreme Learning Machine (ELM) model, SaE-ELM, enhanced for DDoS attack detection in cloud computing. It introduces improvements including adaptive crossover operator selection and automatic determination of hidden neurons. Evaluated using NSL-KDD, ISCX IDS 2012, UNSW-NB15, and CICIDS 2017 datasets, the model showcases detection accuracies up to 99.99%, outperforming both the original SaE-ELM and other advanced techniques. However, it exhibits longer inference time.

The study [106] introduces a hybrid machine learning technique for DDoS attack detection in cloud computing, combining Extreme Learning Machine (ELM) with Blackhole Optimization. It assesses the model's performance using four benchmark datasets: NSL KDD, ISCX IDS 2012, CICIDS2017, and CICDDoS2019, achieving high accuracies. The technique outperforms other ELM-based methods and ANN models trained with Blackhole Optimization and backpropagation. This research underlines the effectiveness of hybrid approaches in enhancing DDoS detection accuracy in cloud environments. The inference time of this process is prolonged.

The study [107] introduces a novel approach to detect DDoS attacks in SDNs using a cloud–edge collaboration framework and an algorithm based on SOM and KD-tree. The effectiveness of the method is evaluated through experiments. Future research directions include enhancing the speed of the KD-tree algorithm.

The study [108] introduces a novel approach for detecting DDoS attacks by utilizing a wrapper feature selection model employing binary particle swarm optimization (BPSO) algorithm alongside a decision tree classifier. Its goal is to enhance accuracy and efficiency by selecting a minimal set of relevant features from vast DDoS datasets (CICIDS2018, CICIDS2017, CICDoS2016). Demonstrating intelligence, the model identifies 19 pertinent features out of 76, then evaluates them using various machine learning algorithms like decision tree, random forest, and multi-layer perceptron. Remarkably, it achieves high accuracy rates across these algorithms. Comparison with previous models highlights its efficacy. It is recommended further validation and exploration in diverse real-world scenarios.

This study [109] presents a Stacked Ensemble (SE) approach to improve the generalization of classifier predictions in detecting Distributed Denial of Service (DDoS) attacks in cloud networks. The proposed SE model consists of a two-layered architecture, with base models stacked at level-0 and a final model at level-1, which is trained using the predictions of the base models. The performance of the SE model is evaluated using the CICIDS-2017 dataset and is shown to outperform existing techniques in detecting DDoS attacks, achieving an accuracy of 99.9%. The study employs a combination of ensemble techniques and feature extraction to achieve these results. However, the study does not discuss specific strategies for prevention or mitigation of DDoS attacks. The limitations of the study include the potential for overfitting, as well as the need for further evaluation on diverse datasets. Future research could explore the application of the SE model to other types of cybersecurity threats and investigate techniques to improve its robustness and adaptability.

The study [110] introduces an ensemble-based machine learning method for detecting DDoS attacks, merging supervised and unsupervised algorithms. Testing on NSL-KDD, UNSW-NB15, and CICIDS2017 datasets, the ensemble outperforms single-classifier systems, detecting up to 99.1% of attacks with minimal false alarms. Future work may refine ensemble methods, explore feature selection, and assess real-world network data efficacy.

The study [111] evaluates the efficiency of clustering-based DDoS attack detection using metaheuristic search techniques for feature selection, specifically testing the BestFirst algorithm's performance. It leverages the CICIDS2017 dataset, concluding that enhancements in metaheuristic search parameters do not substantially surpass the BestFirst method in detecting DDoS attacks. The dimensionality challenge is seen as a constraint and it is suggested that additional research be conducted on DDoS detection techniques using diverse datasets and a wider set of metaheuristic parameters.

The study [112] proposes a multi-modal, noise-robust DDoS attack detection architecture for large-scale networks, utilizing tensor-based Singular Value Decomposition (SVD) and XGBoost classification model. It introduces a novel framework that includes data representation through tensors, a multi-modal denoising algorithm leveraging tensor SVD, and an efficient anomaly detection system suitable for large networks. The methodology employs simulations to validate its effectiveness, achieving a high detection rate of 98.84%. This work highlights the challenges of accurately detecting DDoS attacks in complex network environments.

The study [113] proposes an intelligent system for DDoS detection in Smart Environments (SEs) using Machine Learning (ML), supported by Fog and Cloud Computing. It focuses on traffic segmentation and features selection to enhance detection accuracy and reduce data processing volume. Real network traffic data demonstrates the system's high accuracy (99%) in detecting DDoS attacks. It employs traffic segmentation to distinguish between IoT and personal device data, enhancing the detection process. A significant limitation is the necessity for further evaluation in different settings to validate the system's effectiveness broadly.

The study [114] explores ML-based DDoS detection and identification using cloud telemetry, particularly focusing on SYN Flood and GET

Flood attacks. It utilizes datasets from an experimental testbed based on OpenStack for controlled attack scenarios. The study demonstrates an 87% accuracy in detecting these attacks, significantly outperforming traditional IDS like Snort in specific scenarios. Key contributions include leveraging native cloud telemetry for DDoS detection, an approach promising for non-intrusive and efficient threat mitigation in cloud environments. However, a significant limitation is the necessity for further evaluation in different settings to validate the system's effectiveness broadly.

The study [115] introduces a system for detecting DDoS attacks in OpenStack-based private clouds using Apache Spark for distributed processing. It explores the use of Spark clusters for real-time DDoS attack detection, comparing machine learning models and selecting the random forest model for its superior accuracy and efficiency. The study demonstrates the system's effectiveness in reducing detection times and improving efficiency, utilizing both benchmark and real-time datasets for evaluation. Future research aims to explore deep learning models and parameter tuning for enhanced computational efficiency in detecting various types of DDoS attacks.

The study [116] presents an optimized Radial Bias Function Neural Network (RBF-NN) for DDoS detection in cloud environments, utilizing a Harmonic Mean based optimization algorithm. It emphasizes enhanced detection accuracy through advanced feature analysis on the CICDDoS2019 and UNSW-NB15 datasets. A noted limitation includes the challenge of determining the optimal threshold for attack detection. it is highly recommended to validate the approach by utilizing real-world data.

The study [117] focuses on mitigating DDoS attacks in SDN environments, leveraging the ONOS Flood Defender. It employs machine learning models, specifically XGBoost and Multilayer Perceptron, to analyze data from public datasets: CICDoS2017, CICDDoS 2019, CICIDS2018, and InSDN. Key contributions include high detection accuracy and rapid mitigation strategies. The scalability of the proposed solutions could be examined through further research in a range of network environments and in response to developing DDoS attack techniques.

The study [118] develops an Optimized Dual Intrusion Detection System (OD-IDS) leveraging machine learning for DDoS attack detection in SDN environments. It combines hyperparameter tuning, Recursive Feature Elimination, and a Deep Grid Network, using both public (CICIDS2019) and custom-simulated datasets. The approach significantly reduces feature dimensions, enhancing prediction efficiency and outperforming existing IDS models. Further investigation could explore the adaptability of the proposed solutions across diverse network settings and against evolving DDoS attack strategies.

The study [119] focuses on improving the Gaussian Naïve Bayes (GNB) classifier for detecting DDOS attacks in cloud computing by employing an iterative feature selection method and a novel data preprocessing strategy to address the zero-frequency problem and data imbalance. Utilizing the public CICD2018 dataset, it demonstrates significant enhancements in accuracy and precision. The study proposes 'Filtering' for feature selection. Despite its achievements, it is highly recommended to validate the approach by utilizing real-world data.

The study [120] presents a novel DDoS detection framework using the Matching Pursuit and Wavelet techniques, integrated with an artificial neural network. It focuses on resource depletion attacks, achieving a detection accuracy above 99% and a false positive rate below 0.7% using data from the CAIDA dataset and simulations conducted at Boğaziçi University. The study highlights the framework's effectiveness in low-density DDoS attack detection and suggests further research on adapting detection mechanisms to evolving network traffic patterns.

The paper [121] presents an integrated SDN framework called RDAER for early detection of DDoS attacks in cloud computing environments. It combines feature selection, clustering, time series analysis, and event correlation techniques to enable fast and accurate detection of DDoS traffic patterns at the SDN switch level. Using the public CICDDoS2019 dataset, RDAER achieved 99.92% accuracy and a detection time of 20 s, outperforming existing methods. Key aspects include using only two critical features (USIA and NUDIA), employing DBSCAN clustering and parallel processing of clusters, applying time series techniques like ARIMA for anomaly prediction, and utilizing rule-based event correlation to classify traffic. The framework enables early detection at switches before attacks reach the controller and activates countermeasures to block attack traffic. Compared to previous approaches, RDAER demonstrates significant improvements in accuracy and detection speed for DDoS detection in SDN-based cloud networks.

The paper [122] presents an innovative approach for detecting Distributed Denial of Service (DDoS) attacks using an evolutionary K-Nearest Neighbors (KNN) model optimized with a genetic algorithm. The study employs various machine learning classifiers, including Random Forest, Decision Tree, and Gradient Boosting, to detect DDoS attacks. The research utilizes the APA-DDoS dataset, which is publicly available. Key findings show that Random Forest achieves the highest accuracy in detecting attacks initially. The genetic algorithm optimization further enhances classifier performance, with KNN emerging as the top performer, demonstrating a 25% increase in accuracy compared to AdaBoost and Logistic Regression. The study's limitations include the use of a single dataset and the potential for overfitting. Future research could explore real-world malware samples and deep learning algorithms for more robust DDoS detection.

Table 5 offers a comprehensive analysis of the current state and advancements in defense strategies against DDoS attacks within cloud computing environments. This emphasizes the widespread application of Machine Learning (ML) methods, including Naive Bayes, Random Forest, Decision Trees, and XGBoost, which have demonstrated considerable success in identifying and counteracting DDoS attacks. These ML models achieve remarkable accuracy, often surpassing 99%, showcasing their capability to distinguish between benign and malicious traffic accurately in complex attack scenarios.

A significant aspect of the research focuses on the enhancement of ML models through advanced feature selection, optimization techniques, and the integration of novel algorithms. Techniques like Principal Component Analysis (PCA), hybrid optimization algorithms, and ensemble methods, including data fusion and deep belief networks, have been explored to improve the models' accuracy, efficiency, and adaptability to varied DDoS attack patterns.

However, a recurring theme across studies is the recognition of a gap in real-world data validation. While many models exhibit impressive performance on simulated or benchmark datasets such as NSL-KDD, CICIDS2017, and CICDDoS2019, there is a critical need for testing these models in real-world network environments to validate their effectiveness and generalizability. This underscores the importance of employing diverse datasets and real-world attack scenarios in research to ensure the practical applicability of DDoS defense strategies.

Further exploration is encouraged in areas such as ensemble and hybrid ML approaches, which combine multiple detection techniques or integrate ML with other computational methods to achieve superior detection and mitigation results. The potential of cloud–edge collaboration is also highlighted, suggesting a synergistic approach that leverages both cloud computing and edge computing resources for efficient and less intrusive DDoS mitigation.

Despite the focus on detection, there is a need for more research into practical prevention and mitigation strategies. While some studies mention approaches for filtering malicious traffic or leveraging cloud services for real-time attack mitigation, comprehensive solutions that encompass both detection and active defense mechanisms are essential for a robust DDoS defense strategy.

In conclusion, the insights gathered from the table reveal significant progress in the application of ML techniques for DDoS defense in cloud environments. These approaches demonstrate high levels of accuracy and performance, yet the necessity for further research into real-world validation, diverse dataset evaluation, and the development of integrated prevention and mitigation strategies remains evident. Addressing these gaps is crucial for advancing the effectiveness of DDoS defense mechanisms in practical, evolving cloud computing landscapes.

Table 5
Machine learning approaches to combatting DDoS attacks in cloud environments: techniques, effectiveness, and future prospects.

N	Ref	Year	Datasets	Techniques	Advantages	Results	Prev/Miti	Research gap
1	[81]	2024	Simulated data	Naive Bayes, Random Forest	High accuracy in DDoS detection	Accuracy: 99.78%	No	Real-time detection, other ML techniques
2	[82]	2024	Simulated data	Random Forest, Decision Tree	High accuracy, energy efficiency	Accuracy: 99.59%, Precision: 99.67%, Recall: 99.51%, F1-score: 99.59%	No	Further ML exploration, diverse datasets
3	[83]	2022	IEEE Dataport IoT DoS/DDoS	SWASTHIKA model	High detection capabilities	Accuracy: 90.91%	No	Real-world data validation
4	[84]	2020	NSL-KDD, ISCX	V-ELM	High accuracy, outperforms traditional models	Accuracy: 99.18%, Sensitivity: 99.50%, Specificity: 98.86%, Training time: 2.76 s	No	Parameter optimization, real-world applicability
5	[85]	2023	gureKddcup	LCDT-M framework	High accuracy, filters malicious traffic	Accuracy: 99.83% Error rate: 0.17%	Yes	Explore other attack types
6	[86]	2023	CICD-DoS2019	Data fusion, ML classifiers	High accuracy, effective differentiation	Accuracy: 99%, Precision: 99%, Recall: 99%, F1-score: 99.%	No	Further ML exploration, diverse datasets
7	[87]	2023	CICD-DoS2019	ML classifiers, Decision Tree	High accuracy	Accuracy: 99.07%	No	Further ML exploration, diverse datasets
8	[88]	2023	Simulated data	Decision Tree, Naïve Bayes, Random Forest	Effective feature selection	Accuracy: 92%, Precision: 85%, Recall: 75%, F1-score: 79%	No	Diverse real-world scenarios
9	[89]	2023	NSL-KDD, ISCXIDS2012, CIC-IDS2017, UNSW-NB15	BCO-BPNN	Superior accuracy and detection rates	Accuracy: 99.87%, Sensitivity: 98.76%, Specificity: 99.65%, F1-score: 99.27%	No	Real-world data validation
10	[90]	2023	CICID2018	Feature selection methods	High detection accuracy	Accuracy: 99.27%, Precision: 97.60%	Yes	Advanced ML techniques, diverse datasets
11	[91]	2022	NSL-KDD, UNSW-NB15, ISCX, CICIDS2017	SVM-based DEHO, KPCA	Superior performance	Accuracy: 99.99%, Sensitivity: 100%, Specificity: 100%, F1-score: 100%	No	Real-world data validation
12	[92]	2022	CICIDS2018, NSL-KDD, HTTP CSIC 2010	PCA, clustering algorithms	High effectiveness	Accuracy: 99.03%, Precision: 98.22%, Recall: 99.43%, F1-score: 99.33%	No	Real-world data validation
13	[93]	2022	NSL-KDD	Hybrid optimization-enhanced SVM	Superior accuracy and efficiency	Accuracy: 97.05%, Sensitivity: 97.62%, Precision: 97.62%, F1-score: 97.67%	No	Advanced ML techniques, diverse datasets
14	[94]	2024	CICD-DoS2019, DDoS-SDN, CICIDS2018, DDoS-botnet, APA-DDoS	Novel feature selection, Random Forest	Nearly perfect accuracy and recall	Accuracy: 100%, Precision: 100%, Recall: 100%, F1-score: 100%, AUC score: 100%	No	Real-world scenarios validation
15	[95]	2022	CICD-DoS2019, DDoS-SDN, CICIDS2018	Deep Belief Networks, novel algorithm	Improved network performance	Accuracy: 99.99%	Yes	Real-world application and testing

(continued on next page)

6.2. Some insights from machine learning studies for ddos attack detection, prevention and mitigation in the cloud

Fig. 13 provides a visual breakdown of the proportion of studies published over a five-year period, each contributing to the field of machine learning applications within the context of defending against DDoS attacks in cloud computing environments. The selection of studies prioritizes a focus on recent research. Specifically, the study choices are weighted towards more recent publications, starting with a 7.1% share of all studies in 2020, increasing to 16.7% in 2021, peaking at 31.0% in 2022, and maintaining a significant presence with 21.4% in 2023 and 23.8% in 2024. This trend indicates a consistent focus on recent research.

Fig. 14 illustrates the use of various datasets in studies related to defense strategies against DDoS attacks in cloud environments using machine learning techniques. It is evident that 'Simulated data' is the most frequently used, suggesting that researchers often create custom datasets based on their specific requirements. Following this, 'CICD-DoS2019', 'NSL-KDD' and 'CICDDoS2017' are the most commonly used

Table 5 (*continued*).

16	[96]	2022	CICD-DoS2019	XGBoost, LGBM, CatBoost	Improved detection accuracy and efficiency	Accuracy: 99.79%, Sensitivity: 85%, Precision: 97%, F1-score: 91%	No	Diverse datasets examination
17	[97]	2022	CICIDS 2017, CICDDoS 2019	ML models, feature selection	Notable accuracy with Random Forest	Accuracy: 99.99%	No	Diverse real-world scenarios
18	[98]	2022	CICD-DoS2019	Majority voting among classifiers	Significant improvement in detection	Accuracy: 98.02%, Sensitivity: 97.45%, Specificity: 98.65%	No	Diverse real-world scenarios
19	[99]	2022	gureKddcup	GFS, DTA	High detection rates and accuracy	Accuracy: 98.42%, Precision: 99.99%, True positive rate: 98.5%, F1-score: 99.2%	No	Diverse real-world scenarios
20	[100]	2022	NSL-KDD	Perplexed Bayes Classifier, feature selection	High detection rates and accuracy	Accuracy: 99.15%, Sensitivity: 99.10%, Specificity: 99.22%	No	In-depth analysis of diverse datasets
21	[101]	2024	Simulated data	Naive Bayes, Random Forest	Enhances system resilience	Accuracy: 99.78%	Yes	Real-world scenario testing
22	[102]	2022	CICIDS2017, Simulated data	ML algorithms, DNS traffic analysis	Improved detection accuracy and speed	Accuracy: 100%, Precision: 100%, Recall: 100%, F1-score: 100%, Detection time: 0.15 s	No	Deep learning methods
23	[103]	2022	Simulated data	sFlow, improved SOM	Efficient DDoS mitigation strategies	Detection rate: 95%	Yes	Diverse real-world scenarios
24	[104]	2021	Simulated data	RMPSOM	Improved detection accuracy	Precision: 98.9%, Recall: 98.6%	Yes	Diverse real-world scenarios
25	[105]	2021	NSL-KDD, ISCX IDS 2012, UNSW-NB15, CICIDS 2017	SaE-ELM	High detection accuracies	Accuracy: 99.80%, Sensitivity: 100%, Specificity: 100%	No	Longer inference time
26	[106]	2021	NSL KDD, ISCX IDS 2012, CICIDS2017, CICD-DoS2019	ELM, Blackhole Optimization	High accuracies, outperforms ELM and ANN	Accuracy: 99.23%, Sensitivity: 100%, Specificity: 100%	No	Prolonged inference time
27	[107]	2021	Simulated data	Cloud-edge collaboration, SOM, KD-tree	Effective detection method	Recall: 99.5%, F1-score: 99.5%,	No	Speed enhancement for KD-tree algorithm
28	[108]	2021	CICIDS2018, CICIDS2017, CICDoS2016	BPSO, decision tree	High accuracy rates	Accuracy: 99.59%, Precision: 99.24%, Recall: 99.93%, F1-score: 99.59%	No	Diverse real-world scenarios
29	[109]	2023	CICIDS2017	Stacked Ensemble (SE)	Improved generalization	Accuracy: 99.9%, Precision: 99.99%, Recall: 99.99%, F1-score:9.99%, Specificity: 99.99%, FPR: 0.12%, FNR: 0.1%	No	Real-world data validation
30	[110]	2024	NSL-KDD, UNSW-NB15, CICIDS2017	Ensemble ML methods	High detection rate, minimal false alarms	Up to 99.1% detection	No	Real-world network data efficacy
31	[111]	2024	CICIDS2017	Clustering, BestFirst	Enhancements in detection	Detection rate: 100%. FPR: 0%	No	Dimensionality challenge

(*continued on next page*)

public benchmarks. These public datasets are essential for validating proposed defense strategies.

The prevalence of simulated data may be due to difficulties in obtaining real-world DDoS attack data because of privacy issues, the rare occurrence of specific attack types, or the need for controlled experimental conditions. Researchers might generate simulated data to study particular features or characteristics of DDoS attacks that are not available in existing public datasets.

Furthermore, the choice of dataset may be influenced by the specific research questions and methodologies employed in DDoS defense studies. Researchers focusing on particular aspects of DDoS defense, such as detection, mitigation, or resource allocation, may gravitate towards datasets that align with their research objectives and provide the necessary features and attack scenarios to validate their proposed solutions.

Table 5 (*continued*).

32	[112]	2023	Simulated data	Tensor SVD, XGBoost	High detection rate	Accuracy: 98.84%, FAR: 0.82%, Recall: 99.93%, F1-score: 98.74%	No	In-depth analysis of diverse datasets
33	[113]	2021	Simulated data	ML	High accuracy in SEs	99% accuracy	No	Evaluation in different settings
34	[114]	2021	Simulated data	Cloud telemetry, ML	Non-intrusive, efficient mitigation	Accuracy: 87.37%, Recall: 87.28%, F1-score: 85.91%	No	Evaluation in different settings
35	[115]	2020	KDD Cup, Simulated data	Apache Spark, ML models	Reduced detection times, improved efficiency	Accuracy: 99.91%, FPR: 0.3%	No	Deep learning models, parameter tuning
36	[116]	2022	CICD-DoS2019, UNSW-NB15	RBF-NN	Enhanced detection accuracy	Accuracy: 88.59%, Precision: 89.49%, Recall: 89.36%, F1-score:88.59%, Specificity: 89.12%, FPR: 10.88%, FNR:10.64%	No	Optimal threshold determination
37	[117]	2024	CICDoS2017, CICDDoS 2019, CICIDS2018, InSDN	XGBoost and MLP	High detection accuracy	Accuracy: 99.8%	Yes	Real-world network data efficacy
38	[118]	2024	CICD-DoS2019, simulated data	ML	High detection accuracy	Accuracy: 100%, Precision: 100%, Recall: 100%, F1-score:100%,	No	Applicability to diverse contexts
39	[119]	2023	CICIDS2018	Gaussian Naïve bayes	Enhanced detection accuracy	Accuracy: 97.57%, Precision: 91.26%, Recall: 99.98%, F1-score: 98.69%	No	Real-world network data efficacy
40	[120]	2020	CAIDA, simulated data	ANN	High detection accuracy	Accuracy: 99.83%, True positive rate 99.93%, False positive rate: 0.62%, AUC Score: 100%	No	Applicability to diverse contexts
41	[121]	2024	CICD-DoS2019	RFE, DBSCAN, time series analysis	High accuracy	Accuracy: 99.92%, Precision: 99.99%, Recall: 99.99%, F1-score: 99.99%	Yes	Diverse real-world scenarios
42	[122]	2024	APA-DDoS	Evolutionary K-Nearest Neighbors	High accuracy	Accuracy: 100%, Precision: 100%, Recall: 100%, F1-score: 100%	No	Applicability to diverse contexts

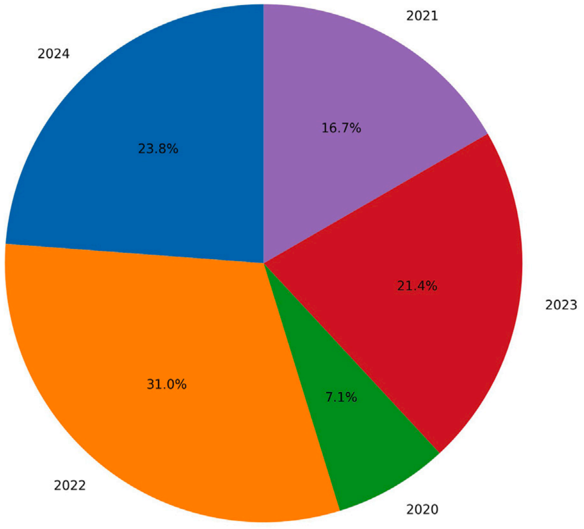

Fig. 13. The distribution of studys by years.

Fig. 15 presents an analysis of various performance metrics critical to the detection of DDoS attacks in cloud computing environments. The focus is on understanding the significance of these metrics in ensuring the reliability, accuracy, and timeliness of detection systems.

- **Accuracy:** With an occurrence frequency of 37 times, accuracy is paramount in DDoS detection systems. High accuracy is essential to distinguish between legitimate and malicious traffic effectively, which is crucial in cloud environments with vast and diverse traffic.
- **Recall:** Appearing 26 times, recall is critical to minimizing false negatives. In cloud computing, failing to detect an actual attack can lead to significant resource strain and downtime.
- **F1-Score and Precision:** The importance of F1-Score (21 times) and Precision (18 times) indicates a need for a balanced detection system that minimizes both false positives and false negatives. This balance is crucial for maintaining service availability while ensuring accurate DDoS attack detection.
- **Sensitivity and FAR:** Sensitivity (9 times) and False Alarm Rate (FAR, 4 times) reflect the ongoing concern to accurately identify attacks while avoiding disruptions due to false alarms. False alarms in cloud computing can lead to unnecessary resource scaling and increased operational costs.

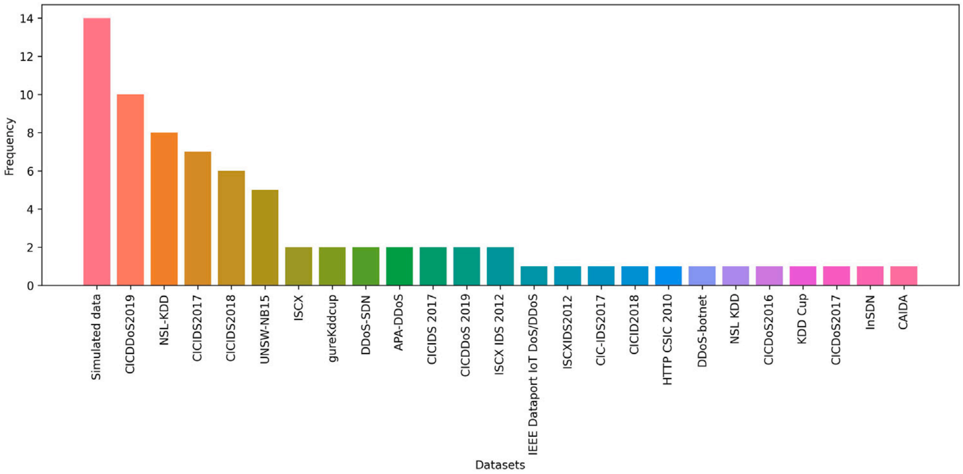

Fig. 14. Comparative analysis of dataset utilization.

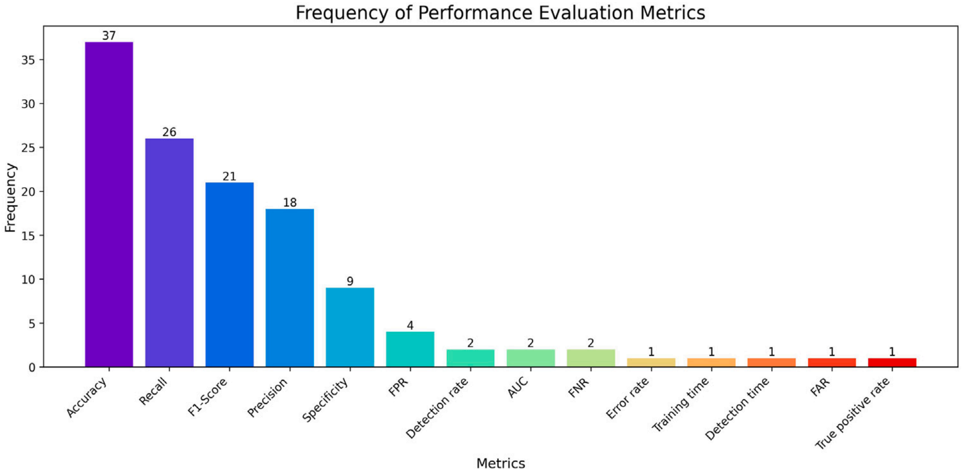

Fig. 15. Frequency of performance metrics in DDoS detection systems in the cloud using machine learning.

- **Other Metrics:** Metrics such as Detection time, FPR, FNR, TPR, AUC score, Detection rate, Training time, and Error rate, though less frequently mentioned, highlight specific areas of concern in DDoS detection, such as the need for quick mitigation and the minimization of detection errors.

The analysis underscores the nuanced priorities in developing DDoS detection systems for cloud environments. Accuracy, recall, precision, and F1-Score emerge as critical metrics. However, there is a potential area for future research in enhancing the speed of detection and mitigation to better protect cloud resources against DDoS attacks.

This section reviews studies on using machine learning for DDoS attack detection and mitigation in cloud networks. It finds that ML techniques like Naive Bayes, Random Forest, and Decision Trees are effective, with high accuracy rates. However, more research is needed using real-world data and developing comprehensive prevention and mitigation strategies. Future work should also explore ensemble and hybrid ML methods and cloud–edge collaboration.

7. Advancements and challenges in cloud-based DDoS attack defense (alternative approaches)

In this section, we will present an overview of several studies that investigate alternative approaches (excluding machine learning and deep learning) for identifying and addressing DDoS attacks in cloud network environments.

7.1. Investigating alternative approaches for DDoS attack detection, prevention and mitigation in cloud network environments, excluding machine learning and deep learning techniques

The study [123] introduces an interactive anomaly-based DDoS attack detection method in cloud computing, utilizing a Third-Party Auditor (TPA) to enhance security. It proposes a novel approach integrating TPA with cloud service providers' datacenters to detect and mitigate DDoS attacks through direct communication. This method employs a threshold anomaly-based detection strategy, leveraging simulations for validation. The study highlights the method's effectiveness in improving attack detection and reducing excessive filtering stages, categorizing its mitigation strategy mainly under 'Filtering.'. Optimizing the detection process and expanding the applicability of methods for cloud computing environments are indeed important areas for further research.

The study [124] develops a framework for Moving Target Defense (MTD) against DDoS attacks, offering a novel taxonomy to classify MTD techniques, such as shuffling, diversity, and redundancy, aimed at complicating attackers' efforts by dynamically altering system configurations. Utilizing simulations and theoretical analyses, it underscores the potential of MTD in enhancing defense mechanisms across various platforms, including IoT and cloud computing. Additional research should encompass the practical implementation and assessment of the suggested framework within real-world contexts.

The study [125] introduces a detection and mitigation method for DDoS attacks in Kubernetes environments, utilizing eBPF and XDP for efficient traffic monitoring and malicious packet filtering. This approach aims to secure Kubernetes clusters with minimal performance impact, classified under 'Filtering' techniques. The study, based on simulations, identifies the potential for eBPF and XDP to enhance cloud security. Limitations include the complexity of eBPF programs and the scalability of this solution as Kubernetes clusters grow. Future research could explore integrating eBPF with other Kubernetes security technologies for comprehensive protection.

The study [126] presents a DDoS attack defense strategy for cloud environments, focusing on resource isolation via separate physical machines (PMs) and virtual machines (VMs). This approach is compared to container and page level separations. The findings indicate that PM and VM isolation effectively maintain service access for legitimate users during DDoS attacks, significantly decreasing request failures and improving response times. The study uses simulations to support its findings, suggesting that resource separation can be crucial in DDoS defense, with PM level separation providing the greatest isolation, but requiring additional physical resources. Further study is needed to examine the scalability and real-world application of these separation techniques.

The study [127] introduces the ID3-MMDP method for detecting DDoS attacks in cloud computing, employing the Iterative Dichotomiser 3 (ID3) algorithm with a Maximum Multifactor Dimensionality Posteriori approach. Utilizing simulations, it showcases how this methodology distinguishes between attacker and legitimate user behavior, aiming to improve cloud security. The method is validated against existing techniques like eHIPF, Naive Bayes, and FLS, demonstrating superior performance in detection accuracy and response times. While the study presents a promising approach, further research is recommended to explore scalability and real-world application potential.

This study [128] presents a hybrid algorithm combining Multivariate Correlation Analysis, Spearman Coefficient, and mitigation techniques to detect and prevent DoS and DDoS attacks in cloud computing environments. It utilizes the KDD CUP 99 dataset for validation, demonstrating a detection accuracy of 99% against various DoS and DDoS attacks. The proposed system efficiently differentiates between normal and attack traffic, significantly enhancing network security. The study underscores the hybrid algorithm's superiority in accuracy compared to traditional methods and suggests its potential for broader application in cloud security. Further research could explore its adaptability to different settings.

The study [129] investigates ICMP-Flood DDoS attack mitigation in cloud and edge computing environments using simulated experiments. It focuses on applying Packet Filtering and Circuit-Level Gateway Firewalls for forensic and mitigation purposes. The research demonstrates significant traffic reduction and server resource usage decrease, with Packet Filtering Firewall showing a 64%–69% success rate in traffic reduction in cloud computing, and Circuit-Level Gateway Firewall achieving up to 98.88% traffic reduction in edge computing. A limitation highlighted is determining the optimal configuration for these firewalls to balance between security and network performance. Further research could explore adaptive firewall configurations to dynamically respond to attack patterns.

The study [130] presents the EDOS-TCP SYN mitigation model (EDOS-TSM) for countering TCP SYN flooding attacks in cloud computing using SDN technology. It employs binomial probability, TTL field value analysis, and multi-TCP SYN requests to distinguish between legitimate and spoofed IP traffic, aiming to reduce Economic Denial of Sustainability (EDoS) attacks. The model was validated on an OpenStack cloud with real-time traffic, demonstrating improved efficiency in mitigating both source-based and spoofing attacks compared to existing models. A limitation includes the challenge of determining optimal thresholds for attack detection. Further research could explore adaptive threshold settings and broader attack scenarios.

The study [131] introduces the Scattered Denial-of-Service Mitigation Tree Architecture (SDMTA) for DDoS mitigation in hybrid clouds, using network monitoring and an attacker database for high accuracy detection (99.7%). It employs a public dataset (KDD-999) for evaluation, highlighting the architecture's efficiency in quick DDoS detection and data shift issue management. The study focuses on filtering as the primary mitigation technique. It highlights the potential of this approach in real-time DDoS attack detection, suggesting further validation and exploration in diverse real-world scenarios.

The article [132] presents an original strategy to reduce the effects of DDoS attacks in cloud computing. This method combines the Dynamic Cloud Load Balancing (DCLB) algorithm with fuzzy logic for efficient resource allocation and DDoS attack identification. The algorithm does this by analyzing traffic patterns and adjusting resources accordingly. The research's findings, based on simulation, show a significant improvement in detection rates compared to existing models. The main DDoS mitigation technique used is a hybrid load balancing and traffic analysis. However, this approach has limitations, such as the inability to effectively detect low-rate DDoS attacks. Future research will focus on improving detection capabilities for such attacks and minimizing false positives.

The study [133] proposes a Three-Layer Filtering (3L-F) mechanism to prevent DDoS attacks in cloud environments. It introduces an innovative approach by segmenting the filtering process into three distinct layers: user authentication, request limit verification, and spoofed packet detection. The methodology involves practical tests in a simulated cloud environment, demonstrating improved performance metrics such as detection rate, CPU overhead, and throughput compared to existing models. A significant limitation noted is the model's evaluation under simulated conditions, suggesting the need for real-world testing to validate its effectiveness across diverse cloud settings. Future research directions include developing self-configuring systems for dynamic threat mitigation.

The study [134] presents an Artificial Immune System (AIS)-based method for DDoS attack mitigation in cloud environments, inspired by human immune responses. It focuses on identifying critical features of DDoS attacks using AIS for efficient detection. Public domain datasets, specifically the KDD Cup 99, were utilized for evaluation, showcasing the system's high detection accuracy and low false alarm rate. Emphasizing the need for additional validation in a wide range of settings is crucial to ensure the strength and efficacy of the approach in various scenarios.

The study [135] introduces a DDoS defense mechanism in SDN-cloud environments, leveraging entropy variations for attack detection and mitigation. Utilizing the POX controller and simulated network traffic, the approach demonstrated a high detection rate (98.2%) with a minimal false positive rate (0.04%). The study uniquely contributes by combining entropy-based detection with SDN's dynamic control capabilities. However, it is limited to simulations and a single controller setup, suggesting the need for real-world validations and exploring multi-controller configurations for future research.

The study [136] introduces a novel framework for detecting Economic Denial of Sustainability (EDoS) attacks in cloud environments, utilizing a Feature Classification (FC) algorithm to minimize false positives and negatives while conserving bandwidth and memory. It leverages machine learning for accurate EDoS detection, tested with metrics such as NSL-KDD, CAIDA, and CICDDoS2019, showing a significant accuracy improvement. Despite its effectiveness, the framework's limitation lies in handling simultaneous HTTP and Database attacks, it is highly recommended to validate the approach by utilizing real-world data.

The study [137] proposes an SDN-assisted defense mechanism against the Shrew DDoS attack in cloud environments, focusing on detection, mitigation, and source traceback. It employs information entropy variations for attack detection and deterministic packet marking for source identification, tested in real SDN-cloud scenarios. The methodology achieves 97.6% detection accuracy with minimal packets required to locate attackers. Despite its effectiveness, further validation in varied environments is recommended to ensure its adaptability and effectiveness against different DDoS strategies.

The study [138] presents a novel collaborative approach for detecting and mitigating DDoS attacks in Software-Defined Networks (SDNs) using sflow-RT application, Snort rules for traffic flow detection, and Redis Simple Message Queue (RSMQ) for rule sharing among Ryu SDN controllers. This technique effectively lowers controller overhead and ensures early detection and mitigation of DDoS attacks across multi-controller domains. The study, based on simulation data, highlights the potential of RSMQ for collaborative defense in SDN environments. Despite its effectiveness, further validation in varied environments is recommended to ensure its adaptability and effectiveness against different DDoS strategies.

The study [139] proposes a reputation score policy and Bayesian game theory-based mechanism for mitigating DDoS attacks. It introduces an incentivized approach, leveraging pricing rules and incentives to deter malicious activities within networks. The methodology combines Bayesian game theory for modeling uncertain interactions between users and a reputation assessment mechanism for evaluating user behavior. Utilizing simulations in MatLab, the study assesses the impact of this mechanism on social welfare and utility variations among users. While it offers a novel approach for DDoS mitigation, further exploration in real-world scenarios and against diverse attack vectors is recommended.

The study [140] introduces a novel method for detecting low-rate DDoS attacks using a multidimensional sketch structure and an improved behavior divergence measurement based on daub 4 wavelet transform. It incorporates a dynamic threshold mechanism to enhance detection accuracy. Real low-rate DDoS attack datasets (SUEE8 and MAWI_BOUN DDoS) were used for evaluation, demonstrating lower false positive and negative rates and higher accuracy compared to other methods. A noted limitation includes the challenge of determining the optimal threshold for attack detection. it is highly recommended to validate the approach by utilizing real-world data.

The study [141] introduces TSWA, a new method combining TSW and attack detection techniques to combat interest flooding attacks in cloud environments. Key achievements include the ability to identify attacks through analysis of data name prefix distribution, optimal detection window sizing, and attacker restriction via PIT routing. Tested in real and simulated settings, TSWA shows superior performance over existing methods in accuracy, precision, F-Score, GMean, specificity, and sensitivity, aiming to boost defense against interest flooding in NDN and future Internet architectures. However, the study lacks discussion on specific prevention or mitigation strategies.

The study [142] introduces a multi-level defense system against DDoS attacks in cloud environments, incorporating a novel filtering component (Filter Sniffer Analyzer, FSA), a game theory-based attack prevention algorithm, and a ϕ-entropy component for detection. It utilizes the CAIDA dataset for validation, achieving 97% detection accuracy, which surpasses existing systems. This system integrates detection, filtering, and prevention strategies effectively, showcasing significant improvements in handling both low-rate and high-rate DDoS attacks. As future work, exploring advanced machine learning and deep learning techniques to refine the system's accuracy and efficiency represents a significant opportunity.

The study [143] introduces a method for mitigating DDoS attacks in cloud environments by employing Cipher-text Policy Attribute-based Encryption (CP-ABE) and a novel encryption strategy. It relies on simulated attacks for evaluation, showing effectiveness in protecting against EDoS attacks. The strategy primarily focuses on redirection through dynamic encryption. Despite its success, the study highlights the trade-off between enhanced security and computational overhead. In order to strike a balance between security and performance, future efforts should prioritize the optimization of encryption techniques. The goal should be to enhance the efficiency of encryption algorithms without compromising the overall level of security.

The study [144] proposes a secure approach to address the challenge of DDoS attacks in cloud environments by utilizing a combination of encryption techniques, including CP-ABE. Key findings include a secure cloud storage mechanism and the use of dynamic identity-based encryption. Limitations include the need for further research on data privacy, transparency, and resource allocation in cloud environments. Future research should focus on enhancing encryption methods, improving DDoS attack detection, and securing cloud infrastructures.

The study [145] proposes an efficient framework using an Intrusion Detection System (IDS) to detect and prevent brute force and DDoS attacks in cloud networks. The study utilizes simulations to evaluate the effectiveness of the framework and discusses various prevention and mitigation strategies, including filtering, blocking, redirection, and other techniques. The key findings emphasize the importance of IDS in safeguarding cloud servers. The study's potential areas for further research include scalability and performance testing in larger cloud networks and exploring advanced intrusion detection techniques for enhanced cloud security.

The study [146] proposes CloudGuard, a system for DDoS detection in cloud-based web applications, using a tree-based model and simulations on Google Cloud Compute Engine to analyze traffic. It efficiently detects DDoS attacks through volume and web profile analysis, showcasing the system's accuracy and the model's quick detection. The study primarily uses simulated data. Further investigation could explore the adaptability of the proposed solutions across diverse network settings and against evolving DDoS attack strategies.

The study [147] proposes a two-line defense system against DDoS attacks, combining resource reservation, bandwidth limiting, and containerization. It separates requests based on connection count and uses bandwidth limiting and load balancing across containers. Using simulated data, the system maintains 98% service availability for benign requests during massive DDoS attacks, with near-normal response times. The approach primarily uses filtering and blocking strategies. Limitations include potential increased response times and difficulty handling low-rate DDoS attacks. Future work could focus on optimizing bandwidth use and adaptive thresholds for request separation.

Table 6 presents a comprehensive examination of diverse research concerning the detection, prevention, and mitigation of DDoS attacks through alternate methodologies. It highlights prevalent trends, strategies used, benefits, outcomes, and identifies areas lacking in current research.

Common Trends and Techniques A wide range of techniques have been explored in the literature, including anomaly-based detection, Moving Target Defense (MTD), resource isolation, hybrid algorithms, packet filtering, and encryption optimization. The majority of studies rely on simulated data for validation, which underscores the necessity for practical implementation and validation in real-world settings.

Advantages and Results The studies collectively highlight enhanced cloud network security and improved attack detection as key advantages. Moreover, efficiency in terms of reduced resource usage and increased processing speeds is also a significant outcome of these research efforts.

Identified Research Gaps

- **Real-World Application and Scalability** A significant gap identified across studies is the transition from theoretical models and simulated environments to real-world applications. The scalability and adaptability of proposed solutions in the face of evolving DDoS attack vectors also represent key areas for future research.
- **Detection of Low-Rate DDoS attacks** The challenge of detecting low-rate DDoS attacks, which can closely mimic normal traffic, is specifically highlighted as a niche for future exploration.
- **Optimization and efficiency** Despite high detection rates, the optimization of detection algorithms and mitigation techniques to balance security with performance remains a crucial area for improvement.

Table 6
Machine learning approaches to combatting DDoS attacks in cloud environments: techniques, effectiveness, and future prospects.

N	Ref	Year	Datasets	Techniques	Advantages	Results	Prev/Miti	Research gap
1	[123]	2023	Simulated data	Anomaly-based detection, TPA	Improved attack detection, reduced filtering	Accuracy: 96.35%	Yes	Optimization, applicability
2	[124]	2023	Simulated data	MTD (shuffling, diversity, redundancy)	Enhanced defense mechanisms	Potential in IoT and cloud computing	Yes	Practical implementation and assessment in real-world contexts
3	[125]	2023	Simulated data	eBPF, XDP	Demonstrated potential in cloud computing	Accuracy: 100%	Yes	Practical implementation and assessment in real-world contexts
4	[126]	2023	Simulated data	Resource isolation (PMs, VMs)	Decreased request failures, improved response times	Effective in DDoS defense	Yes	Scalability, real-world application
5	[127]	2023	Simulated data	ID3-MMDP	Superior detection accuracy and response times	Accuracy: 88%	No	Scalability, real-world application
6	[128]	2022	KDD CUP 99	Hybrid algorithm	Enhanced network security	99% detection accuracy	Yes	Scalability and adaptability to different settings
7	[129]	2022	Simulated data	Packet Filtering, Circuit-Level Gateway Firewalls	Significant traffic reduction	64%–98.88% traffic reduction	Yes	Optimal configuration
8	[130]	2022	Simulated data	EDOS-TCP SYN mitigation, SDN	Reduced EDoS attacks	Improved efficiency	Yes	Adaptive threshold settings
9	[131]	2022	KDD CUP 99	SDMTA	Quick DDoS detection	Accuracy: 99.7%, Sensitivity: 99.92%, Specificity: 98.32%	Yes	Validation in diverse scenarios
10	[132]	2022	Simulated data	DCLB algorithm, fuzzy logic	Improved detection rates	Detection rate: 93%	Yes	Detection of low-rate DDoS attacks
11	[133]	2021	Simulated data	Three-Layer Filtering	Improved performance metrics	Detection rate: 93%, FPR: 9%	Yes	Developing self-configuring systems for dynamic threat mitigation
12	[134]	2020	KDD Cup 99	Artificial Immune System (AIS)	High detection accuracy	Accuracy: 96.56%, Sensitivity: 91.9%, Specificity: 91.9% Precision: 95.6%	No	Additional validation
13	[135]	2021	Simulated data	Entropy variations, SDN	High detection rate	Detection rate: 93%, FPR: 0.04%	Yes	Multi-controller configurations
14	[136]	2021	NSL-KDD, CAIDA, CI-CDDoS2019	Feature Classification algorithm	Minimized false positives/negatives	Accuracy: 99.1%	No	Validation using real-world data
15	[137]	2020	Simulated data	Information entropy, deterministic packet marking	High detection accuracy	Accuracy: 97.6%	Yes	Validation in varied environments
16	[138]	2020	Simulated data	sflow-RT, Snort, RSMQ	Early detection and mitigation	High accuracy in mitigation	Yes	Validation in varied environments
17	[139]	2021	Simulated data	Reputation score policy, Bayesian game theory	Novel approach for DDoS mitigation	High accuracy in mitigation	Yes	Real-world scenarios, diverse attacks
18	[140]	2021	SUEE8, MAWI_BOUN DDoS	Multidimensional sketch, wavelet transform	Lower false positive/negative rates	Accuracy: 99.99%	No	Optimal threshold determination
19	[141]	2023	Simulated data	TSWA	Superior performance in accuracy, precision	Accuracy: 99.59%, Sensitivity: 99.55%, Specificity: 98.58% Precision: 98.55%	No	Validation in varied environments
20	[142]	2023	CAIDA	Multi-level defense system (FSA, game theory, ϕ-entropy)	Effective against low/high-rate attacks	Accuracy: 97%, Precision: 98.55%, Detection rate: 82%, FPR: 6%	Yes	Validation in varied environments
21	[143]	2023	Simulated data	encryption optimization	High detection accuracy	Accuracy: 98%, Sensitivity: 97%, Specificity: 98% Precision: 97%	Yes	Validation in varied environments

(continued on next page)

Table 6 (*continued*).

22	[144]	2023	Simulated data	Rivest-Shamir-Adleman (ERSA)	Better results	Encryption processing time: 250 ms, Decryption processing time: 150 ms	Yes	Scalability and adaptability to different settings
23	[145]	2023	Simulated data	IDS and IPS	High detection accuracy	High accuracy in mitigation	Yes	Scalability and adaptability to different settings
24	[146]	2023	Simulated data	Tree-based	High detection accuracy	Detection rate: 100%	No	Validation in varied environments
25	[147]	2024	Simulated data	Resource reservation, bandwidth limiting, containerization	Maintains service availability for benign requests	Service availability to ~98% of benign requests	Yes	Increased response times

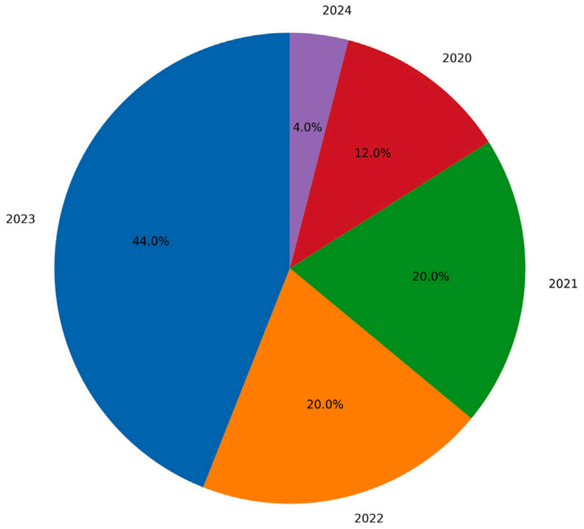

Fig. 16. The distribution of papers by years.

- **Validation in varied environments** The need for further validation of proposed methods in varied, real-world environments is a common conclusion, indicating a recognition of the gap between research and operational security solutions.

The landscape of DDoS defense research is marked by innovative approaches and promising results. However, the prevalent reliance on simulated data and calls for real-world application testing underline a critical gap in current research, steering future directions towards practical implementation, scalability, and comprehensive validation.

7.2. Insights from various studies on DDoS attack detection, prevention, and mitigation in the cloud (excluding ML and DL)

Fig. 16 depicts yearly scholarly paper distribution on DDoS defense strategies in cloud computing, showcasing research trends and cybersecurity advancements. The graph emphasizes recent studies, revealing intensified research activity in recent years. Notably, 2023 emerges as the peak publication year, underscoring a concentrated focus on cutting-edge DDoS defense methodologies and innovations within cloud infrastructures.

Fig. 17 displaying the distribution of datasets used in DDoS attack defense strategies research, particularly focusing on non-machine learning (ML) and non-deep learning (DL) methodologies, reveals a significant preference for simulated data. This preference underscores the importance of controlled experimental conditions in cybersecurity research, allowing for the detailed exploration of defense mechanisms against a variety of synthetic DDoS scenarios. The dominance of simulated data, indicated by 19 occurrences, highlights the research community's need to manipulate attack vectors and defense strategies in a controlled setting, ensuring experiments are repeatable and findings can be rigorously validated.

While public benchmark datasets like "KDD CUP 99", "NSL-KDD", "CAIDA", and "CICDDoS2019" are less frequently utilized, their inclusion reflects the ongoing value of real-world data for benchmarking purposes and the comparison of defense strategy effectiveness against documented attack patterns.

This distribution of dataset usage, especially excluding ML and DL approaches, suggests a robust interest in traditional cybersecurity techniques, such as anomaly detection and infrastructure resilience. It also hints at a potential research gap or opportunity in developing updated, cloud-specific datasets that more accurately mirror contemporary DDoS threats.

Fig. 18 reflecting the occurrences of performance metrics in DDoS attack defense strategies research, specifically within cloud environments and excluding machine learning (ML) and deep learning (DL) approaches, offers significant insights into the evaluation criteria valued by researchers in this domain. The predominant focus on "Accuracy" as a metric, highlighted by its 15 occurrences, underscores the paramount importance of precise detection capabilities in DDoS defense mechanisms. Accuracy ensures that the deployed defense strategies effectively identify and mitigate DDoS attacks without misidentifying legitimate traffic, a critical consideration for maintaining service availability and performance in cloud environments.

The notable attention to "Sensitivity", "Specificity", "Precision", and "Detection rate" metrics, each with multiple occurrences, indicates a comprehensive approach to evaluating defense strategies. Sensitivity and specificity are essential for understanding how well a defense mechanism can detect true positives and true negatives, respectively, reflecting its ability to distinguish between attack and non-attack traffic accurately. Precision focuses on the proportion of true positive detections over all positive detections, highlighting the system's reliability, while the detection rate provides a broader measure of the system's ability to identify attacks.

The inclusion of "FPR" (False Positive Rate), with three occurrences, and "Encryption/Decryption processing time", with one occurrence, further illustrates the nuanced considerations in DDoS defense. A low FPR is crucial for reducing unnecessary responses to false alarms, which can save resources and minimize disruptions to legitimate users. Meanwhile, the processing time for encryption and decryption tasks hints at the importance of efficiency in security measures, ensuring that protective actions do not introduce prohibitive delays in cloud service operations.

These findings, particularly in the context of non-ML/DL strategies, emphasize a multi-faceted evaluation framework that balances effectiveness, reliability, and operational efficiency in DDoS defense. The focus on traditional metrics over ML/DL-centric ones suggests that, despite the growing prominence of advanced learning techniques, there

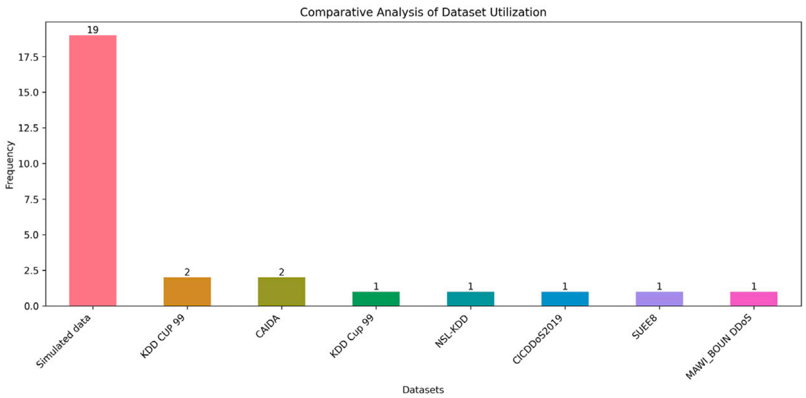

Fig. 17. Comparative analysis of dataset utilization.

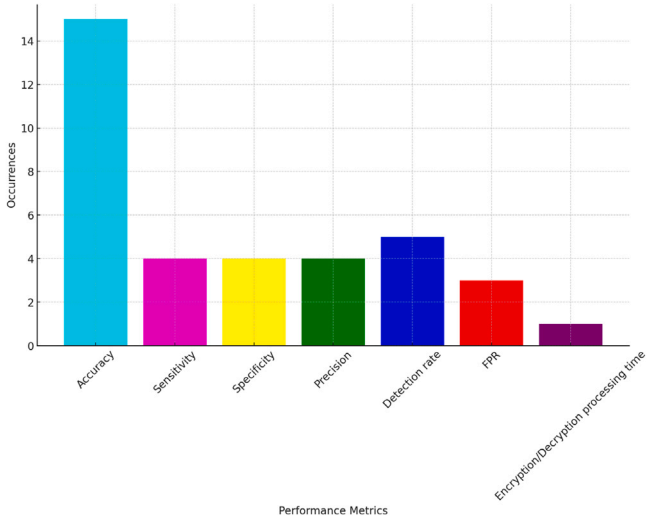

Fig. 18. Evaluating performance metrics in non- ML/DL ddos defense strategies for cloud environments.

remains a significant reliance on foundational principles of cybersecurity. This reliance originates from the immediate practicality, clarity, and potentially less complicated implementation of these traditional approaches in cloud contexts, where swift deployment and uncomplicated management are commonly valued.

This section discusses alternative strategies for identifying and mitigating DDoS attacks in cloud networks, focusing on methods excluding machine learning and deep learning. Approaches such as anomaly-based detection, Moving Target Defense (MTD), resource isolation, hybrid algorithms, packet filtering, and encryption optimization are examined, highlighting improved security and attack detection. Despite advancements in efficiency, reliance on simulated data emphasizes the need for real-world testing. Common challenges include detecting low-rate DDoS attacks and balancing security with performance. Future research should prioritize practical implementation, scalability, and validation in diverse environments to bridge the gap between theory and operational effectiveness in DDoS defense.

8. Research gaps and future work

This section addresses the challenges and future directions in the field of DDoS attack detection, prevention, and mitigation within cloud environments. It identifies key research gaps such as the need for real-world application scalability, detection of low-rate DDoS attacks, optimization of detection algorithms, and validation in diverse settings. The future work focuses on conducting real-world validations, exploring ensemble and hybrid approaches, leveraging cloud–edge collaboration, and developing comprehensive defense strategies. Addressing these areas is crucial for advancing the security and resilience of cloud systems against evolving DDoS threats.

Research Gaps: While previous studies have made significant progress in the field of DDoS attack detection,prevention and mitigation in the cloud, several research gaps have been identified, including:

1. **Real-World application and scalability:** The transition from theoretical models and simulated environments to real-world applications is a critical research gap. The scalability and adaptability of proposed solutions in the face of evolving DDoS attack vectors need further exploration.
2. **Detection of Low-Rate DDoS attacks:** Detecting low-rate DDoS attacks that closely mimic normal traffic poses a significant challenge. Developing effective detection techniques for these attacks is an important area for future exploration.
3. **Optimization and efficiency:** While many detection algorithms achieve high detection rates, there is a need for optimization to balance security with performance. Improving the efficiency of detection and mitigation techniques is crucial for practical deployment.
4. **Validation in varied environments:** Validating proposed methods in varied, real-world environments is essential to bridge the gap between research and operational security solutions. Further validation studies are needed to ensure the effectiveness and generalizability of DDoS defense strategies.

Future Work: To address these research gaps, future work in the field of DDoS attack prevention and mitigation should focus on the following areas:

1. **Real-World validation:** Conducting experiments and validations in real-world network environments is crucial to assess the practical applicability and effectiveness of DDoS defense strategies in the cloud. Utilizing diverse datasets and real-world attack scenarios will help validate the performance of detection and mitigation techniques.
2. **Ensemble and hybrid approaches:** Exploring ensemble and hybrid machine learning approaches that combine multiple detection techniques or integrate machine learning with other computational methods can lead to improved detection and mitigation results. These approaches can leverage the strengths of different techniques to enhance overall defense capabilities.
3. **Cloud-Edge Collaboration:** Leveraging the collaboration between cloud computing and edge computing resources can enable more efficient and less intrusive DDoS mitigation. Further exploration of cloud–edge collaboration can lead to innovative strategies for decentralized DDoS defense.

4. **Comprehensive prevention and mitigation strategies:** While detection has received significant attention, there is a need for comprehensive prevention and mitigation strategies. Developing solutions that encompass both detection and active defense mechanisms will contribute to a robust DDoS defense strategy in the cloud.

By addressing these research gaps and pursuing future work in these areas, we can advance the field of DDoS attack detection, prevention and mitigation in the cloud, improving the security and resilience of cloud systems.

9. Conclusion

This study underscores the critical importance of overcoming the limitations inherent in current methods and formulating more robust approaches for the detection, prevention, and mitigation of DDoS attacks within cloud environments. It sheds light on the notable absence of recent, in-depth reviews on the topic, revealing a substantial void in existing literature that this research seeks to bridge. By introducing a systematic review framework, this work aims to delineate a clear strategy for identifying, preventing, and mitigating the impact of DDoS threats, ultimately aiming to bolster cloud security and minimize the potential for service interruptions and data compromises. Focusing specifically on defense mechanisms tailored for cloud infrastructure, this research makes a significant contribution to the domain. Looking ahead, future research might examine the application of advanced machine learning techniques and the harmonization of the proposed frameworks with current security protocols to further reinforce the security of cloud platforms.

CRediT authorship contribution statement

Mohamed Ouhssini: Writing – original draft, Methodology, Conceptualization. **Karim Afdel:** Writing – review & editing, Supervision, Methodology. **Mohamed Akouhar:** Writing – review & editing. **Elhafed Agherrabi:** Writing – review & editing. **Abdallah Abarda:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work we used Chatgpt in order to improve the linguistic and writing capabilities when writing this paper. After using this service, we reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

[1] Abusaimeh H. Distributed denial of service attacks in cloud computing. Int J Adv Comput Sci Appl 2020;11. http://dx.doi.org/10.14569/ijacsa.2020.0110621.

[2] Aziz Israa T, Abdulqadder Ihsan H, Jawad Thakwan A. Distributed denial of service attacks on cloud computing environment. Cihan Univ Erbil Sci J 2022. http://dx.doi.org/10.24086/cuesj.v6n1y2022.pp47-52.

[3] Kushwah Gopal Singh, Ranga V. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. J Inf Secur Appl 2020;53:102532. http://dx.doi.org/10.1016/j.jisa.2020.102532.

[4] Pahal Sudesh, Saroha Anjana. Distributed denial of services attacks on cloud servers: Detection, analysis and mitigation. Mapana J Sci 2023. http://dx.doi.org/10.12723/mjs.64.7.

[5] Kushwah Gopal Singh, Ranga V. Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Comput Secur 2021;105:102260. http://dx.doi.org/10.1016/J.COSE.2021.102260.

[6] Singh Anshuman, Gupta Brij B. Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. Int J Semant Web Inf Syst 2022;18:1–43. http://dx.doi.org/10.4018/ijswis.297143.

[7] Wahab OA, Bentahar J, Otrok H, Mourad A. Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. IEEE Trans Serv Comput 2020;13:114–29. http://dx.doi.org/10.1109/TSC.2017.2694426.

[8] Gupta B, Dahiya Amrita, Upneja Chivesh, Garg Aditi, Choudhary Ruby. A comprehensive survey on DDoS attacks and recent defense mechanisms. 2020, p. 186–218. http://dx.doi.org/10.4018/978-1-7998-2242-4.ch010.

[9] Saharan Shail, Gupta Vishal. DDoS prevention: Review and issues. 2020, p. 579–86. http://dx.doi.org/10.1007/978-981-15-5243-4_53.

[10] Praseed Amit, Thilagam PS. DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. IEEE Commun Surv Tutor 2019;21:661–85. http://dx.doi.org/10.1109/COMST.2018.2870658.

[11] Somani Gaurav, Gaur Manoj Singh, Sanghi Dheeraj, Conti Mauro, Buyya Rajkumar. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Comput Commun 2017;107:30–48.

[12] Noureldien Noureldien Abdelrhman, Yousif Izzedin M. Accuracy of machine learning algorithms in detecting DoS attacks types. 2016, URL https://api.semanticscholar.org/CorpusID:63628223.

[13] Kabanda Richard, Byera Bertrand, Emeka Henrietta. The history, trend, types, and mitigation of distributed denial of service attacks. J Inf Secur 2023. URL https://api.semanticscholar.org/CorpusID:264531188.

[14] Help Net Security. DDoS attack power skyrockets to 1.6 tbps. 2024, URL https://www.helpnetsecurity.com/2024/02/02/ddos-attacks-h2-2023/.

[15] Predicting DDoS attacks in 2024: Navigating the cyberstorm. 2024, URL https://www.mlytics.com/blog/predicting-ddos-attacks-in-2024-navigating-the-cyberstorm/. [Accessed 28 February 2024].

[16] Smith Gary. DDoS statistics: How large a threat are DDoS attacks? 2024, URL https://www.stationx.net/ddos-statistics/. [Accessed 28 February 2024].

[17] Yoachimik Omer, Pacheco Jorge. DDoS threat report for 2023 Q4. 2024, URL https://blog.cloudflare.com/ddos-threat-report-2023-q4. [Accessed 9 March 2024].

[18] Comparitech. 20+ DDoS attack statistics and facts for 2018–2024. 2024, Comparitech Blog. URL https://www.comparitech.com/blog/information-security/ddos-statistics-facts/. [Accessed March 9 2024].

[19] Palatty Nivedita James. 45 Global DDOS attack statistics 2024. 2024, https://www.getastra.com/blog/security-audit/ddos-attack-statistics/. [Accessed 9 March 2024].

[20] Bhardwaj Akashdeep, Subrahmanyam GVB, Avasthi Vinay, Sastry Hanumat, Goundar Sam. DDoS attacks, new DDoS taxonomy and mitigation solutions—A survey. In: 2016 international conference on signal processing, communication, power and embedded system. SCOPES, IEEE; 2016, p. 793–8.

[21] Somani Gaurav, Gaur Manoj Singh, Sanghi Dheeraj, Conti Mauro, Buyya Rajkumar. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Comput Commun 2017;107:30–48.

[22] Goel Vikas, Goel Pragati, Ranjan Raju, Sharma Amit Kumar. An effective classification of DDoS cloud based attack through tree founded classifiers. In: 2023 1st international conference on innovations in high speed communication and signal processing. IHCSP, IEEE; 2023, p. 446–9.

[23] Somani G, Gaur M, Sanghi D, Conti M, Buyya R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. 2015, http://dx.doi.org/10.1016/j.comcom.2017.03.010, arXiv abs/1512.08187.

[24] Solutions for DDoS attacks on cloud environment. Bentham Science Publishers eBooks; 2023, p. 42–55. http://dx.doi.org/10.2174/9789815136111123010006.

[25] Investigating the impact of DDoS attacks on DNS infrastructure. 2022.

[26] Impacts of DDoS attacks in software-defined networks. Smart Innov Syst Technol 2022;123–32. http://dx.doi.org/10.1007/978-981-19-3571-8_14.

[27] Russo Andrea. Organised firestorm as strategy for business cyber-attacks. 2023, arXiv preprint arXiv:2301.01518.

[28] Perera Srinath, Jin Xiaohua, Maurushat Alana, Opoku De-Graft Joe. Factors affecting reputational damage to organisations due to cyberattacks. In: Informatics. Vol. 9, MDPI; 2022, p. 28.

[29] Bargavi Manju, Senbagavalli M, KR Tejashwini, KR Tejashvar. Data breach–Its effects on industry. Int J Data Inform Intell Comput 2022;1(2):51–7.

[30] Page Matthew J, McKenzie Joanne E, Bossuyt Patrick M, Boutron Isabelle, Hoffmann Tammy C, Mulrow Cynthia D, Shamseer Larissa, Tetzlaff Jennifer M, Akl Elie A, Brennan Sue E, Chou Roger, Glanville Julie, Grimshaw Jeremy M, Hróbjartsson Asbjørn, Lalu Manoj M, Li Tianjing, Loder Elizabeth W, Mayo-Wilson Evan, McDonald Steve, McGuinness Luke A, Stewart Lesley A, Thomas James, Tricco Andrea C, Welch Vivian A, Whiting Penny, Moher David. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372. http://dx.doi.org/10.1136/bmj.n71, arXiv:https://www.bmj.com/content/372/bmj.n71.full.pdf. URL https://www.bmj.com/content/372/bmj.n71.

[31] Pandithurai O, Venkataiah C, Tiwari Shrikant, Ramanjaneyulu N. DDoS attack prediction using a honey badger optimization algorithm based feature selection and Bi-LSTM in cloud environment. Expert Syst Appl 2024;241:122544. http://dx.doi.org/10.1016/j.eswa.2023.122544.

[32] Snehi Manish, Bhandari Abhinav, Verma Jyoti. Foggier skies clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems. Comput Secur 2024;139:103702. http://dx.doi.org/10.1016/j.cose.2024.103702.

[33] Ouhssini Mohamed, Afdel Karim, Agherrabi Elhafed, Akouhar Mohamed, Abarda Abdallah. DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing. J King Saud Univ Comput Inf Sci 2024;36:101938. http://dx.doi.org/10.1016/j.jksuci.2024.101938.

[34] Aydın Hakan, Orman Zeynep, Aydın Muhammed Ali. A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. Comput Secur 2022;118:102725. http://dx.doi.org/10.1016/j.cose.2022.102725.

[35] Arango-Lopez Jeferson, Isaza Gustavo, Duque Nestor, Montes Jose, Ramirez Fabian. Cloud-based deep learning architecture for DDoS cyber attack prediction. Expert Syst 2024;e13552. http://dx.doi.org/10.1111/exsy.13552.

[36] Sureshkumar S, Venkatesan GKD Prasanna, Santhosh R. Detection of DDOS attacks on cloud computing environment using altered convolutional deep belief networks. Int J Comput Netw Inf Secur 2023;15(5):63–72. http://dx.doi.org/10.5815/ijcnis.2023.05.06.

[37] Amitha Marram, Srivenkatesh Muktevi. DDoS attack detection in cloud computing using deep learning algorithms. Int J Intell Syst Appl Eng 2023;11(4):82–90.

[38] Pasha MJahir, Rao KPrasada, MallaReddy A, Bande Vasavi. LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments. Measurement 2023;28:100828. http://dx.doi.org/10.1016/j.measen.2023.100828.

[39] Mansoor Amran, Anbar Mohammed, Bahashwan Abdullah Ahmed, Al-absi Basim Ahmad, Rihan Shaza Dawood Ahmed. Deep learning-based approach for detecting DDoS attack on software-defined networking controller. Systems 2023;11:296. http://dx.doi.org/10.3390/systems11060296.

[40] G.S.R. Emil Selvan, Ganeshan R, Jingle IDiana Jeba, Ananth JP. FACVO-DNFN: Deep learning-based feature fusion and distributed denial of service attack detection in cloud computing. Knowl-Based Syst 2023;261:110132. http://dx.doi.org/10.1016/j.knosys.2022.110132.

[41] Hnamte Vanlalruata, Najar Ashfaq Ahmad, Nhung-Nguyen Hong, Hussain Jamal, Sugali Manohar Naik. DDoS attack detection and mitigation using deep neural network in SDN environment. Comput Secur 2024;138:103661. http://dx.doi.org/10.1016/j.cose.2023.103661.

[42] Benzaïd Chafika, Taleb Tarik, Sami Ashkan, Hireche Othmane. FortisEDoS: A deep transfer learning-empowered economical denial of sustainability detection framework for cloud-native network slicing. IEEE Trans Dependable Secure Comput 2023. http://dx.doi.org/10.1109/TDSC.2023.3318606.

[43] Sureshkumar S, Venkatesan GKD Prasanna, Santhosh R. Adaptive butterfly optimization algorithm (ABOA) based feature selection and deep neural network (DNN) for detection of distributed denial-of-service (DDoS) attacks in cloud. Comput Syst Sci Eng 2023;47(1):1110–22. http://dx.doi.org/10.32604/csse.2023.036267.

[44] Kumar GS, Fred AL, Manic S, Sahoo RJK, Khan MTZ, Gupta B. Hybrid deep learning system for DDoS attack detection in cloud computing environments. J Cloud Comput Adv Syst Appl 2023;2023:23–37. http://dx.doi.org/10.1186/s13677-023-00295-1.

[45] Sanjalawe Yousef, Althobaiti Turke. DDoS attack detection in cloud computing based on ensemble feature selection and deep learning. CMC Comput Mater Contin 2023;75(2):3572–88. http://dx.doi.org/10.32604/cmc.2023.037386, URL https://www.techscience.com/cmc/v75n2/48478.

[46] Thangasamy Anitha, Sundan Bose, Govindaraj Logeswari. A novel framework for DDoS attacks detection using hybrid LSTM techniques. Comput Syst Sci Eng 2023;45(3):2554–67. http://dx.doi.org/10.32604/csse.2023.032078.

[47] Vu Ly, Nguyen Quang Uy, Nguyen Diep N, Hoang Dinh Thai, Dutkiewicz Eryk. Deep generative learning models for cloud intrusion detection systems. IEEE Trans Cybern 2023;53(1):565–76. http://dx.doi.org/10.1109/TCYB.2022.3163811.

[48] Agarwal Ankit, Khari Manju, Singh Rajiv. Detection of DDOS attack using deep learning model in cloud storage application. Wirel Pers Commun 2021. http://dx.doi.org/10.1007/s11277-021-08271-z.

[49] Maheswari KG, Siva C, Nalinipriya G. Optimal cluster-based feature selection for intrusion detection system in web and cloud computing environment using hybrid teacher learning optimization enables deep recurrent neural network. Comput Commun 2023;202:145–53. http://dx.doi.org/10.1016/j.comcom.2023.02.003.

[50] Najar Ashfaq Ahmad, Naik S Manohar. Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks. Comput Secur 2024;139:103716. http://dx.doi.org/10.1016/j.cose.2024.103716.

[51] Almiani Muder, Abughazleh Alia, Jararweh Yaser, Razaque Abdul. Resilient back propagation neural network security model for containerized cloud computing. Simul Model Pract Theory 2022;118:102544. http://dx.doi.org/10.1016/j.simpat.2022.102544.

[52] Balasubramaniam S, Vijesh Joe C, Sivakumar TA, Prasanth A, Satheesh Kumar K, Kavitha V, Dhanaraj Rajesh Kumar. Security framework against DDoS attacks in cloud computing using optimized deep belief networks. Int J Intell Syst 2023;2023:1–16. http://dx.doi.org/10.1155/2023/2039217.

[53] Dennis J Britto, Priya M Shanmuga. Deep belief network and support vector machine fusion for distributed denial of service and economical denial of service attack detection in cloud. Concurr Comput: Pract Exper 2022;34(1):e6543. http://dx.doi.org/10.1002/cpe.6543.

[54] Sumathi S, Rajesh R, Lim Sangsoon. Recurrent and deep learning neural network models for DDoS attack detection. J Sens 2022;2022:21. http://dx.doi.org/10.1155/2022/8530312.

[55] Bhutto Adil Bin, Vu Xuan Son, Tay Wee Peng, Elmroth Erik, Bhuyan Monowar. Reinforced transformer learning for VSI-DDoS detection in edge clouds. IEEE Trans Dependable Secure Comput 2022;19(1):1–16. http://dx.doi.org/10.1109/TDSC.2022.3204812.

[56] Samsu Ahamed Ali, Agoramoorthy Aliar Moorthy, Justindhas Y. An automated detection of DDoS attack in cloud using optimized weighted fused features and hybrid DBN-GRU architecture. Cybern Syst 2023. http://dx.doi.org/10.1080/01969722.2022.2157603.

[57] Akgun Devrim, Hizal Selman, Cavusoglu Unal. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Comput Secur 2022;118:102748. http://dx.doi.org/10.1016/j.cose.2022.102748.

[58] Virupakshar Karan B, Patil Manjunath Asundi, Channal Kishor G, Shettar Pooja, G. Narayan D, Somashekar. Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Comput Sci 2020;167:2297–307. http://dx.doi.org/10.1016/j.procs.2020.03.282.

[59] Novaes Matheus P, Carvalho Luiz F, Lloret Jaime, Proença Jr Mario Lemes. Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments. Future Gener Comput Syst 2021;125:156–67. http://dx.doi.org/10.1016/j.future.2021.06.047.

[60] Paidipati Kiran Kumar, Kurangi Chinnarao, Uthayakumar J, Padmanayaki S, Pradeepa D, Nithinsha S. Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud-based software-defined networks. Multimedia Tools Appl 2023.

[61] Janakiraman Sengathir, Priya M Deva. A deep reinforcement learning-based DDoS attack mitigation scheme for securing big data in fog-assisted cloud environment. Wirel Pers Commun 2023;130:2869–86. http://dx.doi.org/10.1007/s11277-023-10407-2.

[62] Balasubramaniam S, Vijesh Joe C, Sivakumar TA, Prasanth A, Satheesh Kumar K, Kavitha V, Dhanaraj Rajesh Kumar. Optimization enabled deep learning-based DDoS attack detection in cloud computing. Int J Intell Syst 2023;2023:2039217. http://dx.doi.org/10.1155/2023/2039217.

[63] Huang Haiou, Sun Bangyi, Hu Liang. A task offloading approach based on risk assessment to mitigate edge DDoS attacks. Comput Secur 2024. http://dx.doi.org/10.1016/j.cose.2024.103789.

[64] Zhao Ziming, Li Zhaoxuan, Zhou Zhihao, Yu Jiongchi, Song Zhuoxue, Xie Xiaofei, Zhang Fan, Zhang Rui. DDoS family: A novel perspective for massive types of DDoS attacks. Comput Secur 2024;138:103663.

[65] Manjunath C R, Rathor Ketan, Kulkarni Nandini, Patil Prashant Pandurang, Patil Manoj S, Singh Jasdeep. Cloud based DDOS attack detection using machine learning architectures: Understanding the potential for scientific applications. Int J Intell Syst Appl Eng 2022;10(2s):268–71.

[66] Jeba Praba J, Sridaran R. LCDT-M: Log-cluster DDoS tree mitigation framework using SDN in the cloud environment. I J Comput Netw Inf Secur 2023;2(2):62–72. http://dx.doi.org/10.5815/ijcnis.2023.02.05.

[67] Nagaraju Vankayalapati, Raaza Arun, Rajendran V, Ravikumar D. Deep learning binary fruit fly algorithm for identifying SYN flood attack from TCP/IP. Mater Today Proc 2023;80:3086–91. http://dx.doi.org/10.1016/j.matpr.2021.07.171.

[68] Yin Xiaochun, Fang Wei, Liu Zengguang, Liu Deyong. A novel multi-scale CNN and bi-LSTM arbitration dense network model for low-rate DDoS attack detection. Sci Rep 2024;14(1):5111. http://dx.doi.org/10.1038/s41598-024-55814-y.

[69] Songa Asha Varma, Karri Ganesh Redy. Ensemble-RNN: A robust framework for DDoS detection in cloud environment. Majlesi J Electr Eng 2023;17(4):31–44. http://dx.doi.org/10.30486/mjee.2023.1986487.1137.

[70] Shanmuganathan S, Gayathri C, Charumathi R, Ragupathi T, Vijayakumari V, Madhan K. Detection of DDOS attacks in cloud environment using deep learning. J Cloud Comput 2022.

[71] Bhardwaj Aanshi, Mangat Veenu, Vig Renu. Hyperband tuned deep neural network with well posed stacked sparse AutoEncoder for detection of DDoS attacks in cloud. IEEE Access 2020;8:181916–27. http://dx.doi.org/10.1109/ACCESS.2020.3028690.

[72] Zhao Junjie, Liu Yongmin, Zhang Qianlei, Zheng Xinying. CNN-AttBiLSTM mechanism: A DDoS attack detection method based on attention mechanism and CNN-BiLSTM. IEEE Access 2023;11:136308–16. http://dx.doi.org/10.1109/ACCESS.2023.3334916.

[73] Vibhute Amol D, Nakum Vikram. Deep learning-based network anomaly detection and classification in an imbalanced cloud environment. In: Proceedings of the 5th international conference on industry 4.0 and smart manufacturing. Elsevier B.V.; 2024, p. 1636–45. http://dx.doi.org/10.1016/j.procs.2024.01.161, URL https://www.sciencedirect.com/science/article/pii/S1877050924000433.

[74] Public cloud networks oriented deep neural networks for effective intrusion detection in online music education. Comput Electr Eng 2024;115:109095. http://dx.doi.org/10.1016/j.compeleceng.2024.109095.

[75] Mhamdi Lotfi, Isa Mohd Mat. Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation. J Netw Comput Appl 2024;225:103868.

[76] Babbar Himanshi, Rani Shalli, Boulila Wadii. NGMD: Next generation malware detection in federated server with deep neural network model for autonomous networks. Sci Rep 2024;14(10898). http://dx.doi.org/10.1038/s41598-024-61298-7.

[77] Yin Xiaochun, Fang Wei, Liu Zengguang, Liu Deyong. A novel multi-scale CNN and bi-LSTM arbitration dense network model for low-rate DDoS attack detection. Sci Rep 2024;14(1):5111.

[78] Aljuaid WH, Alshamrani SS. A deep learning approach for intrusion detection systems in cloud computing environments. Appl Sci 2024;14(13):5381. http://dx.doi.org/10.3390/app14135381.

[79] Bai V Sujatha, Punithavalli M. Leveraging feature subset selection with deer hunting optimizer based deep learning for anomaly detection in secure cloud environment. Multimedia Tools Appl 2024;1–22.

[80] Reddy K Balachandra, Meera S. DDoS attack detection in cloud using ensemble model tuned with optimal hyperparameter. Internat J Adapt Control Signal Process 2024;38:1594–620. http://dx.doi.org/10.1002/acs.3766.

[81] Shang Yongqiang. Prevention and detection of DDOS attack in virtual cloud computing environment using Naive Bayes algorithm of machine learning. Measurement 2024;31:100991. http://dx.doi.org/10.1016/j.measen.2023.100991.

[82] Setia Himanshu, Chhabra Amit, Singh Sunil K, Kumar Sudhakar, Sharma Sarita, Arya Varsha, Gupta Brij B, Wu Jinsong. Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Secur Appl 2024;2:100037. http://dx.doi.org/10.1016/j.csa.2024.100037.

[83] Sambangi Swathi, Gondi Lakshmeeswari, Aljawarneh Shadi. A feature similarity machine learning model for DDoS attack detection in modern network environments for industry 4.0. Comput Electr Eng 2022;100:107955.

[84] Kushwah Gopal Singh, Ranga Virender. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. J Inf Secur Appl 2020;53:102532. http://dx.doi.org/10.1016/j.jisa.2020.102532.

[85] Jeba Praba J, Sridaran R. LCDT-M: Log-cluster DDoS tree mitigation framework using SDN in the cloud environment. I J Comput Netw Inf Secur 2023;2:62–72. http://dx.doi.org/10.5815/ijcnis.2023.02.05, URL http://www.mecs-press.org/. Published Online on April 8, 2023.

[86] Pattnaik Lal Mohan, Swain Pratik Kumar, Satpathy Suneeta, Panda Aditya N. Cloud DDoS attack detection model with data fusion and machine learning classifiers. EAI Endorsed Trans Scalable Inf Syst 2023;10(6):1–18. http://dx.doi.org/10.4108/eetsis.3936.

[87] Amitha Marram, Srivenkatesh DrMuktevi. Design of a hypermodel using transfer learning to detect DDoS attacks in the cloud security. Int J Adv Comput Sci Appl (IJACSA) 2023;14(9):538.

[88] Ramesh G, Gorantla Venkata Ashok K, Gude Venkataramaiah. A hybrid methodology with learning based approach for protecting systems from DDoS attacks. J Discrete Math Sci Cryptogr 2023;26(5):1317–25. http://dx.doi.org/10.47974/JDMSC-1747.

[89] Arunadevi M, Sathya V. DDoS attack detection using back propagation neural network optimized by bacterial colony optimization. Int J Intell Eng Syst 2023;16(5):301–2. http://dx.doi.org/10.22266/ijies2023.1031.26.

[90] Naiem Sarah, Idrees Amira M, Khedr Ayman E, Marie Mohamed. Iterative feature selection-based DDoS attack prevention approach in cloud. Int J Adv Comput Sci Appl 2023;14(2):197. http://dx.doi.org/10.14569/IJACSA.2023.014021.

[91] Alam Gowthul MM, Kumar Jerald Nirmal S, Mageswari Uma R, Raj Michael TF. An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment. Comput Netw 2022;215:109138. http://dx.doi.org/10.1016/j.comnet.2022.109138.

[92] Abdullayeva Fargana J. Distributed denial of service attack detection in E-government cloud via data clustering. Array 2022;15:100229. http://dx.doi.org/10.1016/j.array.2022.100229.

[93] Sokkalingam Sumathi, Ramakrishnan Rajesh. An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach. Concurr Comput: Pract Exper 2022;34(27):e7334. http://dx.doi.org/10.1002/cpe.7334.

[94] Hossain Md Alamgir, Islam Md Saiful. Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. Measurement 2024;32:101037. http://dx.doi.org/10.1016/j.measen.2024.101037.

[95] Reddy SaiSindhuTheja, Shyam Gopal K. A machine learning based attack detection and mitigation using a secure saas framework. J King Saud Univ Comput Inf Sci 2022;34(2022):4047–61. http://dx.doi.org/10.1016/j.jksuci.2020.10.005.

[96] Kanber Bassam M, Noaman Naglaa F, Saeed Amr MH, Malas Mansoor. DDoS attacks detection in the application layer using three level machine learning classification architecture. I J Comput Netw Inf Secur 2022;3(3):33–46. http://dx.doi.org/10.5815/ijcnis.2022.03.03.

[97] Alduailij Mona, Khan Qazi Waqas, Tahir Muhammad, Sardaraz Muhammad, Alduailij Mai, Malik Fazila. Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. Symmetry 2022;14(6):1095. http://dx.doi.org/10.3390/sym14061095.

[98] Alqarni Ahmed Abdullah. Majority vote-based ensemble approach for distributed denial of service attack detection in cloud computing. J Cyber Secur Mobil 2022;11(2):265–78. http://dx.doi.org/10.13052/jcsm2245-1439.1126.

[99] Praba Jeba, Sridaran R. An SDN-based decision tree detection (DTD) model for detecting DDoS attacks in cloud environment. Int J Adv Comput Sci Appl (IJACSA) 2022;13(7):54–68.

[100] Mishra Narendra, Singh RK, Yadav SK. Detection of DDoS vulnerability in cloud computing using the perplexed Bayes classifier. Comput Intell Neurosci 2022;2022:9151847. http://dx.doi.org/10.1155/2022/9151847.

[101] Shang Yongqiang. Prevention and detection of DDOS attack in virtual cloud computing environment using Naive Bayes algorithm of machine learning. Measurement 2024;31:100991. http://dx.doi.org/10.1016/j.measen.2023.100991.

[102] Kohnehshahri Mitra Akbari, Nassiri Mohammad, Mohammadi Reza, Abdoli Hatam. An efficient method for online detection of drdos attacks on UDP-based services in SDN using machine learning algorithms. Mob Inf Syst 2022;2022:1169035. http://dx.doi.org/10.1155/2022/1169035.

[103] Wang Meng, Lu Yiqin, Qin Jiancheng. Source-based defense against DDoS attacks in SDN based on sflow and SOM. IEEE Access 2022;10:2097–110. http://dx.doi.org/10.1109/ACCESS.2021.3139511.

[104] Harikrishna Pillutla, Amuthan A. Rival-model penalized self-organizing map enforced DDoS attack prevention mechanism for software defined network-based cloud computing environment. J Parallel Distrib Comput 2021;154:142–52. http://dx.doi.org/10.1016/j.jpdc.2021.03.005.

[105] Kushwah Gopal Singh, Ranga Virender. Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Comput Secur 2021;105:102260. http://dx.doi.org/10.1016/j.cose.2021.102260.

[106] Kushwah Gopal Singh, Ranga Virender. Distributed denial of service attack detection in cloud computing using hybrid extreme learning machine. Turk J Electr Eng Comput Sci 2021;29(4):1852–70. http://dx.doi.org/10.3906/elk-1908-87.

[107] Anonymous. Retraction: Ddos detection using a cloud-edge collaboration method based on entropy-measuring SOM and KD-tree in SDN. Secur Commun Netw 2023;2023:9856153. http://dx.doi.org/10.1155/2023/9856153.

[108] Saeed Aween Abubakr, Jameel Noor Ghazi Mohammed. Intelligent feature selection using particle swarm optimization algorithm with a decision tree for DDoS attack detection. Int J Adv Intell Inform 2021;7(1):37–48. http://dx.doi.org/10.26555/ijain.v7i1.553.

[109] Verma Priyanka, Krishna Kowsik A Rama, Pateriya RK, Bharot Nitesh, Vidyarthi Ankit, Gupta Deepak. A stacked ensemble approach to generalize the classifier prediction for the detection of DDoS attack in cloud network. Mob Netw Appl 2023. http://dx.doi.org/10.1007/s11036-023-02225-4.

[110] Das Saikat, Ashrafuzzaman Mohammad, Sheldon Frederick T, Shiva Sajjan. Ensembling supervised and unsupervised machine learning algorithms for detecting distributed denial of service attacks. Algorithms 2024;17(99):1–21. http://dx.doi.org/10.3390/a17030099.

[111] Zeinalpour Alireza, McElroy Charles P. Comparing metaheuristic search techniques in addressing the effectiveness of clustering-based DDoS attack detection methods. Electronics 2024;13:899. http://dx.doi.org/10.3390/electronics13050899.

[112] Xu Jing, Li Xue, Wang Puming, Jin Xin, Yao Shaowen. Multi-modal noise-robust DDoS attack detection architecture in large-scale networks based on tensor SVD. IEEE Trans Netw Sci Eng 2023;10(1):152–3. http://dx.doi.org/10.1109/TNSE.2022.3205708.

[113] Costa Wanderson L, Portela Ariel LC, Gomes Rafael L. Features-aware DDoS detection in heterogeneous smart environments based on fog and cloud computing. Int J Commun Netw Inf Secur (IJCNIS) 2021;13(3):491–2.

[114] Corrêa João Henrique, Villaça Rodolfo S, Ciarelli Patrick M, Ribeiro Moises RN. ML-based DDoS detection and identification using native cloud telemetry macroscopic monitoring. J Netw Syst Manage 2021;29(13):1–28. http://dx.doi.org/10.1007/s10922-020-09578-1.

[115] Gumaste Shweta, Narayan DG, Shinde Sumedha, Amit K. Detection of DDoS attacks in OpenStack-based private cloud using apache spark. J Inf Technol Innov 2020. http://dx.doi.org/10.26636/jtit.2020.146120.

[116] Varghese Meble, Jose M Victor. An optimized radial bias function neural network for intrusion detection of distributed denial of service attack in the cloud. Concurr Comput: Pract Exper 2022;34(27):e7321. http://dx.doi.org/10.1002/cpe.7321.

[117] Aslam Naziya, Srivastava Shashank, Gore MM. ONOS DDoS defender: A comparative analysis of existing DDoS attack datasets using ensemble approach. Wirel Pers Commun 2024. http://dx.doi.org/10.1007/s11277-023-10848-9.

[118] Nalayini CM, Katiravan Jeevaa, Geetha S, Christy Eunaicy JI. A novel dual optimized IDS to detect DDoS attack in SDN using hyper tuned RFE and deep grid network. Cyber Secur Appl 2024;2:100042. http://dx.doi.org/10.1016/j.csa.2024.100042.

[119] Naiem Sarah, Khedr Ayman E, Idrees Amira M, Marie Mohamed I. Enhancing the efficiency of Gaussian Naïve Bayes machine learning classifier in the detection of DDOS in cloud computing. IEEE Access 2023;11:124597. http://dx.doi.org/10.1109/ACCESS.2023.3328951.

[120] Erhan Derya, Anarim Emin. Hybrid DDoS detection framework using matching pursuit algorithm. IEEE Access 2020;8:118912–22. http://dx.doi.org/10.1109/ACCESS.2020.3005781.

[121] Songa Asha Varma, Karri Ganesh Reddy. An integrated SDN framework for early detection of DDoS attacks in cloud computing. J Cloud Comput 2024;13(64):1–22.

[122] Rizvi Fizza, Sharma Ravi, Sharma Nonita, Rakhra Manik, Aledaily Arwa N, Viriyasitavat Wattana, Yadav Kusum, Dhiman Gaurav, Kaur Amandeep. An evolutionary KNN model for DDoS assault detection using genetic algorithm based optimization. Multimedia Tools Appl 2024. http://dx.doi.org/10.1007/s11042-024-18744-5.

[123] Hezavehi Sasha Mahdavi, Rahmani Rouhollah. Interactive anomaly-based DDoS attack detection method in cloud computing environments using a third party auditor. J Parallel Distrib Comput 2023;178:82–99.

[124] Amro Belal M, Salah Saeed, Moreb Mohammed. A comprehensive architectural framework of moving target defenses against DDoS attacks. J Cyber Secur Mobil 2023;12(4):605–28. http://dx.doi.org/10.13052/jcsm2245-1439.1248.

[125] Sadiq Amin, Syed Hassan Jamil, Ansari Asad Ahmed, Ibrahim Ashraf Osman, Alohaly Manar, Elsadig Muna. Detection of denial of service attack in cloud based kubernetes using eBPF. Appl Sci 2023;13(8):4700. http://dx.doi.org/10.3390/app13084700.

[126] Kumar Anmol, Somani Gaurav. Service separation assisted DDoS attack mitigation in cloud targets. J Inf Secur Appl 2023;73:103435. http://dx.doi.org/10.1016/j.jisa.2023.103435.

[127] Kumar Anmol, Somani Gaurav. Service separation assisted DDoS attack mitigation in cloud targets. J Inf Secur Appl 2023;73:103435. http://dx.doi.org/10.1016/j.jisa.2023.103435.

[128] Kumar Anmol, Somani Gaurav. Service separation assisted DDoS attack mitigation in cloud targets. J Inf Secur Appl 2023;73:103435. http://dx.doi.org/10.1016/j.jisa.2023.103435.

[129] Yudhana Anton, Riadi Imam, Suharti Sri. Network forensics against volumetric-based distributed denial of service attacks on cloud and the edge computing. Int J Safety Secur Eng 2022;12(5):577–88. http://dx.doi.org/10.18280/ijsse.120505.

[130] Shah Sayed Qaiser Ali, Khan Farrukh Zeeshan, Ahmad Muneer. Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN. Comput Commun 2022;182:198–211. http://dx.doi.org/10.1016/j.comcom.2021.11.008.

[131] Kautish Sandeep, A. Reyana, Vidyarthi Ankit. SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment. IEEE Trans Ind Inf 2022;18(9):6455–7. http://dx.doi.org/10.1109/TII.2022.3146290.

[132] Nair Amrutha Muralidharan, Santhosh R. Mitigation of DDoS attack in cloud computing domain by integrating the DCLB algorithm with fuzzy logic. Int J Adv Comput Sci Appl (IJACSA) 2022;13(10).

[133] Somasundaram A, Meenakshi VS. A novel three layer filtering (3L-F) framework for prevention of DDoS attack in cloud environment. Int J Comput Netw Appl (IJCNA) 2021;8(4):334. http://dx.doi.org/10.22247/ijcna/2021/209700.

[134] Prathyusha Damai Jessica, Kannayaram Govinda. A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment. Evol Intell 2019;1(3):1–13.

[135] Mishra Anupama, Gupta Neena, Gupta BB. Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommun Syst 2021;77(1):47–62. http://dx.doi.org/10.1007/s11235-020-00747-w.

[136] Dennis J Britto, Priya M Shanmuga. A profile-based novel framework for detecting EDoS attacks in the cloud environment. Wirel Pers Commun 2021;117:3487–503. http://dx.doi.org/10.1007/s11277-021-08280-y.

[137] Agrawal Neha, Tapaswi Shashikala. An SDN-assisted defense mechanism for the shrew DDoS attack in a cloud computing environment. J Netw Syst Manage 2021;29(12):1–28. http://dx.doi.org/10.1007/s10922-020-09580-7.

[138] Tayfour Omer Elsier, Marsono Muhammad Nadzir. Collaborative detection and mitigation of distributed denial-of-service attacks on software-defined network. Mob Netw Appl 2020. http://dx.doi.org/10.1007/s11036-020-01552-0.

[139] Dahiya Amrita, Gupta Brij B. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Gener Comput Syst 2021;117:193–204. http://dx.doi.org/10.1016/j.future.2020.11.027.

[140] Liu Xinqian, Ren Jiadong, He Haitao, Wang Qian, Song Chen. Low-rate DDoS attacks detection method using data compression and behavior divergence measurement. Comput Secur 2021;100:102107. http://dx.doi.org/10.1016/j.cose.2020.102107.

[141] Mohiddin Shaik Khaja, Midhunchakkaravarthy Divya, Hussain Mohammed Ali. TSWA: a unique approach to overcome interest flooding attacks in the cloud using a combination of TSW and attack detection. Multimedia Tools Appl 2023;1(3):1–19.

[142] Mohan M, Tamizhazhagan V, Balaji S. A perspicacious multi-level defense system against DDoS attacks in cloud using information metric & game theoretical approach. J Netw Syst Manage 2023;31(85):1–28. http://dx.doi.org/10.1007/s10922-023-09776-7.

[143] Kalangi Ruth Ramya, Janardhanarao Dr S, Saikumar Kayam, Veeranjaneyulu Pagadala, J Sirisha, Suman M. Prevention of DDOS attacks in cloud using combinational learning approach. In: 4th IEEE global conference for advancement in technology. GCAT, Bangalore, India: Institute of Electrical and Electronics Engineers (IEEE); 2023, p. 1–8. http://dx.doi.org/10.1109/GCAT.2023.979805.

[144] Sujitha S, Kalaivani V, Abul Hassan A Mohamed, Iswarya K. Protecting data from DDOS attack in a cloud based intrusion detection system security through enhanced RSA algorithm. In: Proceedings of the international conference on sustainable communication networks and application. ICSCNA 2023, IEEE; 2023, p. 230. http://dx.doi.org/10.1109/ICSCNA.2023.00020.

[145] Nadeem Muhammad, Arshad Ali, Riaz Saman, Band Shahab S, Mosavi Amir. Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system. IEEE Access 2021;9:152300–11. http://dx.doi.org/10.1109/ACCESS.2021.3126535.

[146] Fugkeaw Somchart, Moolkaew Narongsak, Wiwattanapornpanit Theerapat, Saengsena Thanyathon, Sanchol Pattavee. A resilient cloud-based DDoS attack detection and prevention system. In: Proceedings of the 20th international joint conference on computer science and software engineering. JCSSE2023, IEEE; 2023.

[147] Kumar Anmol, Agarwal Mayank. Quick service during DDoS attacks in the container-based cloud environment. J Netw Comput Appl 2024;229:103946.