Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Cloud Environments

Muhammad Asif Khan [1], Mohd Faizal Ab Razak [1,*], Zafril Rizal Bin M Azmi[1], Ahmad Firdaus[1], Abdul Hafeez Nuhu[1], Syed Shuja Hussain[2]

[1]Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600 Pekan, Pahang, Malaysia
[2]College of Computer Sciences and Information Technology, Majmaah University, Majmaah, Saudi Arabia

Emails: mcn22002@adab.umpsa.edu.my; faizalrazak@umpsa.edu.my; zafril@umpsa.edu.my; firdausza@umpsa.edu.my; pcp22003@adab.umpsa.edu.my; s.hussain@mu.edu.sa

Abstract

Distributed Denial of Service (DDoS) attacks pose a significant threat to cloud computing environments, necessitating advanced detection methods. This review examines the application of Machine Learning (ML) and Deep Learning (DL) techniques for DDoS detection in cloud settings, focusing on research from 2019 to 2024. It evaluates the effectiveness of various ML and DL approaches, including traditional algorithms, ensemble methods, and advanced neural network architectures, while critically analyzing commonly used datasets for their relevance and limitations in cloud-specific scenarios. Despite improvements in detection accuracy and efficiency, challenges such as outdated datasets, scalability issues, and the need for real-time adaptive learning persist. Future research should focus on developing cloud-specific datasets, advanced feature engineering, explainable AI, and cross-layer detection approaches, with potential exploration of emerging technologies like quantum machine learning.

Keywords: DDoS Attack Detection; Machine Learning; Deep Learning; IDS; Cloud Computing Security

1. Introduction

In the rapidly evolving field of cloud computing, Distributed Denial of Service (DDoS) attacks have become a significant threat to the functioning and safety of online services. These attacks, overwhelming target systems with excessive traffic from multiple sources, have increased in both frequency and complexity. Netscout reported over 7 million global DDoS attacks in the latter half of 2023, a 15% increase from the preceding six months [1]. Similarly, Cloudflare's Q4 2023 DDoS Threat Report revealed a 117% year-over-year surge in HTTP DDoS attacks, with cloud and IT services as primary targets [2]. This trend requires urgent need for effective detection and prevention methods, especially in cloud environments where resources are shared and the potential for widespread damage is considerable. To fully appreciate the gravity of this issue, it is essential to understand the role of cloud computing in modern digital infrastructure and the specific vulnerabilities it presents to DDoS attacks.

Cloud computing, with its scalability, flexibility, and lower costs, has become very important for today's digital infrastructure. However, this centralization of resources makes it a target for cybercriminals [3]. The impact of DDoS attacks on cloud environment can be severe. Service disruptions can render cloud services unavailable, affecting not just the target but potentially multiple clients sharing the same infrastructure. The financial losses can be significant, with a report by Ponemon stating that IT systems downtime costs about $9,000 per minute on average for large companies [4]. Frequent service disruptions can cause customers to lose trust and the company's reputation can be hurt. Also, in cloud environment, DDoS attacks can lead to rapid consumption of computing power, which might lead to higher costs for cloud users [5].

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

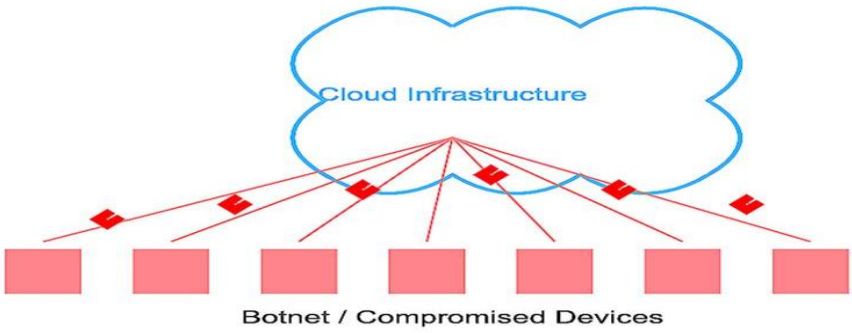

Figure 1. DDoS attack in cloud environment

The adoption of cloud computing continues to accelerate. According to Gartner projections, the deployment of new digital workloads on cloud-native platforms is expected to rise from 30% in 2021 to more than 95% by 2025 [6]. This rapid shift amplifies the importance of developing effective DDoS detection mechanisms tailored to cloud architectures. The COVID-19 pandemic has further accelerated cloud adoption, with Nemertes reporting that 64% of organizations are expected to use cloud-based solutions more than initially planned due to the pandemic [7].

Traditional methods of DDoS detection, such as signature-based approaches and static threshold mechanisms, have proven inadequate in the face of increasingly sophisticated and dynamic attack vectors. These methods often struggle with adaptability, failing to detect new or evolving attack patterns [8]. They may not efficiently handle the massive data volumes in cloud environments, and often misclassify legitimate traffic spikes as attacks, particularly in dynamic cloud settings [9].

To address these limitations, researchers has increasingly turned to more advanced techniques, particularly machine learning (ML) and deep learning (DL). These approaches offer promising solutions for detecting DDoS attacks in cloud environments. They excel at analyzing complex patterns, adapt to new threats, and handle large-scale data processing. ML and DL algorithms can learn from historical data, identify subtle anomalies, and make real-time predictions, characteristics that align well with the dynamic nature of cloud computing [10], [11], [12].

Machine learning encompasses a wide array of algorithms. These algorithms can learn from data without explicit programming [13]. They fall into several categories. Supervised learning methods like Support Vector Machines (SVMs) and Random Forests. Unsupervised techniques comprise K-means clustering and Principal Component Analysis (PCA). Semi-supervised approaches combine small amounts of labeled data with larger sets of unlabeled data. This combination aims to improve detection accuracy.

In addition to these traditional machine learning approaches, deep learning techniques have emerged as particularly promising for DDoS detection due to their ability to model highly complex data relationships. Deep learning, a subset of machine learning, uses artificial neural networks with multiple layers to model complex patterns in data [14]. Several deep learning architectures show promise for DDoS detection. Convolutional Neural Networks (CNNs) are effective at identifying spatial patterns in network traffic data. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can capture temporal dependencies in traffic flows. Autoencoders are useful for anomaly detection. They learn to reconstruct normal traffic patterns.

The primary objective of this review is to provide a comprehensive and up-to-date analysis of ML and DL approaches specifically tailored for DDoS attack detection in cloud environments. While previous reviews have explored DDoS detection in general network settings or specific contexts like Software-Defined Networking (SDN), this paper aims to offer a focused examination of ML and DL techniques applied to cloud-based DDoS detection. The review will evaluate the effectiveness of various ML and DL methods, identify current challenges and limitations in this field, and highlight potential directions for future research. Additionally, this study will provide a detailed analysis of available datasets for DDoS detection in cloud environments, examining their characteristics, strengths, and limitations. This comprehensive evaluation of datasets will offer valuable insights for researchers selecting appropriate data for their studies. By addressing these aspects, the study aims to fill a crucial gap in the existing literature and provide valuable insights for researchers and practitioners working on enhancing security in cloud computing infrastructures.

The contributions of this review paper are to provide a comprehensive analysis of the current state of research in applying ML and DL approaches to DDoS attack detection in cloud environments. Specifically, these contributions are to:

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

1. Evaluate the effectiveness of various ML and DL techniques in detecting and classifying DDoS attacks.
2. Evaluate and analyze available datasets for DDoS attack detection in cloud environments, providing a detailed examination of each dataset's characteristics, strengths and limitations.
3. Identify challenges and limitations in current research in the field of ML and DL approaches for detecting DDoS attacks in cloud environment.
4. Identify potential directions for future work in DDoS detection.

This paper is structured in several sections. Section 2 reviews related works, focusing on recent surveys about DDoS attack detection. Section 3 explains the methodology used for this review. It covers the search strategy, inclusion and exclusion criteria, and data extraction methods. Section 4 provides an overview of DDoS attacks in cloud environments. It discusses various attack types. Sections 5 and 6 form the core of the review. They examine ML and DL approaches for DDoS detection, respectively. These sections analyze recent research, including methods, datasets, and performance metrics. Section 7 discusses analysis of datasets used in DDoS detection in cloud environment. Section 8 discusses challenges and limitations in current research. Section 9 explores future research directions of deep learning-driven DDoS attack detection in cloud environments. Section 10 concludes the paper and suggests future research directions. Throughout the paper, tables and figures summarize key findings and compare different approaches.

2. Related Work

DDoS attacks are becoming more frequent in cloud environments. This has led to extensive research on detection and prevention methods. Many researchers now focus on ML and DL techniques. This section critically examines recent survey papers and reviews in this field. It analyzes their contributions and identify research gaps. The aim is to place the current review in context within the broader field of DDoS attack detection research. The focus is specifically on cloud environments. This analysis helps us understand the current state of research and shows how our review contributes to existing knowledge in this area.

Table 1 presents a comparative overview of related survey papers on this topic, illustrating the scope and focus of recent literature. In the table, '✓' indicates that the paper thoroughly discusses the topic, '*' denotes partial discussion, and 'x' signifies that the topic was not discussed. This notation helps to quickly visualize the coverage and emphasis of each review paper across different aspects of DDoS attack detection in various environments.

Table 1: Comparative overview of related survey papers on this topic

Paper	Year	Focused domain	ML methods	DL methods	Dataset analysis	Time frame covered
[15]	2024	DDoS in SDN enabled cloud	*	*	X	NA
[16]	2023	DDoS in network security	✓	x	✓	2023 and older
[17]	2022	IDS in cloud environment	*	x	*	2010 - 2020
[18]	2021	Cloud security	✓	x	*	2004 - 2019
This paper	2024	DDoS in cloud environment	✓	✓	✓	2019 - 2024

Chahal et al. [15] reviewed DDoS attacks and defenses in SDN-enabled cloud environments. The authors covered a detailed classification of DDoS attack types and strategies. The review also covered defense mechanisms for these specific infrastructures. The authors examined minor ML and DL-based detection methods. Additionally, the study addressed the unique challenges of SDN's dynamic nature. It also discussed scalability issues in cloud environments. The review concluded by identifying open research problems. It emphasized the need for more adaptable and scalable DDoS defenses. These improved solutions are crucial for SDN-enabled cloud systems.

Najafimehr et al. [16] performed a thorough review of DDoS attacks and machine learning-based detection methods. The authors created a detailed classification of DDoS attack types, strategies, and defense mechanisms. The review focused on ML techniques. The authors examined various ML-based detection approaches. These

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

included supervised, unsupervised, and hybrid methods. The authors outlined the benefits and drawbacks of each technique. The researchers discussed several challenges in this field. These included diverse attack types, network heterogeneity, and complex communication protocols. Different relevant datasets were analyzed, noting their strengths and weaknesses. The review also suggested future research directions to address current gaps.

Lata and Singh [17] conducted a comprehensive study on IDS in cloud environments. The researchers examined current security methods and future research areas, providing a detailed overview of cloud security issues. The study emphasized the importance of feature selection and analyzed various IDS techniques. The authors classified these techniques based on the types of attacks identified, their placement, and configuration. Categories included signature-based, anomaly-detection-based, VM introspection-based, hypervisor introspection-based, and hybrid IDS techniques. The authors discussed the strengths and limitations of each approach. The researchers also reviewed existing datasets used for IDS performance evaluation.

Bou Nassif et al. [18] conducted a systematic review in 2021. They focused on ML techniques used for cloud security. The review categorized results into three main areas. These were types of cloud security threats, ML techniques used, and performance outcomes. The researchers identified 11 cloud security areas. DDoS and data privacy were the most common threats. The authors analyzed 63 studies in total. Support Vector Machines (SVM) emerged as the most popular ML technique. SVM was used in both hybrid and standalone models. The authors found 13 different evaluation metrics. The true positive rate was the most frequently applied metric.

While these previous reviews offer valuable insights, there are some gaps in the existing literature. Many reviews primarily focus on general network environments security, with limited exploration of the unique challenges posed by cloud environments in DDoS detection. There is a notable lack of comprehensive comparative analysis of various ML and DL approaches specifically tailored for cloud-based DDoS detection. Furthermore, recent advancements in ML and DL techniques optimized for cloud environments have not been fully explored in some reviews. Additionally, the analysis of datasets specific to cloud-based DDoS detection scenarios is often limited or absent in existing literature. The current review aims to address these gaps by providing a focused, up-to-date analysis of ML and DL approaches for DDoS attack detection in cloud environments, complementing and extending the insights from existing reviews that cover broader or different network contexts.

3. Methodology

To conduct a comprehensive review of ML and DL approaches for detecting DDoS attacks in cloud environments, the study employed a structured methodology. This approach encompasses a detailed search strategy, clearly defined inclusion and exclusion criteria, screening, and systematic data extraction and synthesis methods.

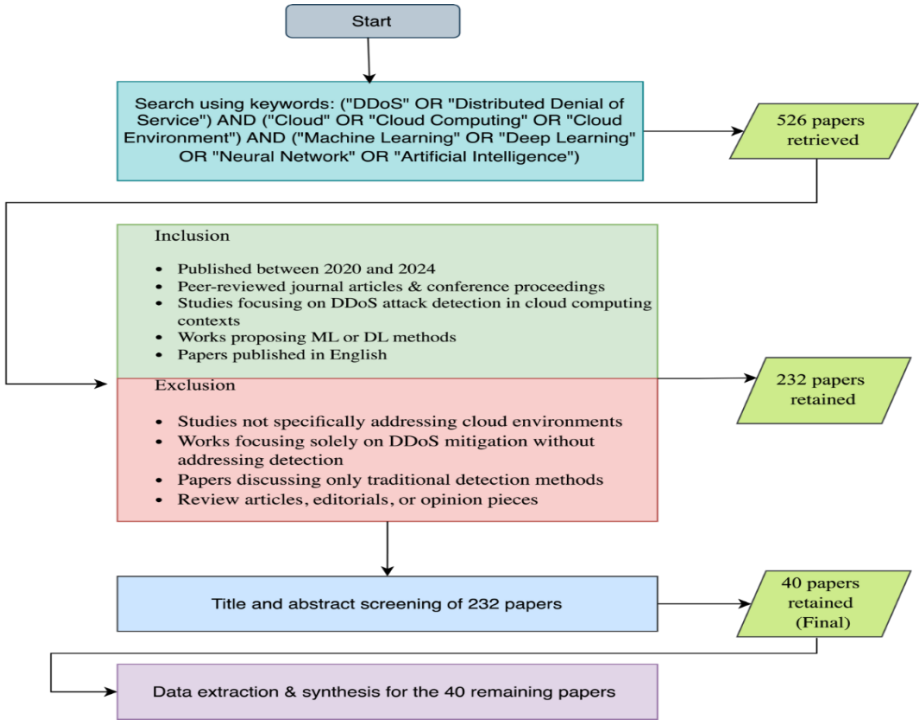

Figure 2. Methodology process

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

3.1 Search Strategy

The literature search focused on Scopus, one of the largest abstract and citation databases of peer-reviewed literature. Scopus covers scientific journals, books, and conference proceedings in various fields, including computer science, engineering, and information technology [19]. Scopus was chosen for its comprehensive coverage, advanced search features, and robust citation analysis capabilities. Its interdisciplinary scope is particularly suitable for the topic at hand, which spans cloud computing, cybersecurity, and machine learning.

The following search string was used in Scopus:

("DDoS" OR "Distributed Denial of Service") AND ("Cloud" OR "Cloud Computing" OR "Cloud Environment") AND ("Machine Learning" OR "Deep Learning" OR "Neural Network" OR "Artificial Intelligence")

This search string was designed to capture papers discussing DDoS attacks in cloud environments, with a specific focus on ML and DL approaches. This initial search yielded a total of 526 papers.

3.2 Inclusion and Exclusion Criteria

The following inclusion criteria were applied:

- Articles published between 2019 and 2024
- Peer-reviewed journal articles and conference proceedings
- Studies focusing on DDoS attack detection in cloud computing contexts
- Works proposing or evaluating ML or DL methods
- Papers published in English

Papers were excluded based on the following criteria:

- Studies not specifically addressing cloud environments
- Works focusing solely on DDoS mitigation without addressing detection
- Papers discussing only traditional detection methods without machine learning components
- Review articles, editorials, or opinion pieces

After applying these criteria, 232 papers remained for further evaluation.

3.3 Screening

The screening phase involved a thorough examination of the remaining 232 papers. This process included title and abstract screening, where each paper's title and abstract were carefully reviewed to ensure relevance to the research question and adherence to the inclusion criteria. After this screening process, 40 papers were selected for the final in-depth analysis and synthesis.

3.4 Data Extraction and Synthesis Methods

The data analysis process for the 40 selected papers involved several key steps. Initially, each paper underwent a thorough examination to extract relevant information, including research objectives, methodologies, key findings, and conclusions. This information was then categorized based on various aspects such as ML/DL techniques used, types of DDoS attacks addressed, and specific cloud environment contexts. A comparative analysis was conducted to identify patterns, trends, and gaps in the current research. The strengths and limitations of each approach were evaluated, considering factors such as detection accuracy. The analyzed information was then synthesized to draw meaningful conclusions about the state of ML and DL approaches for DDoS attack detection in cloud environments.

4. Overview of DDoS Attacks in Cloud Environments

DDoS attacks have evolved into a significant threat to cloud computing environments, exploiting the very features that make cloud services attractive. These attacks aim to overwhelm target systems, rendering them unavailable to legitimate users [20]. Understanding the types of DDoS attacks, is crucial for developing effective defense mechanisms.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

4.1 Types of DDoS Attacks

DDoS attacks targeting cloud environments can be broadly categorized into three main types, each exploiting different vulnerabilities and presenting unique challenges:

Volumetric Attacks: These attacks aim to saturate the bandwidth of the target system. In cloud environments, they often exploit the elastic nature of resources, potentially causing unexpected scaling and associated costs [21]. Types of Volumetric Attacks include UDP Flood, ICMP Flood, DNS Amplification, and NTP Amplification.

Protocol Attacks: These attacks target layer 3 and layer 4 of the OSI model, exploiting vulnerabilities in network protocols. In cloud settings, they can be particularly challenging due to the distributed nature of resources [16]. Types of Protocol Attacks include SYN Flood, Ping of Death, Smurf Attack, and TCP State-Exhaustion.

Application Layer Attacks: These sophisticated attacks target vulnerabilities in web applications and are often difficult to distinguish from legitimate traffic [22]. They are particularly effective against cloud-based web services. Types of Application Layer Attacks include HTTP Flood, Slowloris, RUDY (R-U-Dead-Yet), and DNS Query Flood.

5. Machine Learning Approaches for DDoS Detection

ML has become a valuable tool for detecting and combating DDoS attacks in cloud environments. These methods can learn from data and recognize patterns without much human input. They can also make decisions automatically. Many studies have looked at how well different ML algorithms can detect DDoS attacks. This research has been done extensively in recent years. Table 2 provides a summary of these studies. The results show that ML is effective for this purpose.

Table 2 provides a thorough summary of recent research on ML techniques for DDoS attack detection in cloud environment. It covers various techniques, from basic methods to advanced ones. Basic methods include Naïve Bayes, Decision Trees, and Support Vector Machines. Advanced approaches involve ensemble methods models. The studies in the table are from 2019 to 2024. This shows that researchers are continuously working to make DDoS detection more accurate and efficient.

Table 1: Recent research on ml techniques for DDoS attack detection

Ref	Year	Method	Dataset(s)	Performance (Accuracy %)	Limitations
[23]	2024	Naïve Bayes	KDD, NSL-DD & CIDDS	99.75	High false positive rates & not real-time detection.
[24]	2024	DT, RF	Generated from experimental simulation	99.5 for both DT & RF	The findings are based on simulations, which does not fully capture the complexities of real-world VANET Cloud environments
[25]	2024	RDAER	CICDDoS 2019	99.92	Makes use of one dataset, limiting the generalizability of the framework
[26]	2024	SVM, RF, ANN, NB, Isolation Forest	KDD Cup 1999	SVM: 99.85, RF: 99.99, ANN: 99.92, NB: 92.21, Isolation Forest: 79.71	The study used an outdated dataset

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[27]	2023	DT, NB, SVM, KNN	Generated from experimental simulation	DT: 99.9 NB: 99.7 SVM: 98.9 KNN: 98.7	The feature selection process used in this study may not be fully optimized, potentially impacting the effectiveness of the model.
[28]	2023	Gaussian Naïve Bayes	CICDDoS2018	97.57	The study solely utilizes on dataset, potentially limiting the generalizability of the findings to other datasets
[29]	2023	Ensemble Classifier (SVM, LSTM, XGBoost, FLN)	NSL-KDD, Kyoto, and CSE-CIC-IDS-2018	NSL-KDD: 99.01, Kyoto: 98.99 CSE-CIC-IDS-2018: 99.99	Lacks current datasets. Imbalanced datasets.
[30]	2023	DT, NB, SVM, and KNN	CICDDoS2019	DT: 99, NB: 96 KNN: 95 SVM: 98	Difficulty in determining optimal fusion strategies
[31]	2023	Stacked-Ensemble	CICIDS-2017	99.9	The method may not detect zero-day attacks
[32]	2023	Hybrid SVM-KNN-LR	IIOT Cloud Dataset	96	The study primarily relies on a single dataset
[33]	2023	LR, RF, & NB	Own generated	LR: 99.97, RF: 96.83 NB: 92.68	The study focusses on OpenStack, while relevant to specific cloud environments, limits the generalizability of the findings to other cloud platforms.
[34]	2022	CNN-RF	CIDDS-001	99.99	The system has not been tested in a genuine operational environment
[35]	2022	Perplexed Bayes Classifier	NSL-KDD	99.15	The study solely utilizes on dataset, potentially limiting the generalizability of the findings to other datasets
[36]	2022	K-means clustering	KDD99	97.80	The study used an outdated dataset

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[37]	2022	SaE-ELM	NSL-KDD	97.23	Exhibit longer training times
			ISCX IDS 2012	91.46	
			CIDDS-001	99.28	
[38]	2022	Decision Tree Detection	GureKddcup	98.42	The model is evaluated with one dataset
[39]	2021	DT, KNN, ANN, SNM, RF, & NB	ISOT-CID	DT: 100 KNN: 100 ANN: 94 SVM: 84 RF: 100 NB: 60	Lack of real-time performance. Reliance on a vast dataset. Potential slowdown in real network deployment.
[40]	2021	SaE-ELM	NSL-KDD	86.80	It takes longer training times
			ISCX IDS 2012	98.90	
			UNSW-NB15	89.17	
			CICIDS 2017	99.99	
[41]	2021	Majority Voting Ensemble	CICDDOS2019	98.02	The model is evaluated with one dataset
[42]	2020	V-ELM	NSL-KDD	99.18	High computational resources required for training
			ISCX	92.11	
[31]	2024	BaysCNN, BaysFusCNN	CICDDoS2019		Focused on one dataset

Shang [23] proposed a DDoS attack detection system based on the Naive Bayes algorithm. The system was evaluated using multiple datasets, including KDDCUP99, NSL-KDD, and CIDDS. The proposed approach achieved a high detection accuracy of 99.75%. The author highlighted that while the Naive Bayes algorithm is simple and effective, it exhibited high false positive rates and did not detect DDoS in real-time. The study also compared the Naive Bayes algorithm with other machine learning techniques like Random Forest, showing that Naive Bayes had better predictive power in identifying DDoS attacks.

Setia et al. [24] proposed a DDoS attack detection system for VANET Cloud environments using various machine learning models, including Decision Tree (DT), Random Forest (RF), K-Nearest Neighbour (KNN), Naive Bayes (NB), Logistic Regression (LR), and Kernel SVM. The system was evaluated using datasets generated from NS2 simulations. The DT and RF models achieved the highest detection accuracy of 99.59%, while the KNN, NB, and LR models also performed well with accuracies of 97.74%, 97.13%, and 97.13% respectively. However, the Kernel SVM model demonstrated significantly lower performance with an accuracy of 58.40%. Additionally, the findings are based on simulations, which may not fully capture the complexities of real-world VANET Cloud environments.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

Songa and Karri [25] introduced a DDoS attack detection framework named RDAER, which integrates multiple machine learning techniques including Recursive Feature Elimination (RFE), Density-Based Spatial Clustering of Applications with Noise (DBSCAN), Auto Regressive Integrated Moving Average (ARIMA), Exponential Smoothing, and a Rule-based Classifier. Their system was evaluated using the CICDDoS 2019 dataset and achieved an impressive accuracy of 99.92%. The RDAER framework focuses on early detection by analyzing traffic at the SDN switch level and consolidating data through event correlation.

Rexha et al. [27] developed a system to detect DDoS attacks using ML. They tested several algorithms: DT, SVM, NB, and KNN. The system was evaluated with data from simulated DDoS and MitC attacks. DT performed best, with 99.9% accuracy. NB followed at 99.7%, then SVM at 98.9%, and KNN at 98.7%. The study noted that feature selection process employed in the study may not be fully optimized, potentially impacting the accuracy and effectiveness of the detection model.

Naiem et al. [28] proposed an enhanced DDoS detection system using a Gaussian Naïve Bayes (GNB) classifier, focusing on improving its efficiency through iterative feature selection and data preprocessing. The system was evaluated using the CICDDoS2018 dataset. The proposed enhancements led to a 2% increase in accuracy for the mutual information model and an average overall accuracy and precision improvement of 1.5%. The authors addressed the zero-frequency problem by replacing missing values with the mode or mean and handled data imbalances using SMOTE. Despite these improvements, the GNB classifier's accuracy remained lower than other classifiers such as DT, RF, and SVM, primarily due to the zero-frequency issue and the assumption of feature independence.

Mishra et al. [35] introduced a novel DDoS attack detection framework utilizing the Perplexed Bayes Classifier. The system was trained and tested using the NSL-KDD dataset, achieving an impressive accuracy of 99.15%. The proposed classifier was compared with existing ML algorithms such as NB and RF, demonstrating superior performance. Additionally, the study compared the classifier with nature-inspired feature selection methods like Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), finding that the Perplexed Bayes Classifier outperformed these methods by 2% and 8%, respectively.

Arunkumar and Kumar [36] proposed a method for detecting DDoS attacks in cloud environments using a combination of rule-based classification and K-Means clustering. The system was evaluated using the KDD 99 dataset, achieving an accuracy of 97.8%. The approach involves capturing traffic, extracting vital attributes using entropy, grouping traffic using K-Means clustering, and classifying it with a rule-based system. The proposed method demonstrated high accuracy and low false positive rates in detecting UDP, TCP, and ICMP-based malicious traffic.

Kushwah and Ranga [40] proposed a DDoS attack detection system based on an improved Self-adaptive evolutionary extreme learning machine (SaE-ELM). Their system was evaluated using multiple datasets, including NSL-KDD, ISCX IDS 2012, UNSW-NB15, and CICIDS 2017. The proposed approach achieved high detection accuracies across all datasets, ranging from 86.80% to 99.99%. The authors improved the original SaE-ELM by incorporating two additional features: the ability to adapt the best suitable crossover operator and automatic determination of the appropriate number of hidden layer neurons. These enhancements aimed to improve the learning and classification capabilities of the model. While the system showed improved performance compared to the original SaE-ELM and other state-of-the-art techniques, it did exhibit longer training times.

Kushwah and Ranga [42] proposed a DDoS attack detection system based on a voting extreme learning machine (V-ELM) classifier. Their system was evaluated using two benchmark datasets, NSL-KDD and ISCX intrusion detection datasets. The proposed approach achieved detection accuracies of 99.18% with the NSL-KDD dataset and 92.11% with the ISCX dataset. The V-ELM classifier uses multiple extreme learning machines simultaneously, combining their results through majority voting to improve detection accuracy and reduce false alarms.

6. Deep Learning Approaches for DDoS Detection

In recent years, DL techniques have emerged as powerful tools for detecting DDoS attacks in cloud environments. These advanced machine learning models, inspired by the structure and function of the human brain, have demonstrated remarkable capabilities in identifying complex patterns and anomalies in network traffic data [40]. Unlike traditional machine learning approaches, deep learning models can automatically extract high-level features from raw data, making them particularly well-suited for the dynamic and complex nature of cloud computing environments [41].

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

This section explores the application of various deep learning techniques in DDoS attack detection within cloud environments. We will examine the strengths and weaknesses of each approach, discuss their implementation challenges, and evaluate their performance in real-world scenarios. By understanding these advanced methodologies, we can gain insights into the current state-of-the-art in DDoS detection and identify potential areas for future research and improvement. Table 3 provides a summary of recent research on DL techniques for DDoS attack detection in cloud environment.

Table 2: Recent research on DL techniques for DDoS attack detection

Ref	Year	Method	Dataset	Performance (Accuracy %)	Limitations
[43]	2024	BaysCNN, BaysFusCNN	CICDDoS2019	BaysCNN: 99.66, BaysFusCNN: 99.79	The study's reliance on offline datasets limits its applicability to dynamic real-world DDoS attack scenarios.
[44]	2024	CNN-DT	CIDDS-001	99.97	The dataset used in the study suffers from limited features, class imbalance, and data duplication, potentially impacting the depth of analysis and reliability of results.
[45]	2024	Bi-LSTM	CSE-CIC-IDS2018-AWS, CICIDS2017, CIC DoS datasets (2016) and source dataset	97.00	The study focuses on evaluating the model's performance using offline datasets. However, real-world DDoS attacks occur in dynamic network environments with real-time traffic flows.
[46]	2024	Deep Neural Network	NSL-KDD	96.31	The model is evaluated with one dataset
[47]	2024	EFS-DNN	CIC-IDS 2017	96.12	Exhibited computational complexity. Limited Discussion on Mitigation Strategies
[48]	2024	ML & DL	CIC-IDS 2017	CNN: 95.85 LSTM: 96.49 Bi-LSTM: 96.34 GRU:96.22	Limited Discussion on Computational Complexity
[49]	2023	Hybrid CNN-LSTM	CICIDS 2017	97.9	The current study lacks real-time detection capabilities for network anomalies
[50]	2023	Ensemble-based DL combining K-means clustering with deep learning classifiers (CNN, RNN, GRU, DNN, LSTM)	CICIDS 2018, SDN-based DDoS attack datasets	99.68	Limited Focus on Real-Time Attack Detection and Mitigation
[51]	2023	MMEDRL-ADM	SDN-specific dataset created using a mininet emulator	Training, testing split (70:30) 98.84 (60:40) 98.19	Limited Discussion on the Impact of Network Dynamics on Detection Accuracy

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[52]	2023	FACVO- DNFN	NSL-KDD	93.04	The proposed model does not support real-time applications
			BoT-IoT	92.00	
[53]	2023	GHLBO-DSA	BoT-IoT	91.70	The study doesn't include an overhead analysis of the proposed model
			NSL-KDD	91.40	
[8]	2023	HA-LRDD	CIC-DDoS2019	Detection Rate: 95.32	Needs significant computational resources
[54]	2023	Hybrid LSTM and RNN for feature selection, MLP Classifier for detection	Kaggle dataset	98.85	The authors acknowledge the dataset has been modified from its original form to protect confidential information. This modification could potentially impact the representativeness of the dataset and the generalizability of the study's findings.
[55]	2022	LSTM	CICDDoS 2019	99.83	High computational cost during training and testing; the system was not tested in a real cloud environment.
[56]	2022	DNN with Particle Swarm Optimization	CICIDS 2017	99.81	The model is evaluated with one dataset
[57]	2022	Deep Generative Radial Neural Network	NSL-KDD	90.00	The study evaluates the model using simulation parameters
[58]	2021	FS-WOA–DNN	CICIDS2017	95.35	High computational complexity and resource consumption during feature selection and classification
[59]	2021	Big data and DL techniques	KDDCUP99	99.73	The study is limited by its evaluation on a single dataset
[60]	2020	AE and DNN	NSL-KDD	98.43	Limited validation across diverse datasets. Lack of real-time detection capabilities. High computational complexity for big data analysis
			CICIDS2017	98.92	
[61]	2022	Stacked contractive autoencoder & SVM	NSL-KDD	2-class: 88.73 5-class: 87.33 13-class: 89.93	The study focuses on evaluating the model's performance using offline datasets. However, real-world DDoS attacks occur in dynamic network environments with real-time traffic flows
			KDD Cup 99	2-class: 98.11 5-class: 97.87	

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

AlSaleh et al. [43] introduced a novel Bayesian-based Convolutional Neural Network (BaysCNN) model for DDoS cloud detection. Their research utilized the CICDDoS2019 dataset and achieved an impressive average accuracy of 99.66% across 13 multi-class attacks. The authors further enhanced their model with a Data Fusion approach (BaysFusCNN), reaching an even higher accuracy of 99.79%. This study demonstrated the potential of combining Bayesian techniques with deep learning architectures to improve DDoS detection in cloud environments. The high accuracy rates suggest that this approach could be particularly effective in identifying and classifying various types of DDoS attacks in cloud computing settings.

Ouhssini et al. [44] introduced DeepDefend, a framework for real-time DDoS attack detection and prevention in cloud environments. It uses CNN-LSTM-Transformer networks to predict network traffic entropy and identify potential attacks. A genetic algorithm is used for optimal feature selection. This improves the AutoCNN-DT model's ability to distinguish between normal and attack traffic. The system was tested with the CIDDS-001 traffic dataset and showed high accuracy in entropy forecasting and quick, precise DDoS attack detection.

Pandithurai et al. [45] proposed a DDoS attack prediction model utilizing a Honey Badger Optimization (HBO) algorithm for feature selection and a Bi-Directional Long Short-Term Memory (Bi-LSTM) classifier. The model was evaluated using multiple datasets, including a DDoS attack dataset from Kaggle, CSE-CIC-IDS2018-AWS, CICIDS2017, CIC DoS datasets (2016) and source dataset. The proposed approach achieved an accuracy of 97%. The authors employed Bayesian and Z-Score normalization for preprocessing and minimized the Mean Square Error (MSE) to select optimal features.

Haval and Dash [47] proposed a DDoS attack detection system using an Ensemble Feature Selection-Deep Neural Network (EFS-DNN). Their system was evaluated using the CIC-IDS 2017 dataset. The proposed approach achieved a high detection accuracy of 96.12%. The authors improved the detection efficiency by employing an ensemble feature selection method that combines PSO, GWO, and WOA to identify the most relevant features. These selected features were then used in a DNN classifier to distinguish between normal and malicious data. While the system demonstrated superior performance compared to other models, it exhibited computational complexity due to the ensemble feature selection and deep learning model.

Sanjalawe and Althobaiti [49] proposed a DDoS attack detection system utilizing a hybrid CNN and LSTM model combined with an ensemble feature selection approach. The system was evaluated using the CICIDS 2017 dataset and achieved an accuracy of 97.9%. The ensemble feature selection method incorporated PSO, GWO, Krill Herd (KH), and Whale Optimization Algorithm (WOA) to select the most significant features, enhancing the detection performance. While the proposed IDS demonstrated high accuracy and efficiency, it was tested only on a single dataset, indicating a need for further validation on more current datasets to ensure robustness and generalizability.

Bingu and Jothilakshmi [50] proposed an ensemble-based deep learning technique for detecting DDoS attacks in cloud and SDN-based cloud environments. Their system integrates K-means clustering with various deep learning classifiers, including CNN, RNN, GRU, DNN, and LSTM. The proposed model was evaluated using the CICIDS 2018 and SDN-based DDoS attack datasets, achieving an accuracy of 99.685%. The ensemble approach was designed to enhance the performance of deep learning classifiers without significant computational complexity.

Selvan et al. [32] introduced a DDoS attack detection system utilizing a Fractional Anti Corona Virus Optimization-based Deep Neuro-Fuzzy Network (FACVO-based DNFN). The system was tested on the NSL-KDD and BoT-IoT datasets, achieving high detection accuracies of 93.04% and 92.00%, respectively. The FACVO algorithm, which combines Fractional Calculus (FC) and Anti Corona Virus Optimization (ACVO), was used to train the DNFN. This approach aimed to enhance the detection performance by fusing features. Despite its high accuracy, the model's limitation lies in its lack of support for real-time applications.

Balasubramaniam et al. [53] developed a DDoS attack detection system using a novel Gradient Hybrid Leader-Based Optimization (GHLBO) algorithm to train a Deep Stacked Autoencoder (DSA). The system was evaluated on the BOT-IoT and NSL-KDD datasets, achieving high detection accuracies of 91.7% and 91.4%, respectively. The GHLBO algorithm integrates gradient descent with a hybrid leader-based optimization approach, enhancing the training process of the DSA. The method also incorporates feature fusion using a Deep Maxout Network (DMN) and data augmentation through oversampling. While the proposed system demonstrated high performance, the authors noted that overhead analysis was not included and suggested incorporating advanced optimization methods and additional performance metrics in future research.

Pasha et al. [8] proposed a framework for detecting low-rate DDoS attacks in cloud environments using a hybrid approach that combines Sparse Autoencoder (SAE) and Convolutional Neural Network (CNN). The proposed system, named Hybrid Approach for Low-Rate DDoS Detection (HA-LRDD), was evaluated using the CIC-DDoS2019 dataset. The framework achieved a high detection rate of 95.32% and a low false positivity rate of 0.57%. The authors used DL techniques to extract and classify features from network traffic, aiming to improve

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

detection accuracy and mitigate the impact of low-rate DDoS attacks. While the framework demonstrated superior performance compared to existing methods, it may require significant computational resources for training and could face challenges in adapting to various low-rate DDoS attack patterns.

Aydın et al. [55] introduced LSTM-CLOUD, a system for detecting DDoS attacks. This system uses LSTM. It was tested with the CICDDoS2019 dataset and showed high accuracy at 99.83%. LSTM-CLOUD has two main parts: detection and defense. The detection part uses an LSTM model to detect DDoS attacks. The defense part then acts to reduce these attacks. While very accurate, the system hasn't been tested in a real cloud setting yet.

Agarwal et al. [58] proposed a DDoS attack detection system using a combination of Feature Selection-Whale Optimization Algorithm and Deep Neural Network (FS-WOA–DNN). The system was evaluated using the CIC-IDS 2017 dataset and achieved an accuracy of 95.35%. The proposed method involves pre-processing the dataset using min-max normalization, selecting optimal features with the Whale Optimization Algorithm, and classifying the data using a DNN. Despite its high detection accuracy, the system faces limitations in terms of computational complexity and resource consumption during the feature selection and classification processes.

7. Analysis of DDoS Detection Datasets

Choosing the right datasets is vital for creating and testing effective DDoS detection models in cloud environment. This section examines commonly used datasets in recent studies. It looks at their features, strengths, and weaknesses. Datasets are essential for developing and accessing DDoS detection systems, especially in cloud environments. They give researchers standard benchmarks to test their algorithms. These benchmarks help compare results and confirm the effectiveness of proposed solutions. However, cloud technologies and attack methods are changing rapidly. This makes it challenging to keep datasets relevant and current. Table 4 provides an overview of commonly used datasets in recent DDoS detection research, focusing on their relevance to cloud environments

Table 4: Commonly used datasets for DDoS attack detection in cloud environment

Ref	Dataset	Year	Cloud-specific	DDoS Variety	Size
[62]	CICDDoS2019	2019	Partial	High	50,006,249
[63]	CICIDS2017	2017	No	Medium	2,827,876
[64]	NSL-KDD	2009	No	Low	148,517
[65]	UNSW-NB15	2015	No	Medium	2,540,044
[66]	CSE-CIC-IDS2018	2018	Partial	Low	16,233,002
[67]	BoT-IoT	2018	Partial	Low	73,370,443
[68]	CIDDS-001	2017	Yes	Low	32,000,000
[69]	KDDCup99	1999	No	Low	4,898,430
[70]	ISCXIDS 2012	2012	No	High	1,526,148
[71]	Kyoto	2006+	No	Medium	216,887

While these datasets are widely used in DDoS detection research, it is important to note that many of them are not specifically designed for cloud environments. Researchers often adapt these general network security datasets to cloud scenarios, which may not fully capture the unique characteristics of cloud-based DDoS attacks.

The CICDDoS2019 and BoT-IoT datasets stand out for their large number of samples, which can be beneficial for training robust models. The CSE-CIC-IDS2018 and CIDDS-001 datasets also offer a substantial number of samples while providing some relevance to cloud environments. Despite having fewer samples, the NSL-KDD dataset remains widely used due to its balanced nature and the absence of redundant records found in its predecessor, the KDD Cup 1999 dataset. However, both these datasets are considered outdated for modern DDoS detection scenarios. The UNSW-NB15 and CICIDS2017 datasets offer a moderate number of samples with a good variety of modern attack types, although they lack cloud-specificity.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

The continued use of older and non-cloud-specific datasets highlights the need for more up-to-date, cloud-specific datasets in this field. As cloud technologies and attack methods continue to evolve, the development of new, specialized datasets that accurately reflect the current landscape of cloud-based DDoS attacks, with many samples representing diverse scenarios, remains a crucial area for future work in this field.

8. Challenges and Limitations

The application of ML and DL techniques for DDoS attack detection in cloud environments, while promising, faces several significant challenges and limitations. One of the primary issues is the lack of up-to-date, cloud-specific datasets. Many commonly used datasets are outdated or not representative of modern cloud environments, making it difficult to develop and validate models that can effectively detect contemporary DDoS attacks. Creating realistic datasets that capture the complexity of cloud-based DDoS attacks remains a significant challenge, hindering the development of more accurate and reliable detection systems.

Scalability is another major concern in current research. Many proposed models are tested on small-scale datasets or simulated environments, which may not accurately represent the massive traffic volumes encountered in real cloud infrastructures. Scaling detection methods to handle these enormous data streams in real-time poses significant challenges, both in terms of computational resources and maintaining detection accuracy. This scalability issue is closely tied to the challenge of real-time detection, where researchers must balance the trade-off between detection speed and accuracy. Implementing complex ML/DL models for real-time detection without introducing significant delays or compromising accuracy remains a formidable task.

The rapid evolution of DDoS attack techniques presents another substantial challenge. As attackers continually develop new methods, detection models can quickly become outdated. This necessitates frequent model updates and retraining, which can be resource-intensive and time-consuming. Moreover, detecting zero-day or previously unseen attack patterns remains a significant challenge for many current ML/DL approaches, highlighting the need for more adaptive and robust detection methods.

False positive rates continue to be a concern in many studies. While high accuracy rates are often reported, the issue of false positives is not always adequately addressed. In dynamic cloud environments, distinguishing between legitimate traffic spikes and DDoS attacks is particularly challenging. High false positive rates can lead to unnecessary service disruptions and resource allocation, potentially impacting the overall performance and reliability of cloud services.

The interpretability of ML/DL models, particularly deep learning models, poses another significant challenge. Many of these models operate as "black boxes," making it difficult to understand their decision-making processes. This lack of transparency can be problematic for security audits and compliance requirements, especially in highly regulated industries. Developing more interpretable models without sacrificing detection performance remains an important area for future research.

Finally, feature selection and engineering present additional difficulties. Identifying the most relevant features for cloud-based DDoS detection remains challenging, especially given the dynamic nature of cloud environments. Maintaining optimal feature sets over time and across different cloud configurations adds to the complexity of developing effective detection models.

Addressing these challenges and limitations will be crucial for advancing the field of ML and DL-based DDoS attack detection in cloud environments. Future research should focus on developing more robust, scalable, and adaptive models that can effectively operate in real-world cloud environments while addressing privacy concerns and maintaining interpretability

9. Future Work and Research Directions

The detection of DDoS attacks in cloud environments ML and DL is a fast-changing field. There are many promising areas for future study. These research directions aim to overcome current limitations. They also seek to improve how well detection systems work in real cloud settings. Researchers are looking at ways to make these systems more effective and efficient.

- Development of Cloud-Specific Datasets:

A key area for future research is developing new, comprehensive datasets. These datasets should accurately reflect modern cloud environments. They need to include various DDoS attack types and normal traffic patterns. Cloud-specific network behaviors should also be represented. Collaboration is essential for this task. Cloud service providers, security researchers, and academic institutions could work together. Their goal would be to create

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

standardized datasets that are publicly available. Such datasets would greatly benefit research in this field. They would help researchers better understand and address DDoS attacks in cloud settings.

- Advanced Feature Engineering and Selection:

Future research should focus on developing more sophisticated feature engineering techniques tailored to cloud environments. This could involve exploring dynamic feature selection methods that adapt to changing network conditions and emerging attack patterns. Incorporating cloud-specific metrics, such as resource utilization and auto-scaling behaviors, into feature sets could enhance detection accuracy and reduce false positives.

- Hybrid and Ensemble Models:

A promising research direction is the use of hybrid or ensemble models. These models combine multiple ML and DL techniques. Future studies could investigate how to integrate different algorithms. Each algorithm could specialize in detecting specific DDoS attack types. They could also analyze aspects of network traffic. This approach may result in more robust detection systems. These systems could be more versatile and handle various attack scenarios. By combining different techniques, researchers aim to improve overall detection performance. This could lead to more effective protection against DDoS attacks in cloud environments.

- Real-Time Adaptive Learning:

Exploring techniques for continuous, real-time model updating and adaptation is essential for keeping pace with evolving DDoS attack strategies. Future work could investigate online learning algorithms and incremental training methods that allow models to dynamically adjust to new patterns without requiring complete retraining.

- Explainable AI for DDoS Detection:

Developing interpretable ML and DL models is essential. These models help build trust in automated DDoS detection systems. Future research should focus on developing explainable AI techniques. These techniques would provide clear insights into how detection models make decisions. Interpretable models offer several benefits. They can help refine the detection systems. They also assist in meeting regulatory requirements in cloud environments. By making AI decisions more transparent, researchers can improve the reliability and acceptance of DDoS detection systems.

- Cross-Layer Detection Approaches:

Future studies could investigate cross-layer detection methods. These methods would analyze data from multiple network stack layers at the same time. This approach offers a more complete view of network behavior. It examines information from various network levels simultaneously. By doing so, it could enhance detection accuracy. It might also help reduce false positive alerts. This holistic strategy could provide a more thorough understanding of network activities.

- Transfer Learning for Cloud Environments:

Investigating transfer learning techniques to adapt pre-trained models to different cloud environments or new types of DDoS attacks could significantly reduce the time and resources required for model development and deployment.

- Quantum Machine Learning for DDoS Detection:

As quantum computing advances, exploring its potential applications in DDoS detection presents an intriguing long-term research direction. Quantum machine learning algorithms could potentially offer significant improvements in processing speed and pattern recognition for large-scale network traffic analysis.

- Automated Response and Mitigation Integration:

Future work should focus on seamlessly integrating ML and DL-based detection systems with automated response and mitigation mechanisms. This could involve developing intelligent systems that not only detect attacks but also automatically implement appropriate countermeasures based on the specific characteristics of the detected threat.

By pursuing these research directions, the field of ML and DL-based DDoS attack detection in cloud environments can continue to advance, leading to more robust, efficient, and effective security solutions for modern cloud infrastructures. As cloud technologies evolve and new challenges emerge, ongoing research in these areas will be crucial for maintaining the security and reliability of cloud services in the face of increasingly sophisticated DDoS threats.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

10. Conclusion

This comprehensive review has examined the application of ML and DL approaches for detecting DDoS attacks in cloud environments, analyzing research from 2019 to 2024. The review reveals that while ML and DL techniques show significant promise in improving DDoS detection accuracy and efficiency, several challenges persist. These include the lack of up-to-date, cloud-specific datasets, scalability issues in real-world cloud environments, and the need for real-time adaptive learning to combat evolving attack patterns. Despite these challenges, the field is advancing rapidly, with hybrid and ensemble models, as well as deep learning architectures like CNN and LSTM, showing particularly promising results. Future research directions should focus on developing cloud-specific datasets, advancing feature engineering techniques, exploring explainable AI for better interpretability, and investigating cross-layer detection approaches. Additionally, the integration of quantum machine learning and automated response mechanisms presents exciting long-term research opportunities. As cloud technologies continue to evolve, ongoing research in these areas will be crucial for developing robust, efficient, and adaptive DDoS detection systems capable of securing modern cloud infrastructures against increasingly sophisticated threats.

Acknowledgements

The authors would like to thank the University Malaysia Pahang Al-Sultan Abdullah for providing financial support under Internal Research grant **RDU210321**.

References

[1] Chris Conrad *et al.*, "NETSCOUT DDoS THREAT INTELLIGENCE REPORT / FINDINGS FROM 2ND HALF 2023." Accessed: Jun. 14, 2024. [Online]. Available: https://www.netscout.com/threatreport/wp-content/uploads/2023/09/Threat_Report_1h2023.pdf

[2] Y. Omer and P. Jorge, "DDoS threat report for 2023 Q4." Accessed: Jul. 03, 2024. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q4

[3] J. S. Saini, D. K. Saini, P. Gupta, C. S. Lamba, and G. M. Rao, "Cloud Computing: Legal Issues and Provision," *Security and Communication Networks*, vol. 2022, pp. 1–13, Aug. 2022, doi: 10.1155/2022/2288961.

[4] Ponemon Institute, "Cost of Data Center Outages." Accessed: Jul. 04, 2024. [Online]. Available: https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

[5] Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy," *Applied Sciences*, vol. 12, no. 23, p. 12441, Dec. 2022, doi: 10.3390/app122312441.

[6] Gartner, "Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences." Accessed: Jul. 15, 2024. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

[7] K. Finnell, "Time to move to UCaaS? UC's future indeed looks 'cloudy,'" TechTarget. Accessed: Jul. 16, 2024. [Online]. Available: https://www.techtarget.com/searchunifiedcommunications/ehandbook/Time-to-move-to-UCaaS-UCs-future-indeed-looks-cloudy

[8] M. J. Pasha, K. P. Rao, A. MallaReddy, and V. Bande, "LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments," *Measurement: Sensors*, vol. 28, p. 100828, Aug. 2023, doi: 10.1016/j.measen.2023.100828.

[9] H. Attou *et al.*, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Applied Sciences*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[10] Q. Li *et al.*, "A comprehensive survey on DDoS defense systems: New trends and challenges," *Computer Networks*, vol. 233, p. 109895, Sep. 2023, doi: 10.1016/j.comnet.2023.109895.

[11] N. Ahmed *et al.*, "Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction," *Sensors*, vol. 22, no. 20, p. 7896, Oct. 2022, doi: 10.3390/s22207896.

[12] I. Ahmad, Z. Wan, and A. Ahmad, "A big data analytics for DDOS attack detection using optimized ensemble framework in Internet of Things," *Internet of Things*, vol. 23, p. 100825, Oct. 2023, doi: 10.1016/j.iot.2023.100825.

[13] K. Arumugam *et al.*, "Towards applicability of machine learning techniques in agriculture and energy sector," *Mater Today Proc*, vol. 51, pp. 2260–2263, 2022, doi: 10.1016/j.matpr.2021.11.394.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[14] M. Soori, B. Arezoo, and R. Dastres, "Artificial intelligence, machine learning and deep learning in advanced robotics, a review," *Cognitive Robotics*, vol. 3, pp. 54–70, 2023, doi: 10.1016/j.cogr.2023.04.001.
[15] J. K. Chahal, A. Bhandari, and S. Behal, "DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges," *Comput Sci Rev*, vol. 53, p. 100644, Aug. 2024, doi: 10.1016/j.cosrev.2024.100644.
[16] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, "DDoS attacks and machine-learning-based detection methods: A survey and taxonomy," *Engineering Reports*, May 2023, doi: 10.1002/eng2.12697.
[17] S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100134, Nov. 2022, doi: 10.1016/j.jjimei.2022.100134.
[18] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021, doi: 10.1109/ACCESS.2021.3054129.
[19] J. Baas, M. Schotten, A. Plume, G. Côté, and R. Karimi, "Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies," *Quantitative Science Studies*, vol. 1, no. 1, pp. 377–386, Feb. 2020, doi: 10.1162/qss_a_00019.
[20] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.
[21] R. M. A. Haseeb-ur-rehman *et al.*, "High-Speed Network DDoS Attack Detection: A Survey," *Sensors*, vol. 23, no. 15, p. 6850, Aug. 2023, doi: 10.3390/s23156850.
[22] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput Sci Rev*, vol. 39, p. 100332, Feb. 2021, doi: 10.1016/j.cosrev.2020.100332.
[23] Y. Shang, "Prevention and detection of DDOS attack in virtual cloud computing environment using Naive Bayes algorithm of machine learning," *Measurement: Sensors*, vol. 31, p. 100991, Feb. 2024, doi: 10.1016/j.measen.2023.100991.
[24] H. Setia *et al.*, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Security and Applications*, vol. 2, p. 100037, 2024, doi: 10.1016/j.csa.2024.100037.
[25] A. V. Songa and G. R. Karri, "An integrated SDN framework for early detection of DDoS attacks in cloud computing," *Journal of Cloud Computing*, vol. 13, no. 1, p. 64, Mar. 2024, doi: 10.1186/s13677-024-00625-9.
[26] A. Naithani, S. N. Singh, K. Kant Singh, and S. Kumar, "Machine Learning for Cloud-Based DDoS Attack Detection: A Comprehensive Algorithmic Evaluation," in *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, Jan. 2024, pp. 561–567. doi: 10.1109/Confluence60223.2024.10463504.
[27] B. Rexha, R. Thaqi, A. Mazrekaj, and K. Vishi, "Guarding the Cloud: An Effective Detection of Cloud-Based Cyber Attacks using Machine Learning Algorithms," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 18, pp. 158–174, Dec. 2023, doi: 10.3991/ijoe.v19i18.45483.
[28] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, "Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing," *IEEE Access*, vol. 11, pp. 124597–124608, 2023, doi: 10.1109/ACCESS.2023.3328951.
[29] M. Bakro *et al.*, "Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier," *Electronics (Basel)*, vol. 12, no. 11, p. 2427, May 2023, doi: 10.3390/electronics12112427.
[30] L. M. Pattnaik, P. K. Swain, S. Satpathy, and A. N. Panda, "Cloud DDoS Attack Detection Model with Data Fusion & Machine Learning Classifiers," *ICST Transactions on Scalable Information Systems*, Sep. 2023, doi: 10.4108/eetsis.3936.
[31] P. Verma, A. R. K. Kowsik, R. K. Pateriya, N. Bharot, A. Vidyarthi, and D. Gupta, "A Stacked Ensemble Approach to Generalize the Classifier Prediction for the Detection of DDoS Attack in Cloud Network," *Mobile Networks and Applications*, Aug. 2023, doi: 10.1007/s11036-023-02225-4.
[32] U. Islam, A. Al-Atawi, H. S. Alwageed, M. Ahsan, F. A. Awwad, and M. R. Abonazel, "Real-Time Detection Schemes for Memory DoS (M-DoS) Attacks on Cloud Computing Applications," *IEEE Access*, vol. 11, pp. 74641–74656, 2023, doi: 10.1109/ACCESS.2023.3290910.
[33] R. Patil, G. Kandakur, R. Vardhamane, S. Kotyal, N. D. G., and A. Kachavimath, "A Collaborative Approach to Detect DDoS Attacks in OpenStack-based Cloud using Entropy and Machine Learning," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10306629.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[34] M. Ouhssini and K. Afdel, "Machine Learning Methods for DDoS Attacks Detection in the Cloud Environment," 2022, pp. 401–413. doi: 10.1007/978-3-030-90639-9_32.
[35] N. Mishra, R. K. Singh, and S. K. Yadav, "Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier," *Comput Intell Neurosci*, vol. 2022, pp. 1–13, Jul. 2022, doi: 10.1155/2022/9151847.
[36] M. Arunkumar and K. Ashok Kumar, "Malicious attack detection approach in cloud computing using machine learning techniques," *Soft comput*, vol. 26, no. 23, pp. 13097–13107, Dec. 2022, doi: 10.1007/s00500-021-06679-0.
[37] G. S. Kushwah and V. Ranga, "Detecting DDoS Attacks in Cloud Computing Using Extreme Learning Machine and Adaptive Differential Evolution," *Wirel Pers Commun*, vol. 124, no. 3, pp. 2613–2636, Jun. 2022, doi: 10.1007/s11277-022-09481-9.
[38] J. Praba. J and R. Sridaran, "An SDN-based Decision Tree Detection (DTD) Model for Detecting DDoS Attacks in Cloud Environment," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 7, 2022, doi: 10.14569/IJACSA.2022.0130708.
[39] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," *J Big Data*, vol. 8, no. 1, p. 90, Dec. 2021, doi: 10.1186/s40537-021-00475-1.
[40] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Comput Secur*, vol. 105, p. 102260, Jun. 2021, doi: 10.1016/j.cose.2021.102260.
[41] A. A. Alqarni, "Majority Vote-Based Ensemble Approach for Distributed Denial of Service Attack Detection in Cloud Computing," *Journal of Cyber Security and Mobility*, Mar. 2022, doi: 10.13052/jcsm2245-1439.1126.
[42] G. S. Kushwah and V. Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," *Journal of Information Security and Applications*, vol. 53, p. 102532, Aug. 2020, doi: 10.1016/j.jisa.2020.102532.
[43] I. AlSaleh, A. Al-Samawi, and L. Nissirat, "Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements," *Sensors*, vol. 24, no. 5, p. 1418, Feb. 2024, doi: 10.3390/s24051418.
[44] M. Ouhssini, K. Afdel, E. Agherrabi, M. Akouhar, and A. Abarda, "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, p. 101938, Feb. 2024, doi: 10.1016/j.jksuci.2024.101938.
[45] O. Pandithurai, C. Venkataiah, S. Tiwari, and N. Ramanjaneyulu, "DDoS attack prediction using a honey badger optimization algorithm based feature selection and Bi-LSTM in cloud environment," *Expert Syst Appl*, vol. 241, p. 122544, May 2024, doi: 10.1016/j.eswa.2023.122544.
[46] R. Verma, M. Jailia, M. Kumar, and B. Kaliraman, "Deep Neural Network Model for Improved DDoS Attack Detection in Cloud Environments," in *2024 5th International Conference for Emerging Technology (INCET)*, IEEE, May 2024, pp. 1–6. doi: 10.1109/INCET61516.2024.10593561.
[47] A. H. Madhukar and S. D. Sasmita, "Optimization of a Deep Learning-Based Model for Detecting DDoS Attacks in Cloud Computing," *Nanotechnol Percept*, vol. 20, no. S4, May 2024, doi: 10.62441/nano-ntp.v20iS4.19.
[48] A. Abdullah and M. A. Bouke, "Towards Image-Based Network Traffic Pattern Detection for DDoS Attacks in Cloud Computing Environments: A Comparative Study," in *Proceedings of the 14th International Conference on Cloud Computing and Services Science*, SCITEPRESS - Science and Technology Publications, 2024, pp. 287–294. doi: 10.5220/0012725600003711.
[49] Y. Sanjalawe and T. Althobaiti, "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning," *Computers, Materials & Continua*, vol. 75, no. 2, pp. 3571–3588, 2023, doi: 10.32604/cmc.2023.037386.
[50] R. Bingu and S. Jothilakshmi, "Design of Intrusion Detection System using Ensemble Learning Technique in Cloud Computing Environment," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, 2023, doi: 10.14569/IJACSA.2023.0140580.
[51] K. K. Paidipati, C. Kurangi, J. Uthayakumar, S. Padmanayaki, D. Pradeepa, and S. Nithinsha, "Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud based software defined networks," *Multimed Tools Appl*, vol. 83, no. 11, pp. 32367–32385, Sep. 2023, doi: 10.1007/s11042-023-16894-6.
[52] E. S. G.S.R., R. Ganeshan, I. D. J. Jingle, and J. P. Ananth, "FACVO-DNFN: Deep learning-based feature fusion and Distributed Denial of Service attack detection in cloud computing," *Knowl Based Syst*, vol. 261, p. 110132, Feb. 2023, doi: 10.1016/j.knosys.2022.110132.

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024

[53] S. Balasubramaniam *et al.*, "Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing," *International Journal of Intelligent Systems*, vol. 2023, pp. 1–16, Feb. 2023, doi: 10.1155/2023/2039217.

[54] R. A. Karthika, P. Sriramya, and A. Rohini, "Detection and Classification of DDoS Attacks in Cloud Data Using Hybrid LSTM and RNN for Feature Selection," in *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, IEEE, Aug. 2023, pp. 1491–1495. doi: 10.1109/ICCPCT58313.2023.10244979.

[55] H. Aydın, Z. Orman, and M. A. Aydın, "A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment," *Comput Secur*, vol. 118, p. 102725, Jul. 2022, doi: 10.1016/j.cose.2022.102725.

[56] D. Srilatha and N. Thillaiarasu, "DDoSNet: A Deep Learning Model for detecting Network Attacks in Cloud Computing," in *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, IEEE, Sep. 2022, pp. 576–581. doi: 10.1109/ICIRCA54612.2022.9985524.

[57] G. Kiruthiga, P. Saraswathi, S. Rajkumar, S. Suresh, B. Dhiyanesh, and R. Radha, "Effective DDoS Attack Detection using Deep Generative Radial Neural Network in the Cloud Environment," in *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2022, pp. 675–681. doi: 10.1109/ICCES54183.2022.9835916.

[58] A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application," *Wirel Pers Commun*, vol. 127, no. 1, pp. 419–439, Nov. 2022, doi: 10.1007/s11277-021-08271-z.

[59] B. B. Gupta, A. Gaurav, and D. Perakovic, "A Big Data and Deep Learning based Approach for DDoS Detection in Cloud Computing Environment," in *2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)*, IEEE, Oct. 2021, pp. 287–290. doi: 10.1109/GCCE53005.2021.9622091.

[60] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud," *IEEE Access*, vol. 8, pp. 181916–181929, 2020, doi: 10.1109/ACCESS.2020.3028690.

[61] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1634–1646, Jul. 2022, doi: 10.1109/TCC.2020.3001017.

[62] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, IEEE, Oct. 2019, pp. 1–8. doi: 10.1109/CCST.2019.8888419.

[63] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[64] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.

[65] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.

[66] Canadian Institute for Cybersecurity, "CSE-CIC-IDS2018 on AWS: A collaborative project between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC)." Accessed: Mar. 23, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html

[67] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.

[68] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," in *European Conference on Information Warfare and Security, ECCWS*, 2017, pp. 361–369.

[69] S. HETTICH, "The UCI KDD Archive," *http://kdd.ics.uci.edu*, 1999, Accessed: Aug. 11, 2024. [Online]. Available: https://cir.nii.ac.jp/crid/1572543025502459520.bib?lang=en

[70] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput Secur*, vol. 31, no. 3, pp. 357–374, May 2012, doi: 10.1016/j.cose.2011.12.012.

[71] "Traffic Data from Kyoto University's Honeypots." Accessed: Jul. 10, 2024. [Online]. Available: https://www.takakura.com/Kyoto_data/

DOI: https://doi.org/10.54216/FPA.170207
Received: January 22, 2024 Revised: April 15, 2024 Accepted: September 19, 2024