IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 March 2024, accepted 13 April 2024, date of publication 18 April 2024, date of current version 26 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3390844

SURVEY

Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques–Recent Research Advancements

AMIRA MAHAMAT ABDALLAH[1], AYSHA SAIF RASHED OBAID ALKAABI[1], GHAYA BARK NASSER DOUMAN ALAMERI[1], SAIDA HAFSA RAFIQUE[1], NURA SHIFA MUSA[1,2], AND THANGAVEL MURUGAN[1], (Senior Member, IEEE)

[1]College of Information Technology, United Arab Emirates University, Al Ain, Abu Dhabi, United Arab Emirates
[2]College of Engineering, Al Ain University, Al Ain, Abu Dhabi, United Arab Emirates

Corresponding author: Thangavel Murugan (thangavelm@uaeu.ac.ae)

This work was supported in part by United Arab Emirates University through the Research Start-Up Proposal under Grant G00004612/12T048.

ABSTRACT In the rapidly evolving landscape of computing and networking, the concepts of cloud networks have gained significant prominence. Although the cloud network offers on-demand access to shared resources, anomalies pose potential risks to the integrity and security of cloud networks. However, protecting the cloud network against anomalies remains a challenge. Unlike traditional detection techniques, machine learning (ML) and deep learning (DL) offer new and adaptable methods for detecting anomalies in cloud networks. The objective of this study is to comprehensively explore existing ML /DL methods for detecting different anomalies based on distributed denial of service anomaly (DDoS) and intrusion detection systems (IDS) in cloud networks. The study seeks to address the gaps in anomaly detection for cloud networks, proposing potential solutions for anomaly detection in these cloud environments. The ultimate goal is to contribute valuable insights and practical solutions to enhance the security and reliability of cloud networks through effective anomaly detection by ML/ DL techniques. Methodologies for ML/DL are explained, along with their advantages, disadvantages, and respective approaches. In addition, a summary of the comparison between different ML/ DL models is also included.

INDEX TERMS Cloud network, cloud computing, could, machine learning (ML), deep learning (DL), distributed denial of service (DDoS), intrusion detection system (IDS), anomaly detection, security.

I. INTRODUCTION

Within the expansive field of computing, a cloud network represents an intricate and advanced distributed infrastructure that capitalizes on the functionalities of remote servers and interconnected networks for the storage, management, and processing of data facilitated by internet connectivity. Departing from the traditional dependence on local servers or personal devices for computational functions, cloud networks tap into the extensive resources made available through a complex network of interlinked servers housed in strategically positioned data centers. This paradigm shift in computing architecture signifies a departure from localized, hardware-dependent operations to a globally interconnected, resource-abundant model that has become synonymous with the modern technological landscape. Cloud computing comprises three layers, a system layer, a platform layer, and an application layer. The initial two layers focus on virtual machines (VMs) and operating systems [1], [2]. On the other hand, the third layer deals with cloud-hosted applications, such as web-based applications. This highlights the benefits and widespread adoption of cloud computing [3]. Although cloud networks include several security measures, their security should not be underestimated. The cloud network, like many new technologies, is constantly under attack from adversaries who are always coming up with new ways to get

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Tang.

access to end users' devices and data [4]. However, with the benefits and wide popularity of cloud services, current studies have highlighted the issues and concerns related to security and service delivery caused by cloud services. Cloud incidents such as failures, losing data, and privacy violations have the potential to cost businesses billions of dollars, particularly those who use these services to store important company data and applications. Several examples illustrate this principle. For instance, on February 28th, 2017, an Amazon S3 service disruption in Northern Virginia affected AWS services, incurring significant costs due unauthorized removal of servers due to a command error, impacting a wide range of customers and end users utilizing those services and leading to service disruption and potential data access concerns within the affected Amazon S3 subsystems [5]. Furthermore, On March 5th, 2024, thousands of individuals reported experiencing spontaneous logouts from Meta Facebook and Instagram platforms, therefore, there was a widespread outage in the global meta-network that appeared to disrupt the entire company infrastructure, rendering users their accounts inaccessible, and they were unable to regain access. However, there was also inevitable speculation that Meta may have been experiencing a cyber-attack [6]. Therefore, the most significant challenge that cloud service providers face is controlling the occurrence of cloud-related incidents and threats to provide consumers with a dependable and high-quality service. However, numerous studies on anomaly detection have employed ML /DL to identify anomalies.

Ji et al. [7] tackled challenges in anomaly detection in multivariate time series data, focusing on high dimensionality, noise, and asynchronous anomalies. They aimed to develop an efficient space-embedding strategy for anomaly detection (SES-AD) in multivariate time series, capable of accurately identifying abrupt changes without relying on specific signal distributions. SES-AD utilized a space-embedding strategy to project data for dissimilarity calculation, enabling precise localization of changes. Experimental results showed SES-AD high accuracy on public datasets, outperforming existing models and demonstrating its effectiveness in real-time anomaly detection.

Hu et al. [8] identified limitations in current anomaly detection techniques for multivariate time series (MTS) data, such as lack of continuous learning ability and long learning times for high-dimensional datasets. They aimed to develop a novel computational framework, based on local recurrence rate-based discord search (LRRDS) to detect anomalies within MTS data. LRRDS involved generating recurrence plots, segmenting raw MTS for accurate discord subsequence identification, and evaluating the approach on various datasets.

Iqbal and Amin [9] focused on addressing challenges in anomaly detection and time series forecasting using DL models. Their objectives include improving accuracy in anomaly detection, enhancing time series forecasting, and exploring preprocessing techniques' impact on model performance. Their proposed system involves anomaly detection using various deep learning techniques like long short-term memory (LSTM), LSTM-autoencoder, ensembled models, generative adversarial network (GAN), and transformer architectures.

Also, He et al. [10] presented a topology-aware multivariate time series anomaly detector (TopoMAD), a deep learning method that detects anomalies in cloud systems without supervision. Their aims included integrating system topology, employing graph neural networks (GNN) and long short-term memory (LSTM) networks, and deploying a stochastic seq2seq model. Results show significant improvements in accuracy and precision, highlighting the effectiveness of DL in handling complex data.

However, the use of DL/ ML approaches in anomaly detection in cloud systems brings both potential and challenges, as described in [11]. One of the most significant issues is the inherent complexity and variety of cloud data, which includes various sources such as network traffic, system logs, and user behavior. This heterogeneity complicates feature extraction and model training since the data may contain non-linear patterns and minor anomalies that are difficult to detect. Furthermore, the dynamic nature of cloud systems, which includes rapid scaling, resource allocation, and workload changes, complicates the task of maintaining model resilience and adaptation over time. Also, the scalability and processing requirements associated with DL/ML methods. Moreover, ensuring the privacy and security of sensitive data used for training DL/ML models in multi-tenant cloud environments remains a paramount concern, necessitating robust encryption, access controls, and privacy-preserving techniques to mitigate the risk of data breaches and adversarial attacks. Addressing these challenges requires interdisciplinary efforts to develop scalable, resource-efficient, and privacy-aware methods. DL/ML algorithms tailored to the unique characteristics of cloud environments, while also fostering collaboration between academia, industry, and regulatory bodies to establish best practices and standards for secure and effective anomaly detection in the cloud.

This paper provides a literature overview of ML/ DL models for cloud-based anomaly detection. The article describes ML/DL methods and their applications in detecting cloud network anomalies. It focuses on relevant studies concerning the utilization of ML /DL for detecting Distributed denial of service (DDoS) attacks and Intrusion detection systems (IDS).

Our investigation focused on publications meeting standard criteria, employing "Cloud Networks," "Cloud computing," "Could," "Machine learning (ML)," "Deep learning (DL)," "Distributed denial of service (DDoS)," "Intrusion detection system (IDS)," "Anomaly detection," and "Security" as keywords. Particularly, we find value in the latest cutting-edge papers, as they address trending methodologies. This paper acts as an in-depth academic resource designed for those interested in exploring anomaly detection in cloud environments within the realms of ML/ DL. Therefore, significant importance is given to providing detailed explanations of the ML/DL methods, discussing the advantages and

disadvantages of different proposed systems, and pinpointing opportunities for future research and development. The effectiveness of these systems in identifying and addressing DDoS attacks and IDS, emphasizes the need for enhancing detection and mitigation methodologies for anomalies in cloud networks. However, modern strategies for detecting anomalies in cloud networks commonly involve utilizing state-of-the-art technologies and following the best cloud-based anomaly detection methods.

The contributions of this review are: (i) a Detailed review and discussion of ML/ DL techniques in DDoS detection and IDS anomaly based are introduced, (ii) Various cloud network scenarios employing ML / DL for DDoS attack detection and IDS are analyzed, (iii) Review of cloud network dataset used to detect anomalies in a cloud network, (iv) Characteristics and advantages of each ML/DL model in anomaly detection are summarized, (v) Research gap also discussed, and (vi) Scope of improvements for future research also addressed.

The rest of this review is structured as follows: Section III focuses on security issues in cloud networks. Section IV introduces cloud network-based anomaly detection. Section V describes the data set source. Sections VI and VII described the methods and related papers for ML and DL in DDoS detection and IDS anomaly based. Section VIII discusses the research gap. Section IX introduced the scope of improvement. Section X presents conclusions.

II. RESEARCH METHODOLOGY

This study uses a literature review to identify papers relevant to the research topic or to address specific research focused on cloud anomalies, with a main focus on DDoS attack detection and IDS anomaly-based techniques. In this literature review, we used the most appropriate and reliable way to document and assess existing research studies. The literature review technique enables researchers to review both the advantages and disadvantages of previous research studies, conduct a thorough study to identify prospective research gaps as well as future trends and difficulties, and provide an excellent structure and starting point in establishing a new research topic. The overall process for selecting papers, following the creation of search strings, is depicted in Fig.1.

We conducted a rigorous and systematic literature review encompassing various reputable digital databases, including IEEE Xplore, Springer, Elsevier, Wiley, Taylor and Frances, MDPI, and Hindawi chosen for their proven track record in delivering the latest and most reliable papers addressing issues in cloud networks and established security solutions.

Spanning from 2020 to 2024, our chronological scope aimed to capture the most recent advancements in the field. Employing a carefully crafted set of search terms such as ''Cloud Network,'' ''Cloud computing,'' ''Could,'' ''Machine learning (ML),'' ''Deep learning (DL),'' ''Distributed denial of service (DDoS),'' ''Intrusion detection system (IDS),'' ''Anomaly detection,'' and ''Security''. We thoroughly investigated major library repositories.

As a result, 2702 articles that could be potentially relevant were identified. Following this, articles published before 2020 (372) were eliminated, leading to a focus on 2330 articles published between 2020 and 2024. To further narrow down the selection, articles not related to Machine Learning or Deep Learning (863) were removed, along with conference papers, books, workshops, and magazines resulting in 702 articles falling within the Artificial Intelligence (AI) domain. Through a review of titles and abstracts, 442 articles were excluded, leaving 260 articles that were confirmed to be published exclusively in peer-reviewed journals. After excluding survey and review articles (82), we also excluded any articles related to SDN, Fog, and Edge environments (114). The final compilation for detailed analysis consisted of 64 articles (refer to Fig.1).

III. SECURITY ISSUES IN CLOUD NETWORKS

The architecture of cloud computing comprises two primary components, the front end, and the back end. The front end serves as the interface through which users interact with the system. Meanwhile, the back end encompasses various cloud service models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Fig.2 illustrates the user types associated with each model, alongside examples of applications utilized within them.

A. SOFTWARE-AS-A-SERVICE (SaaS)

This is the first layer of the service model. In this cloud model, providers offer database and software access, but Software-as-a-service (SaaS) faces security challenges, putting responsibility on users. Users must be cautious about shared information and access.

Recent cyber threats highlight the appeal of cloud providers as targets, requiring users to scrutinize provider security [12]. DDoS attacks pose a significant threat to SaaS implementations, impacting both providers and users. SaaS, being a prominent model in cloud computing, attracts attention from malicious actors seeking to disrupt services. With SaaS, the software is centrally hosted and accessed remotely, making it susceptible to DDoS attacks aimed at overwhelming servers and rendering services unavailable to legitimate users. These attacks can disrupt business operations, cause financial losses, and tarnish the reputation of SaaS providers. Implementing robust security measures, including IDS, firewalls, and encryption protocols, is crucial to mitigate the risk of DDoS attacks. Additionally, continuous monitoring and prompt response mechanisms are essential to detect and thwart such attacks effectively, safeguarding the integrity and availability of SaaS platforms for users [13]. Meanwhile, Intrusion detection in SaaS setups is vital for safeguarding both the service provider and its users. SaaS involves multiple users sharing the same application instance, posing unique security challenges. Traditional IDS may not fit SaaS due to limited control over infrastructure. Thus, tailored multi-tenant IDS frameworks are necessary. These

TABLE 1. Summary of the criteria for inclusion and exclusion criteria.

CRITERIA	INCLUSION	EXCLUSION	REASONING
PUBLICATION DATE	2020 and after it	Before 2020	The publication date aligns with the surge in cloud network relevance, emphasizing analysis and security concerns in the scientific literature
SOURCE	Journals articles	Conference, books, workshops, magazines	The exclusion criteria prioritize straightforward, relevant, and reliable research findings over complex discussions or subjective viewpoints that have not passed the same careful review as journal papers
FOCUS	Anomalies in cloud environment	Anomalies in SDN, edge, and fog environments	The emphasis on anomalies in cloud computing in the selected publications guarantees that the research remains focused and relevant to the topic at hand
AVAILABILITY	Authors can access it through open access or other ways.	The content is either shielded or inaccessible	Prioritizing accessible publications, the study ensures thorough examination and accurate representation of source material, enhancing review accountability and encouraging finding replication
LANGUAGE	English	Other than English	This allows for a more precise and efficient analysis, while also minimizing the possibility of misunderstandings or inaccuracies related to language during the review process. Also, most peer-reviewed papers published in the top journals written in the English language
OTHER	-	Duplicate	We only counted a paper's first appearance in multiple sources

frameworks should enable providers to offer IDS as a service, monitoring network traffic and system activities to spot and counter malicious actions in real-time. Effective intrusion detection mechanisms help SaaS providers enhance platform security, shielding sensitive data from unauthorized access [14].

B. PLATFORM-AS-A-SERVICE (PaaS)

This second layer of the service model [12] Platform as a Service (PaaS) offers a computing platform that includes basic resources like operating systems, programming languages, databases, and web servers. These resources automatically adapt to handle changes in application demands. In this setup, developers use specific Application interfaces (APIs) to build applications meant for a particular environment. PaaS also allows control over software deployment and configuration settings [15]. However, Habib et al. [16] implemented a DDoS detection system for PaaS and Infrastructure-as-a-service (IaaS) cloud architectures employing a pretrained hybrid ML classifier incorporating models such as Random Forest, Decision Tree, Support Vector Machine, and XGBoost.

C. INFRASTRUCTURE-AS-A-SERVICE (IaaS)

Infrastructure as a Service (IaaS) is a cloud computing model that allows customers to utilize virtualized computing resources such as virtual machines, storage, and networking via the Internet. This service enables organizations to rent IT infrastructure on a flexible pay-as-you-go basis, facilitating resource scaling based on their needs without the necessity of investing in or handling physical hardware [17]. IaaS, one of the three cloud service models, is highly susceptible to DDoS attacks. The shared nature of these cloud resources makes them a prime target for DDoS attacks, which seek to overwhelm the infrastructure and render it inaccessible to legitimate users. DDoS attacks are defended against using a variety of processes and countermeasures, such as intrusion prevention, intrusion detection, and intruder response [18]. Because of the security risks connected to IaaS in cloud computing, there is a significant need to install IDS to address these issues. There is also a need for strong security measures to secure cloud-based infrastructure services, and IaaS-focused IDS is recognized as important [19].

IV. CLOUD NETWORKS BASED ANOMALY DETECTION

Anomalies in a cloud network signify deviations from expected patterns, behaviors, and occurrences, potentially indicating security threats, operational irregularities, or performance issues. Categorized into types such as security, network traffic, resource utilization, application behavior, data, and user behavior anomalies, they encompass unauthorized access, unusual data transmission, and abnormal resource use. Recognizing and addressing these anomalies is crucial for preserving the cloud network's integrity, security, and reliability, safeguarding against cyber threats, and ensuring optimal performance. In the realm of research, diverse anomalies have been recognized, presenting formidable obstacles to the security infrastructure of cloud networks Include the following:

A. DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

Distributed Denial of Service (DDoS) attack is a type of cyber-attack in which multiple systems or devices are used

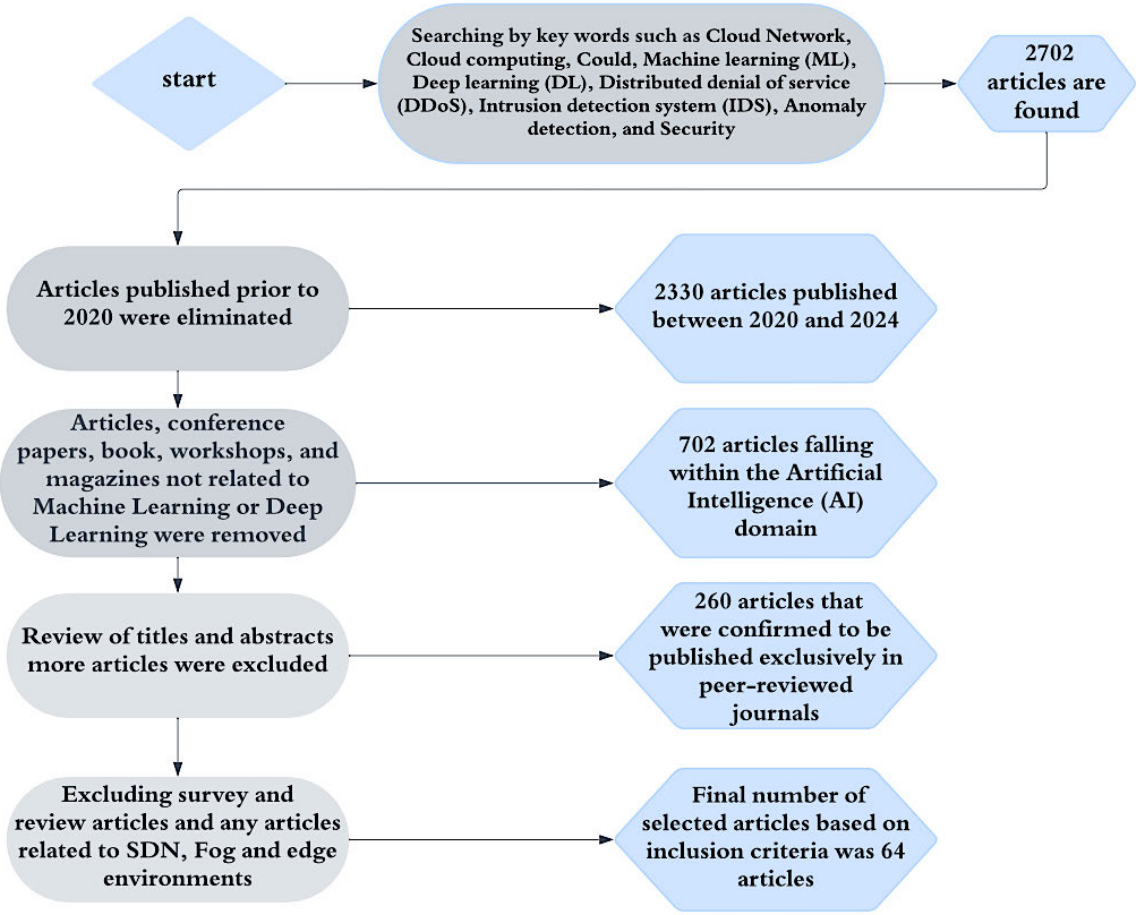

FIGURE 1. Paper selection process.

to flood a targeted server or network with traffic, making it unavailable to legitimate users [20].

In cloud computing, DDoS attacks can cause significant damage to cloud service providers and their customers, leading to downtime, loss of revenue, and reputational damage. Therefore, it is important to have effective detection and prevention mechanisms in place to mitigate the impact of DDoS attacks in cloud computing environments. DDoS types of attacks according to the exploited vulnerability might be categorized as flooding attacks, protocol exploit attacks, amplification attacks, and malformed packet attacks [21]. According to Fig. 3, the number of DDoS attacks is predicted to more than double, reaching 15.4 million by 2023, as reported by Cisco in 2020 [22]. However, to enhance DDoS attack detection and prevention researchers have used ML/ Dl methods, which will be discussed in Section VI.

B. ANOMALY-BASED INTRUSION DETECTION SYSTEMS (IDS)

Intrusions encompass a sequence of interconnected malicious activities executed by internal or external attackers, aiming to compromise the targeted system [23]. Moreover, Intrusion detection is the process of monitoring computer systems and network traffic and analyzing activity to detect potential system threats [24]. In recent times, IDS have become integral components of many organizations' security frameworks, owing to the increased frequency and severity of network attacks. Detecting a security breach involves monitoring and analyzing the target machine or network for indications of unauthorized access. Such breaches are defined as attempts to compromise the confidentiality, integrity, or availability of a computer system or network, or to bypass its security measures [25]. However, the most common intrusion detection approaches are signature-based and anomaly-based. They are often used together, whether integrated or individually, to enhance detection accuracy. In terms of anomaly-based detection different types of anomaly detection techniques are categorized based on the method employed to identify anomalies, such as ML/ DL, fuzzy logic, support vector machine (SVM), and data mining. Over the past decade, numerous studies have investigated these methods, as evidenced in Section VII. As will be explained further in this survey.

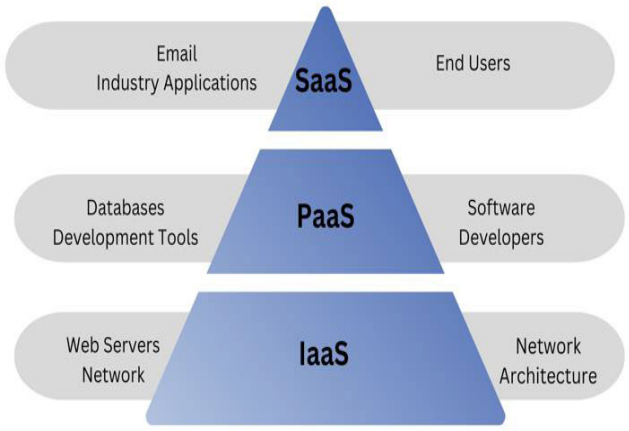

FIGURE 2. Cloud service models.

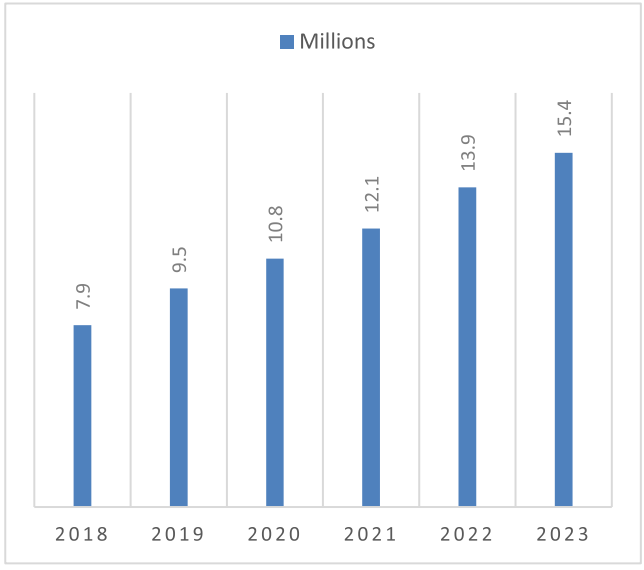

FIGURE 3. DDoS total attacks history and predictions.

V. SOURCE OF DATASETS

In this section, we explain and categorize the datasets utilized in the reviewed literature based on the cloud network traffic data. The frequency of use of datasets in the reviewed literature is shown in Fig. 4. Therefore, the careful selection of a dataset is crucial to ensuring efficient detection and classification of anomalies in cloud environments. However, in cloud computing security, different datasets are utilized to train ML /DL models. Table 2 presents a description of the most used datasets in cloud computing security used in this review.

VI. ML AND DL BASED FOR DDoS DETECTION IN CLOUD NETWORKS

Due to the time-consuming nature of developing, testing, and deploying cloud-based anomaly detection systems after each unexpected attack, there is an urgent need for less human-dependent solutions in anomaly detection. Cloud-based anomaly detection utilizing ML technology addresses this issue by providing a system capable of learning from data and detecting anomalies based on the learned patterns [35]. On the other hand, DL is a sophisticated subset of ML that consists of numerous layers of neurons that reflect the learning process. DL is capable of handling vast amounts of data and has shown effectiveness in a variety of fields [36]. This section will cover the most common use of ML/ DL techniques, followed by a detailed description of each approach used in DDoS detection along with recent relevant publications. Tables 3 and 4 provide a detailed overview of different ML/ DL methods and advantages to detect and mitigate DDoS in cloud environments. Fig. 5 showcases the comprehensive structure of an anomaly detection system based on ML/ DL.

A. DDoS ANOMALY BASED ON ML–EXISTING RESEARCH WORKS

Kushwah et al. [37] focused on the essential difficulty of detecting DDoS attacks in cloud computing, emphasizing the importance of increased security and reliability in cloud-based applications. Their research offered a novel system based on the Voting Extreme Learning Machine (V-ELM) algorithm, to overcome limitations in existing DDoS detection systems in terms of accuracy, speed, and work handling ease. Impressively, the system outperforms a variety of recognized systems. Experimental evaluation demonstrated high detection accuracy, sensitivity, specificity, and minimal training time, further emphasizing the effectiveness of the proposed approach.

Sambangi et al [38] employed ML techniques for detecting DDoS attacks in cloud computing environments. They addressed the challenges associated with DDoS detection in these environments, emphasizing the need for efficient and accurate detection mechanisms to tackle security threats in network infrastructure. The research aims to design an ML model based on multiple linear regression analysis for DDoS attack detection, utilizing data visualization and feature selection techniques to enhance prediction accuracy. Results from experiments include performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix, showcasing promising outcomes with the proposed multiple linear regression analysis approach compared to existing methods.

Abubakar et al. [39] focused on the escalating frequency and diversity of attacks on computer networks, predominantly DDoS attacks, which presented a significant challenge due to their evolving nature and mechanisms. Solutions proposed aimed at developing a mechanism capable of promptly detecting DDoS attacks, identifying their origin, and initiating mitigation procedures at the early stages of detection. This approach integrated an optimized Support Vector Machine (SVM) classification algorithm with the SNORT Intrusion Prevention System (IPS) to provide

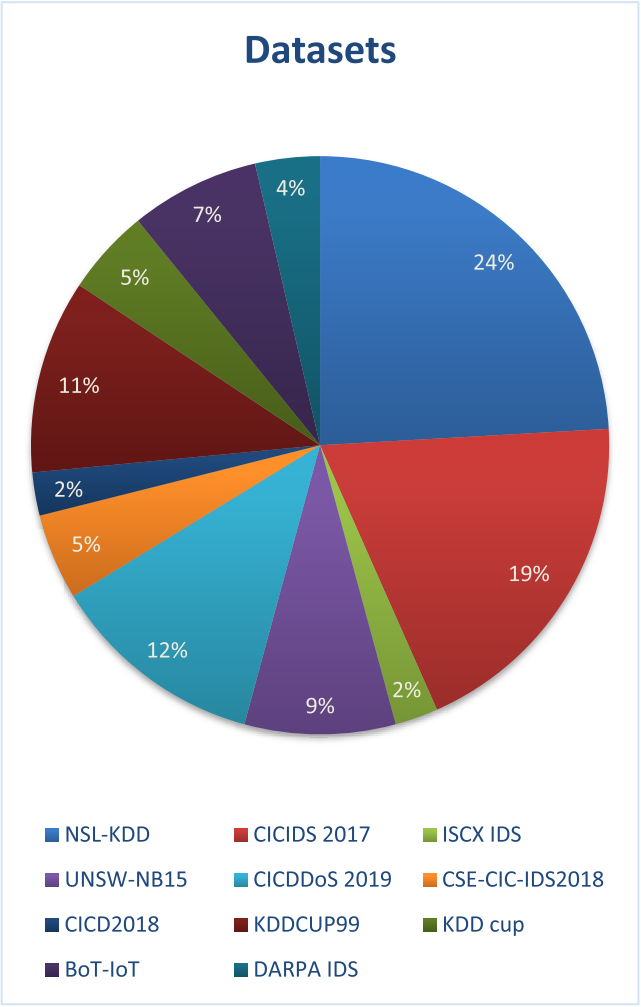

FIGURE 4. Frequency – usage of datasets collected research articles.

preventive measures during DDoS attacks. Experimental results included evaluating the proposed IPS method in both single and multiple-source attack scenarios and comparing performance metrics such as CPU load, latency, average packets, accuracy, detection rate, specificity, and false positive rate. These experiments demonstrated the effectiveness of the proposed method in detecting and mitigating DDoS attacks when compared to existing solutions.

The research [40] addressed various issues concerning cloud computing, particularly the vulnerability to DDoS attacks which could disrupt access to information. It emphasized the necessity for a reliable intrusion detection system to promptly identify and counter such attacks in cloud platforms. The proposed solutions involved creating a classification model utilizing Random Harmony Search optimization (RHS) and Restricted Boltzmann Machines (RBM) to improve DDoS attack detection in cloud setups. The outcomes of the study revealed enhanced accuracy in detecting DDoS attacks compared to conventional methods, along with improved precision, recall, and F1-score metrics. Additionally, the approach led to reduced false positives and increased efficiency in the real-time identification of DDoS attacks in cloud environments.

Alshammari et al. [41] research tackled two main issues, first, identifying abnormal patterns in network traffic data to distinguish between malicious and normal behavior; and second, developing an ML model capable of training IDS to recognize different types of anomalies such as DDoS in cloud computing networks. The solutions proposed in the research included building a comprehensive model that combines various ML techniques such as g K-nearest Neighbor (KNN), Support Vector Machine (SVM), Random Forest (RF), Naive Bayes (NB), Decision Tree (DTREE), and Artificial Neural Network (ANN) to select the most accurate classifier and employing supervised machine learning methods. The results demonstrated the effectiveness of the model in detecting malicious traffic patterns and improving overall network security.

The research [42] focused on detecting DDoS attacks in cloud computing environments using an optimized extreme learning machine. It aimed to address the challenges of developing an effective system for DDoS detection in cloud computing while enhancing accuracy and efficiency. The proposed solutions include utilizing an optimized extreme learning machine and implementing a Self-adaptive Evolutionary Extreme Learning Machine (SaE-ELM) model to improve detection accuracy. The objectives involve proposing the optimized extreme learning machine and introducing the SaE-ELM model to enhance detection accuracy. The research evaluated the proposed system performance using metrics like accuracy, sensitivity, specificity, precision, and F-score, demonstrating significant improvements over existing methods in detecting DDoS attacks in cloud computing environments.

Sachdeva et al. [43] research addressed the classification of attacks in cloud network environments, employing ML and digital forensics. It addresses challenges in detecting and classifying DDoS attacks in cloud networks amidst the increasing complexity of cyber threats and limitations of existing detection methods. Proposed solutions involve developing a fusion algorithm that combines ML techniques with digital forensics, utilizing evidential artifacts for analysis. Experimental setups involve performance metrics like Kappa Statistic, False Positive Rate (FPR), True Positive Rate (TPR), Root Mean Squared Error (RMSE), Precision, and Recall are considered for validation. Results indicate high accuracy, precision, and True Negative Rate in attack classification, along with improved performance in detecting and classifying attacks in cloud networks, validating the fusion algorithm's effectiveness across multiple performance metrics.

The research [44] focused on detecting DDoS attacks in cloud computing environments using an efficient Support Vector Machine-based discrete elephant herding optimization (SVM-DEHO) classifier. It addressed significant cybersecurity issues posed by DDoS attacks, which rapidly exhaust victim communication and computation resources. Objectives

TABLE 2. Common cloud security datasets.

DATASET	DESCRIPTION
NSL-KDD	A refined version of the KDD Cup 99 dataset to reduce redundancy and enhance data quality for intrusion detection research. comprises samples with 41 features that were trained with 20,000 samples and tested with 5,000 samples [26].
CICIDS 2017	This traffic mix includes both benign and malicious threats, including DoS, DDoS, and brute force attacks, suitable for network intrusion detection systems. The total number of traffic packets in the log file was reported to be 225,746 traffic packets [27].
ISCX IDS 2012	Used for evaluating intrusion detection systems, encompassing various types of attacks like DoS, port scans, and data exfiltration attempts. The dataset includes samples with 18 characteristics and was used for training (19,200 samples) and t (4,800) testing samples[28].
UNSW-NB15	Moustafa et al. [29] produced this dataset at the University of New South Wales. It comprises 49 features and approximately 2.5 million occurrences. Total number of samples is 2,540,044, with a subset of 257,673 samples used for training and testing.
CICDDOS 2019	Designed primarily to identify DDoS assaults in IoT environments. It comprises a variety of DDoS attacks as well as typical IoT traffic. One file from this dataset contains 1,209,961 instances and 84 input features. The class attribute is a binary class label with two classes: benign and DDoS [30].
IOT DOS AND DDOS ATTACK	Includes data on DoS and DDoS attacks in IoT environment.
CSE-CIC-IDS2018	This dataset is constructed based on user behavior using various protocols such as HTTPS, HTTP, SMTP, POP3, IMAP, SSH, and FTP. It contains different classes of network traffic, including benign traffic and various types of network attacks [48].
HTTP CSIC 2010	This dataset was developed at the Information Security Institute of CSIC and contains both normal and anomalous requests. It includes URL templates and features related to HTTP requests. contains 36,000 normal requests, more than 25,000 anomalous requests, and 22 features [48].
CICD2018	Contains traffic data from different days, including normal traffic and various types of attacks, such as DOS, Web-attacks, DDOS, infiltration, Botnet, and Brute force. It includes 80 attributes representing the dataset feature [31].
SLOWLORIS	The new dataset was created from scratch using two Android D2D devices to emulate Slowloris attacks. The dataset contains 83 columns and records for Slowloris DDoS attacks with 55,600 entries. This dataset was specifically created for the D2D communication environment [51].
KDDCUP99	To evaluate intrusion detection systems. It consists of both normal and attacks traffic, including many sorts of attacks [26]
KDD CUP	Standard database for anomaly detection, used to identify nodes under attack in network connections [32]
CICIDS 2017 KNN	Contains 78 features with 225,746 records. The dataset includes attack classes such as Benign and DDoS. It is utilized for training and testing the proposed DDoS detection model in the article [65].
CAIDA "DDOS 2007"	Contains 225,746 instances with 79 attributes, including IP addresses, source ports, protocol types, and destination ports. The dataset undergoes preprocessing steps like normalization, discretization, and feature selection before training and testing the M-DBNN [66].
BOT-IOT	Contains network traffic data with details such as packet sequence ID, time, flags, protocol, source and destination addresses, source and destination ports, packets, bytes, duration, mean, and standard deviation. It is used for assessing DDoS attack detection methods in cloud computing [68].
ISCX-2016-SLOWDOS	Contains information about Slow DoS assaults, which are designed to drain server resources over time, experiments, and evaluation of the proposed asynchronous federated learning model for Low-Rate DDoS Attack Detection [71].
CSE-CIC-IDS2018-AWS	A variation of the CSE-CIC-IDS2018 dataset that focuses on attacks against AWS settings [74].
CIC DOS	Contains data related to DoS attacks from the CIC project [74].
CIDDS-001	Consists of various features such as source and destination IP addresses, port numbers, transport protocols, timestamps, duration, data volume, TCP flags, class labels, attack types, and unique identifiers for attacks [76].
WEB APPLICATION LOGS	Contains web application logs that can be utilized to do security analysis and discover anomalies [33].
KYOTO	Created in real-time by Song et al. at [34] Kyoto University in Japan between 2006 and 2015. It comprises 19,683 MB of network traffic collected from darknet sensors, honeypots, web crawlers, email servers, and other servers. The dataset includes 24 statistical attributes, 14 of which are taken from the KDD Cup99 dataset, while the remaining 10 are modern attributes.
CIC BELL DNS EXF 2021	A significant component in the development of the cloud-IDS. It encompasses 270.8 MB of DNS traffic generated through the exfiltration of various file types of diverse sizes. The dataset includes 42 features extracted from the DNS traffic [90].
MQTT-IOT-IDS2020	Designed for detecting intrusions in IoT environments that use the Message Queuing Telemetry Transport (MQTT) protocol [93].
CSIC-2010	The CSIC project provides data on web application security analysis [97].

involve proposing an SVM-DEHO classifier for DDoS detection, with experimental results demonstrating high accuracy, sensitivity, specificity, precision, and F-measure values. Results illustrate the superiority of the proposed approach

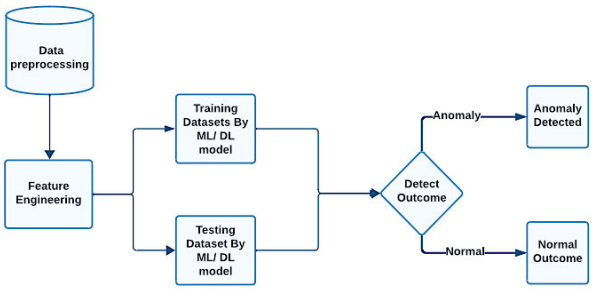

FIGURE 5. ML/ DL- based anomaly detection in cloud network.

over existing methods, affirming its effectiveness in mitigating DDoS attacks in cloud environments.

Mishra et al. [45] research focused on detecting DDoS vulnerability in cloud computing using the Perplexed Bayes Classifier. It addressed challenges in identifying and exploiting vulnerabilities in cloud computing, particularly emphasizing the severity of DDoS attacks and their impact on cloud infrastructure. Solutions involve implementing ML techniques, specifically the Perplexed Bayes Classifier, to detect and mitigate DDoS attacks in cloud environments. Performance metrics such as accuracy, sensitivity, and specificity are used to evaluate the effectiveness of the proposed approach in identifying DDoS attacks. Overall, the results showed that the Perplexed Bayes Classifier can successfully detect and mitigate DDoS vulnerabilities in the cloud environment.

The use of ML in cloud computing to identify DDoS attacks is the subject of research [46]. Reducing misclassification mistakes in DDoS detection is the primary issue, as it impacts the availability of services for authorized users. Reducing misclassification errors, evaluating ML techniques for DDoS attack detection, analyzing misclassifications for more precise measurements, and selecting important features using Mutual Information (MI) and Random Forest Feature Importance (RFFI) approaches are the main objectives of the research. However, the Random Forest method performed the best in terms of detecting DDoS attacks compared to other techniques. F1 score, recall, accuracy, and precision were among the performance metrics.

The study [47] focused on detecting DDoS attacks in modern network infrastructures for Industry 4.0, using ML models and feature transformation methods. It addressed security and data availability issues in modern networking, notably in cloud computing, focusing on the detection of DDoS attacks in cloud networks, which provide new difficulties to the network community. Novel Gaussian-based traffic attribute-pattern similarity functions for evolution feature clustering, as well as Gaussian-based network traffic similarity functions for evaluating similarities between network traffic instances, are proposed as solutions. Furthermore, the study creates the SWASTHIKA machine learning model to detect both low-rate and high-rate network threats. Experimental results show that SWASTHIKA has much higher attack detection rates than state-of-the-art ML classifiers, as measured by performance measures such as accuracy, precision, detection rate, and F-score.

The study [48] addressed cloud security in E-government, including the detection and mitigation of network intrusion, specifically DDoS attacks. It focused on critical security challenges in cloud computing, concentrating on the vulnerable nature of cloud-based E-government systems to attacks from nodes that are compromised and the significance of monitoring internal as well as external traffic in the cloud network for security purposes. The proposed solutions include introducing an ML method for accurate clustering of network data to detect DDoS attacks, utilizing feature selection techniques to improve data clustering efficiency, and using clustering algorithms such as Principal Component Analysis (PCA), Density-Based Spatial Clustering of Applications with Noise DBSCAN, Agglomerative Clustering, and k-means. The experimental results show that the proposed PCA + DBSCAN outperforms standard algorithms.

Sokkalingam et al. [49] research addressed the escalating frequency and complexity of DDoS attacks aimed at cloud computing services and the inadequacies of traditional intrusion detection systems in effectively identifying and addressing these attacks. To tackle these challenges, the study proposed solutions such as developing an intelligent intrusion detection system that utilized ML techniques to enhance DDoS attack detection and employing a Support Vector Machine (SVM) with hybrid Harris Hawks Optimization (HHO) and Particle Swarm Optimization (PSO) algorithm approach to improve accuracy and efficiency in cloud environments. The experimental evaluation utilized performance metrics including precision, sensitivity, selectivity, F1 score, accuracy, and Area Under the Curve (AUC) to evaluate the effectiveness of the proposed system, revealing enhanced detection capabilities and efficiency in countering DDoS attacks within cloud computing environments.

The study [50] aimed to enhance the efficacy of the Gaussian Naïve Bayes classifier to detect DDOS attacks in cloud computing. It discussed the prevalence of DDOS and DOS attacks against cloud services, as well as the difficulty in detecting these attacks due to their distributed character and potential for catastrophic consequences. Proposed solutions for detecting DDOS attacks include using ML techniques, especially the Gaussian Naïve Bayes classifier, pre-processing data to address zero-probability issues, and selecting highly independent features to improve accuracy. The proposed framework improves the accuracy of the Gaussian Naïve Bayes classifier in detecting DDOS attacks, mitigates the zero-probability problem through data pre-processing, improves feature selection efficiency, and measures classifier performance using precision, recall, and F1-score.

The study [51] employed ML to detect DDoS attacks in device-to-device (D2D) connections. Solutions include using ML techniques such as Random Forest, XG Boost,

Ada Boost, and Light Gradient Boosting Machine (LGBM) to detect and prevent DDoS attacks in D2D communication systems. The objectives include providing considerable improvement in terms of detection and prevention time, needed resources, and device battery usage, as well as presenting a useful technique for combating DDoS attacks in D2D communication. The proposed system used ML techniques to classify and detect DDoS attacks, with an emphasis on SYN and Slowloris attacks. The research employed evaluation metrics such as accuracy, precision, recall, Area Under the Curve (AUC), and F1 score to evaluate the performance of ML classification approaches in detecting DDoS attacks within the D2D network communication environment. The results demonstrated significant performance improvements and provided comprehensive evaluations of ML models, contributing to the effectiveness of DDoS attack detection methodologies in real-world scenarios.

Authors in [52] focused on protecting virtual cloud computing environments from DDOS attacks using the Naive Bayes ML algorithm. They tackled challenges stemming from the growing number of users accessing cloud-based applications, which has led to an increase in DDOS attacks targeting cloud services. Additionally, there is a lack of reliable methods for detecting and filtering these attacks, making them a preferred weapon for cyber attackers. To address these issues, the research explores ML techniques and specifically applies the Naive Bayes algorithm to prevent and detect DDOS attacks in virtual cloud environments. Remarkably, the Naive Bayes model showed improved accuracy, recall, specificity, and F-score.

Researchers in [53] focused on using ML to detect DDoS attacks in Vehicular ad-hoc Network (VANE)T cloud environments, aimed to address the challenges of identifying and mitigating such attacks in vehicular networks. They proposed solutions such as employing ML models like Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors (KNN), Naive Bayes (NB), and kernel Support Vector Machine (SVM) to classify ''Normal'' and ''DDoS'' scenarios and implementing fuzzification to categorize correlation degrees in attribute value ranges. Objectives include improving security and safety in vehicular networks by detecting DDoS attacks, using a structured methodology comprising NS2 simulation and ML-driven detection phases. Performance metrics such as accuracy score and precision score are calculated for various classification algorithms, demonstrating the successful application of ML especially DT and RF in addition to fuzzification techniques in enhancing DDoS detection capabilities in VANET cloud environments.

AlSaleh et al. [54] research focused on the use of ML to detect DDoS threats in cloud computing settings. It discussed the cybersecurity threats associated with cloud technology implementation, including DDoS attacks, and emphasized the limits of standard IDS in detecting DDoS attacks in dynamic network environments. The study sought to answer questions about the effectiveness of the proposed Bayesian-based Convolutional Neural Network (BaysCNN) model in detecting DDoS attacks, the extent to which the Data Fusion BaysFusCNN approach improves DDoS detection accuracy, reliability, and performance metrics, and how the proposed models compare to existing methods in terms of accuracy and efficiency. The results demonstrated that the BaysCNN model obtains an average accuracy rate of 99.66% across 13 multi-class attacks, while the Data Fusion BaysFusCNN model gets an even higher average accuracy of 99.79%. The study offered useful insights into the development of robust ML-based intrusion detection systems, as well as improving the reliability and scalability of IDS in cloud computing environments.

Talpur et al. [55] investigated the application of ML and evolutionary algorithms to DDoS attacks in cloud computing systems. The study showed that modern society is becoming increasingly vulnerable to cyberattacks, particularly DDoS attacks, and emphasizes the need for greater detection and cybersecurity measures. The system detected DDoS attacks using TOPT with the genetic algorithm GA. Also, ML methods such as Extreme Gradient Boosting (XGB), Random Forest (RF), and Support Vector Machine (SVM) propose XGB-GA Optimization, RF-GA Optimization, and SVM-GA Optimization methods considered. The technology reached high accuracy levels, considerably boosting cybersecurity measures. The suggested XGB-GA optimization approach outperformed other methods for identifying DDoS attacks in terms of accuracy, precision, recall, and F1 score. Achieving a 99.00% testing accuracy and a best pipeline test accuracy of 1.000%.

The research [56] focused on detecting and categorizing DDoS attacks in distributed networks using hierarchical ML and hyperparameter optimization methods. It tackled the growing threat of DDoS attacks in distributed networks and the challenge of swiftly identifying and preventing them to protect network infrastructure and data. Solutions include employing hierarchical ML models such as Extreme Gradient Boosting (XGBoost), Light Gradient Boosting Machine (LGBM), CatBoost, Random Forest (RF), and Decision Tree (DT) for better attack classification and optimizing hyperparameters to improve intrusion detection system accuracy and efficiency. The objectives involve proposing a LASSO feature selection method with hierarchical ML models, dividing the process into pre-processing, feature selection, and hyperparameter-optimized tuning classification stages, and evaluating performance using metrics like recall, precision, accuracy, and F1-score. The study found the LGBM classifier to be the most effective, achieving 99.77% accuracy, highlighting the success of hierarchical ML techniques in accurately predicting DDoS attacks.

B. DDoS ANOMALY BASED ON DL—EXISTING RESEARCH WORKS

Velliangiri et al. [57] research focused on DDoS attack detection within cloud computing environments, aiming to address

the pressing need for effective detection methods and overcome the limitations of existing algorithms. The objectives involve developing a novel Fuzzy and Taylor Elephant Herd Optimization (FT-EHO) and Deep Belief Network (DBN) classifier specifically designed for DDoS attack detection and comparing its performance against state-of-the-art algorithms like Support Vector Machine (SVM), Neural Network (NN), EHO, and TEHO-based DBN. The proposed system utilizes three databases, including the KDD cup database, to detect DDoS attacks and employs a fuzzy and TEHO-based approach within the FT-EHO Deep Belief Network classifier for classification. Experimental evaluation focused on performance metrics such as accuracy, detection accuracy, precision, and recall. The results showcased the efficacy of the proposed FT-EHO-DBN classifier across varying numbers of users and highlighted its strengths in achieving high accuracy, detection accuracy, precision, and recall, thereby contributing significantly to enhancing DDoS detection in cloud environments.

Bhardwaj et al. [58] focused on enhancing the detection of DDoS attacks in cloud computing environments using a Hyperband Tuned Deep Neural Network coupled with a stacked sparse Autoencoder. This methodology addressed critical challenges such as limited training data, imbalanced datasets, and the complex task of selecting optimal features. While traditional methods and ML approaches struggle with evolving attack vectors and noisy data, the proposed system aims to mitigate these limitations. Experimental validation showcased the system's superior performance compared to existing methods, with notable improvements in accuracy, precision, recall, and F1-Score.

In research [59] Mishra et al. focused on cloud computing, particularly examining, and addressing vulnerabilities to DDoS attacks in cloud environments, alongside concerns such as network errors and intrusions, and load balancing issues. Proposed solutions involve using Neural Networks (NN) to evaluate training performance and detect accurately and employing Swarm optimization to minimize errors and ensure response stability. Results demonstrated reduced network errors, enhanced detection accuracy, and better identification of intrusions, with metrics including mean square error rate, detection accuracy, and precision.

Velliangiri et al. [60] focused on DDoS attacks in cloud computing using optimization-based deep networks. The key problems addressed include detecting DDoS attacks in cloud environments, improving cloud platform security against such attacks, and improving the detection technique's accuracy and efficiency. The solutions consist of creating a Taylor-Elephant Herd Optimization based Deep Belief Network (TEHO-DBN) classifier for DDoS detection, using DL for anomaly detection in clouds, and using an optimization-based strategy to improve detection system performance. A variety of evaluation metrics such as detection rate, accuracy, recall, computational time, and precision are considered when simulating the TEHO-DBN classifier. However, the proposed system demonstrated improved performance metrics compared to existing techniques.

The study [61] focused on detecting DDoS and economic denial of service (EDoS) attacks within cloud computing by combining Deep Belief Network (DBN) and Support Vector Machine (SVM) technologies. It tackled challenges such as accurately recognizing different forms of EDoS and DDoS attacks, preventing attacks from moving between Virtual Machines (VMs) and the hypervisor, and estimating attack percentages while determining sensitivity thresholds based on system requirements. Proposed solutions involve devising a comprehensive method for identifying both EDoS and DDoS attacks, utilizing a global approach to improve threat detection. However, when identifying DDoS and EDoS attacks in cloud computing, some common performance metrics to evaluate such as attack reporting time, request-response time, victim service downtime, defensive cost/hour, True Positive Rate (TPR), True Negative Rate (TNR) and accuracy are considered. The results obtained regarding the fusion of DBN and SVM for detecting DDoS and EDoS attacks in the cloud demonstrate several significant outcomes. These include superior accuracy in identifying DDoS attack traffic, resulting in shorter attack reporting and response times, as well as reduced downtime for victim services. Moreover, the approach leads to lower costs associated with attack detection and mitigation. Notably, the classification accuracy achieved is exceptionally high, reaching 99.78%. Overall, these results highlighted the effectiveness of the proposed method in enhancing the security and resilience of cloud environments against DDoS and EDoS attacks.

Almiani et al [62] investigated network security in containerized cloud computing platforms using a Resilient Back Propagation Neural Network. They aimed to address vulnerabilities such as DDoS attacks on containerized microservices and the need for intelligent intrusion detection in cloud-native environments. The proposed solution involves an IDS based on Neural Networks (NN) to detect and mitigate Reflective DDoS attacks. Objectives include proposing the system, evaluating its performance against DDoS attacks, and ensuring it meets the delay requirements of containerized microservices architectures. Experimental results demonstrate efficient processing times and high accuracy in detecting reflective DDoS attacks, as evaluated using performance metrics including accuracy, sensitivity, F1-score, specificity, precision, and false positive rate.

Akgun et al. [63] focused on developing intrusion detection systems for DDoS attacks. They addressed the escalating frequency and complexity of such attacks, as well as the limitations of traditional detection methods. Existing solutions encompass signature-based and anomaly-based intrusion detection systems, along with ML approaches for identifying unknown malware threats. The research objectives involve proposing a DL-based intrusion detection model, assessing various DL architectures such as Deep Neural Networks (DNN), Convolutional Neural Networks

(CNN), and Long Short-Term Memory (LSTM), benchmarking the proposed models against baseline approaches using the CIC-DDoS2019 dataset. Performance evaluation against baseline models reveals improved accuracy, precision, recall, F1-score, and Area Under Curve (AUC), demonstrating enhanced DDoS attack detection capability. Additionally, security metrics like detection accuracy, false positive rate, and false negative rate are considered.

Aydın et al. [64] aimed to create a Long Short Time Memory (LSTM)-based DDoS detection and defense system in a public cloud setting, emphasizing the urgent need for precise and prompt identification and prevention of DDoS attacks, especially during the COVID-19 era. The goals involve crafting an LSTM-based solution for DDoS detection and defense, incorporating autonomous defense components to counter detected anomalies, and ultimately improving cloud system cybersecurity. The proposed approach utilized network traffic analysis, digital signatures, and autonomous defense strategies to identify and counteract DDoS attacks. The system demonstrated notable accuracy in classifying attacks, competitive performance in training and testing durations compared to prior studies, and thorough assessment using vital performance and security metrics like accuracy, precision, recall, F1-score, and the efficacy of defense mechanisms.

Samsu Aliar et al. [65] research focused on detecting DDoS attacks in cloud environments by employing optimized weighted fused features and a hybrid Deep Belief Network with the Gated Recurrent Unit DBN-GRU architecture. It addressed performance degradation resulting from these attacks in cloud computing, along with the challenge of maintaining data security and privacy. Solutions entail developing a DL-based approach for automated detection, utilizing optimized features and the hybrid architecture. The experimental setup involves evaluating performance metrics such as accuracy, sensitivity, specificity, precision, F-1 score, Mathew's correlation coefficient, false positive rate, false negative rate, and false discovery rate.

Agrawal et al. [66] goal was detecting and mitigating DDoS attacks in cyber environments using a Modified Deep Belief Neural Network (M-DBNN) system. The main goal was the protection of user personal information against intrusion or DDoS attacks. Agrawal et al. goals include employing MDBNN to detect adverse behaviors, preprocessing dataset features to improve detection, optimizing the classifier performance with the Chimp optimization algorithm, and comparing the suggested method to existing techniques. Results demonstrated the superior performance of M-DBNN in terms of accuracy, error rate, F1 score, false positive rate, kappa, Matthew correlation coefficient, precision, sensitivity, and specificity values.

Varghese et al. [67] focused on intrusion detection in cloud systems, notably DDoS attacks, addressing the security difficulties faced by such attacks and protecting data in cloud computing. The proposed solutions include the introduction of a novel intrusion detection model based on an optimized Radial Bias Function Neural Network (RBF-NN) with weights tuned optimally Using Harmonic Mean Based Poor and Rich Optimization (HMPRO) algorithm. The results include the superior performance of the RBF-NN + HMPRO approach when considering specificity, False Negative Rate (FNR), sensitivity, precision, False Positive Rate (FPR), Matthew correlation coefficient (MCC), net predictive value (NPV), and accuracy.

Emil Selvan et al. [68] work focused on detecting and preventing DDoS attacks in cloud computing environments, addressing challenges in identifying such attacks within real-world traffic flows while minimizing identification time, reducing computational complexity, and enhancing detection models to handle diverse attack types. Its objectives involve developing a Fractional Anti Corona Virus optimization (FACVO)-based on a Deep Neuro-Fuzzy Network (DNFN) system specifically tailored for DDoS attack detection in the cloud, incorporating feature fusion, data augmentation, and DL techniques to enhance detection accuracy, True Positive Rate (TPR), True Negative Rate (TNR), and precision. The proposed system operated by utilizing log files generated from simulated cloud environments and employing the DNFN trained by FACVO to identify DDoS attacks. Experimental evaluation conducted using the NSL-KDD and BoT-IoT datasets includes comparison with existing techniques, with a focus on testing accuracy, TPR, TNR, and precision metrics, showcasing the efficacy of the developed FACVO-based DNFN system in robustly detecting DDoS attacks in cloud environments.

Balasubramaniam et al. [69] addressed the challenges posed by insider DDoS attacks impacting cloud performance and service availability. Objectives involve developing a Gradient Hybrid Leader Optimization algorithm (GHLBO) for efficient attack detection, incorporating a Deep Maxout Network (DMN) for feature fusion, oversampling for data augmentation, and integrating gradient descent with hybrid leader-based optimization HLBO for enhanced performance. The experimental evaluation compares the GHLBO-based approach with existing methods using metrics like testing accuracy, TPR, and TNR, with results 0.917, 0.909, and 0.909 respectively, indicating improved performance metrics across different datasets.

In [70], Pasha et al. research targeted how to detect low-rate DDoS attacks in cloud computing using the Low-Rate DDoS Attack Detection Framework (LRDADF), integrating AI technologies like DL. It proposes a Hybrid approach for Low-Rate DDoS detection HA-LRDD algorithm, combining deep Convolutional Neural Networks (CNN) and Autoencoders for enhanced accuracy. Existing methods such as attack filtering are discussed, highlighting the need for improved detection mechanisms. Experimental results demonstrated HA-LRDD effectiveness compared to other algorithms in ensuring cloud service quality showing a high detection rate of 95.32% and a low false positivity rate of 0.56943%.

Liu et al. [71] focused on detecting low-rate DDoS attacks using an asynchronous federated learning arbitration model based on Bidirectional Long Short-Term Memory (bi-LSTM) and mechanism of attention. Liu et al. [71] addressed challenges associated with these attacks, emphasizing the necessity for effective detection mechanisms and highlighting limitations in existing models. Objectives entail designing an equal time step sliding window method for data preprocessing, developing a local model based on bi-LSTM and attention mechanism for attack detection, and proposing a leader node election algorithm alongside an asynchronous federated learning framework. Experimental evaluation involves comparing the proposed model with various classifiers and DL models and evaluating performance metrics like accuracy, precision, recall, and time complexity.

The study [72] focused on detecting DDoS attacks within cloud environments using an AI-based IDS framework, with a primary goal of improving accuracy while minimizing false alarms. Proposed solutions involve employing ensemble feature selection to identify key features and constructing a Deep Neural Network (DNN) model for precise DDoS detection. Results indicate the effectiveness of the proposed FEwDN model, demonstrating superior accuracy compared to conventional machine learning techniques and surpassing existing methods in various performance metrics. The research highlighted the efficiency of the AI-based IDS framework with performance evaluation metrics such as accuracy, precision, recall, F1 score, Area Under the Curve (AUC), and Receiver Operating Characteristic (ROC) used for evolution.

The study [73] focused on predicting cyber-attacks such as Brute_Force, DDoS, ICMP Flood, Port_Scan, and Web Crawling in cloud computing environments using an extremely boosted neural network. It aimed to automate the detection and identification of multistage cyber-attack scenarios while enhancing prediction accuracy and efficiency. Proposed solutions involve utilizing the boosted Neural Network (NN) for more precise prediction and implementing advanced ML techniques to improve cybersecurity measures in cloud systems. The system operated by training the neural network on historical attack data, employing sophisticated algorithms for real-time analysis and prediction, and continuously improving through adaptive learning and feedback mechanisms. Monitoring various performance metrics allows assessment of accuracy, sensitivity, specificity, and overall effectiveness. Results demonstrated improved accuracy in predicting multi-stage cyber-attacks, enhanced efficiency in threat detection and mitigation, and validation of the boosted NN effectiveness through experimental simulations and evaluations.

Pandithurai et al. [74] focused on predicting DDoS attacks in a cloud environment using a combination of honey badger optimization algorithm and Bidirectional Long Short-Term Memory (Bi-LSTM) technology. They addressed challenges associated with cloud adoption such as privacy issues and data leakage, highlighting existing detection system limitations. Experiments showcased superior accuracy. Results present various performances including False Positive Rate (FPR), sensitivity, precision, accuracy, specificity, F1 score, error, and Kappa. However, Bi-LSTM obtained 95% sensitivity, 94% precision, 88% kappa, 5% FPR, and 87% F1 score.

Arango-López et al. [75] focused on enhancing real-time detection and prediction of DDoS cyber-attacks using a cloud-based DL architecture. They addressed challenges such as achieving real-time detection, reducing evaluation metrics with standard datasets, and focusing on specific attack categories amidst network noise. Solutions involve analyzing attack categories using tools like Wireshark, applying filters to isolate specific attack types, and developing a cloud-based DL architecture such as Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN). The proposed system continuously inserts new data for each DDoS attack class to improve real-time detection, carefully analyzes each attack category, and focuses on attacks affecting the HTTP protocol port 80. Experimental results demonstrated optimal accuracy metrics achieved by the DNN, considering accuracy, precision, F1 score, and sensitivity as performance metrics.

Ouhssini et al. [76] addressed DDoS attack detection and prevention in cloud environments through the DeepDefend framework, addressing challenges such as resource efficiency and limitations of existing systems. Solutions involve components like traffic collection, entropy forecasting, and attack prediction. Objectives include presenting a strategy for detection and prevention, utilizing entropy forecasting, and improving, Autoencoders, Neural Networks (CNN), and Decision Tree (DT) model. The system processes data through various stages and employs DL methods such as CNNs, Long Short-Term Memory (LSTM) networks, Autoencoders, and transformers for tasks like entropy forecasting and feature extraction. Experimentation with the CICIDS-001 dataset and performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the effectiveness of the DeepDefend framework in detecting and preventing DDoS attacks. The outcomes highlighted the DeepDefend framework's efficacy and precision in detecting and preventing DDoS attacks in cloud environments.

VII. ML AND DL BASED FOR IDS IN CLOUD NETWORKS

Since a signature-based IDS takes considerable time to build, test, and deploy each time an unexpected attack occurs. An anomaly-based IDS based on ML technology offers a system that can learn from data and make predictions about unseen data by applying the learned data [77]. However, Early ML-based intrusion detection techniques were criticized for having limited throughput and high false positive rates. Hodo et al. [78] study on intrusion detection methods found that DL methods such as deep networks outperform typical ML-based detection approaches. A technique is employed to train hierarchical network layers using unsupervised learning in a step-by-step manner, drawing inspiration from the structure of the human brain. Furthermore, ML/ DL algorithms use autonomous learning to predict final outputs. For instance, IDS can employ these algorithms to safeguard cloud networks

TABLE 3. DDoS detection in cloud network using ML.

REFERENCES	PROBLEM	SOLUTIONS	RESULTS	ADVANTAGES	DISADVANTAGES	DATA SOURS	YEAR
[37]	DDoS Detection	V-ELM	Accuracy of 99.18% with the NSL-KDD	Ability to detect both known and unknown attacks	Real-time detection challenges	NSL-KDD	2020
[38]	DDoS Detection	Multiple linear regression analysis	Accuracy of 97.86%	Using visualization	Assumption of Linearity	CICIDS 2017	2020
[39]	Mitigate real-time DDoS	SVM+ SNORT	Accuracy rate of 97% a	Route identification	Packet processing	KDD, CUP99, DAPRA,	2020
[40]	Improve DDoS detection	RHS- RBM	Accuracy of 99.92%	Feature learning	RBMS can be complex models	KDD 99	2021
[41]	Detect malicious network traffic.	RF-NB-DTREE- ANN-SVM- KNN	Highest accuracy of 100%	Encouraging results	Real network challenges	ISOT-CID	2021
[42]	DDoS Detection in the Cloud	SaE-ELM	Highest accuracy of 99.99% with NSL-KDD	The system is evaluated on multiple datasets,	Training time	NSL-KDD, ISCX IDS 2012, UNSW-NB15, and CICIDS 2017.	2021
[43]	Detecting and classifying (DDoS) attacks	ML techniques with digital forensic method	Average accuracy 99.36%	Real-time detection	Adaptability	NSLKDD	2022
[44]	Detection of DDoS	SVM-DEHO	Accuracy of 99.34%	Efficient detection	Real-time detection	NSL-KDD, UNSW-NB15, ISCX ID and CIC-IDS2017	2022
[45]	Detection of DDoS	Perplexed Bayes Classifier	Accuracy of 99%	Efficient feature selection	Optimization challenges	NSL-KDD	2022
[46]	DDoS detection	RFFI + MI	RF accuracy 0.999977	Reduction in Misclassification Errors	Real-time detection	CICIDS 2017 - CICDDoS 2019	2022
[47]	DDoS attack detection	SWASTHIKA +ML model	Accuracy of 90.74	Adoption of the standard dataset	Sensitivity to Parameter Tuning	IoT DoS and DDoS attack dataset from IEEE Dataport	2022
[48]	DDoS in E-government	PCA-DBSCAN-Agglomerative Clustering	High accuracy of 100% for PCA + DBSCAN	Efficient clustering	Dependency on labeled data	CSE-CIC-IDS2018, NSL-KDD, and HTTP CSIC 2010	2022
[49]	DDoS detection	SVM+ HHO-PSO	Accuracy of 97.05%	Hybrid optimization algorithms	K- value needs to increase	NSL-KDD	2022
[50]	DDoS detection	Gaussian Naïve Bayes classifier	Accuracy of 96.15%	Handling zero-probability issue	Sensitivity to feature Independence Assumption	CICD2018	2023
[51]	DDoS detection	RFe, XG Boost, Ada Boost, and (LGBM)	Higher accuracy with Random Forest Between 99.5% and 99.8%	Capability to detect various types of DDoS attacks	Limited dataset coverage	CICDDoS2019 - Slowloris dataset	2023
[52]	Prevention and detection of DDOS	Naive Bayes model	Success rate 99.78 %	Efficacy of ML methodologies in detecting DDoS	Real-time monitoring challenges.	KDDCUP99	2024

TABLE 3. *(Continued.)* **DDoS detection in cloud network using ML.**

[53]	Detecting and mitigating DDoS attacks in VANET cloud settings	LR, DT, RF, KNN, NB, and SVM	Accuracy of 99.59% for DT and RF	Adaptable to real-world systems	Scalability challenges	-	2024
[54]	DDoS Cloud Detection	BaysCNN - BaysFusCNN	Baysfuscnn with the highest accuracy rate of 99.79%	Groundbreaking solution	Real-world Scenarios	CICDDoS2019	2024
[55]	DDoS Detection	XGB-GA, RF-GA, SVM-GA	Best pipeline accuracy of 1.000% with XGB-GA	Enhanced accuracy and efficiency	Challenges in real-world implementation	NSL-KDD	2024
[56]	Detection and classification of DDoS	XGboost, LGBM, CatBoost, RF, and DT	LGBM with the highest accuracy rate of 99.77%	Early threat identification	Scalability issues	CICIDS 2017	2024

from various attacks, such as DDoS attacks. Additionally, a comprehensive explanation of each method employed in IDS will be provided, along with recent related studies in this section. Tables 5 and 6 describe the method and advantages of IDS based on ML/ DL in detail.

A. IDS ANOMALY BASED ON ML - EXISTING RESEARCH WORKS

The study [79] focused on using ML for log-based intrusion detection in cloud web applications, aiming to enhance cloud security. It addressed challenges such as the need for adaptable security systems in the complex cloud environment, the complexity of deploying multiple platform-specific IDS, and the demand for simpler, easier-to-update detection models. The research aimed to introduce a flexible ML approach such as Random Tree, REP tree, J48, bagging, boosting, Random Forest, and Neural Networks for attack detection using web application logs, proposing configurations of ML algorithms with high performance and minimal time overhead. The study demonstrated the effectiveness of ML algorithms like Decision Trees and Neural Networks in detecting attacks on cloud-based applications. The results, measured through, highlight the potential of ML techniques in enhancing intrusion detection for cloud web applications, offering a more adaptable and efficient approach compared to traditional rule-based systems.

Jaber et al. [80] research focused on improving IDS for cloud computing environments, aiming to improve detection accuracy through a hybrid Fuzzy C Means clustering (FCM) algorithm with the Support Vector Machine (SVM) method. The research addressed the pressing need for enhanced detection systems in the face of rising cyber threats in cloud setups. It tackled challenges in effectively identifying and thwarting different attack types like denial-of-service (DoS), Remote to Local (R2L), User to Root (U2R), and normal traffic within cloud networks. Results include various performance metrics such as accuracy, incorrect classification rate, false negative rate, true positive rate, precision, recall, and F1 score across different attack types. The hybrid FCM-SVM system demonstrated impressive accuracy rates and low false negative rates outperforming other IDS methods.

The research [81] focused on enhancing IDS in the cybersecurity domain by addressing the challenges posed by high-dimensional datasets, including computational complexity, time complexity, system learning complexity, resource consumption, and alert delays. The objectives of the study involve introducing a feature selection method based on rough set theory and Bayes theorem to improve IDS performance. The proposed system involves data normalization, feature selection based on estimated probabilities, and classification using Bayesian Rough set methods to achieve a high detection rate and low false alarm rate. Results indicated a reduction in time and space complexity, high detection rates, and low false alarm rates, with statistical parameters from confusion matrices used to evaluate system performance.

The research [82] addressed cybersecurity, specifically focusing on IDS in cloud computing, utilizing ML techniques. It focused on the growing vulnerability of cloud systems to cyberattacks, given their widespread adoption by organizations, banks, and governments, and the pressing need for robust security measures to safeguard sensitive data like healthcare records from unauthorized access. The study proposed an effective IDS leveraging ML algorithms such as Genetic Algorithms (GA) and Support Vector Machines (SVM) to improve security in cloud computing environments. Experiment results showcased high accuracy rates in classifying normal and abnormal traffic across various attack types, highlighting the system's efficacy in reducing false positives and improving detection rates in cloud computing setups.

TABLE 4. DDoS detection in cloud network using DL.

REFERENCES	PROBLEM	SOLUTIONS	RESULTS	ADVANTAGES	DISADVANTAGES	DATA SOURS	YEAR
[57]	DDoS attack detection	novel FT-EHO DBN classifier	accuracy 93.811%	Enhanced performance	Computational cost	KDD cup database, Database 1, and Database 2	2020
[58]	Detection of (DDoS)	DNN using a well-posed stacked sparse AutoEncoder	accuracy > 98%	Effective feature representation	Scalability for real-world deployment	NSL-KDD and CICIDS2017	2020
[59]	DDoS vulnerabilities analysis	NN	High accuracy	Utilization of advanced techniques	Dataset limitation		2020
[60]	DDoS detection	TEHO-DBN	Accuracy rates 0.830	Optimization-based approach for efficient DDoS detection	Limited scalability	KDD cup database, Database 1, and Database 2	2021
[61]	DDoS and EDoS detection	DBN and SVM	High accuracy 99.78%	Reduced downtime	Dependency on dataset	SMD	2021
[62]	DDoS attack detection	NN-based IDS	highest accuracy 97.07%	supports the delays required by containerized cloud computing.	Performance Trade-offs	CICDDoS 2019	2022
[63]	IDS for DDoS	DNN- CNN- LSTM	CNN achieved high accuracy > 99.99%	Enhancing cybersecurity against DDoS attacks	Feature selection	CIC-DDoS2019	2022
[64]	DDoS detection in public cloud	LSTM	High accuracy rates > 99	Using datasets with real-world DDoS attacks	Scalability considerations for large-scale cloud environments	CCIC- DDoS 2019	2022
[65]	DDoS detection	Hybrid DBN-GRU architecture	High accuracy 97.05%.	Improved Sensitivity	Model tuning challenges	CICIDS 2017 KNN, NSL-KDD, and KDDcup99	2022
[66]	Mitigation DDoS attack	M-DBNN	87% accuracy	Improved performance	Model adaptability	CAIDA "DDoS 2007"	2022
[67]	DDoS detection	RBF-NN + HMPRO	Accuracy > 90 for both datasets	Optimal Weight Tuning for better performance	Real-time detection	CICDDoS2019 UNSW-NB_15	2022
[68]	DDoS attack detection	FACVO-DNFN	Accuracy 0.9304 for NSL-KDD and 0.9200, for BOT-IOT	Maximum detection efficiency	Real-time detection	NSL-KDD and BoT-IoT datasets.	2023
[69]	DDoS detection	GHLBO - DMN	High accuracy 0.917	Feature fusion and data augmentation	Limited evaluation metrics	NSL-KDD and BoT-IoT	2023
[70]	Detection of low-rate DDoS g	LRDADF and HA-LRDD	A high detection rate of 95.32%	Maintaining quality of Service	Resource intensive	CIC-DDoS2019	2023
[71]	Low-Rate DDoS detection	syncFL-bLAM	Highest accuracy is 98.68%,	Decentralized data handling	Training data bias	ISCX-2016-SlowDos	2023
[72]	DDoS detection	FEwDN	high accuracy value 99.67%	Reduced False Alarms	Adaptability to dynamic threats	CICDDoS2019	2023
[73]	Cyber attack prediction	Boosted NN	99.72% accuracy	Real-time monitoring	Adaptability to Zero-Day Attacks	MSCAD	2023

TABLE 4. *(Continued.)* **DDoS detection in cloud network using DL.**

[74]	DDoS attack prediction	Bi-LSTM	High accuracy value 97%	Efficient feature selection	Model Interpretability	Kaggle website-CSE-CIC-IDS2018-AWS, CICIDS2017, and CIC DoS	2024
[75]	DDoS prediction	DNN -CNN	DNN achieved the highest accuracy at 98.86%	Real-time detection	Scalability concerns	CICIDS 2017	2024
[76]	Enhancing DDoS detection	AutoCNN-DT	CNN-DT achieved the highest accuracy 0.9997	Real-time detection capabilities	FP and FN affect the overall accuracy	CIDDS-001	2024

Wang et al. [83] study focused on cloud computing, particularly in developing IDS using DL techniques like the Stacked Contractive Autoencoder (SCAE) and Support Vector Machine (SVM). The study addressed challenges such as the surge in network traffic within cloud environments, the rise of malicious attacks targeting cloud networks, and the pressing need for robust IDS to protect cloud computing resources. To tackle these issues, the research proposed employing the SCAE method for feature extraction and dimensionality reduction, along with integrating the SVM algorithm for classification, aiming to enhance the detection performance of cloud intrusion detection systems. The results of the experiments included the evaluation of various metrics like accuracy rate, precision rate, recall rate, F-measure, confusion matrix, and Receiver Operating Characteristic (ROC) to assess the effectiveness of the SCAE-SVM model. Comparative analysis with other approaches demonstrated the superiority of the proposed model in feature extraction, dimensionality reduction, and intrusion detection in cloud environments.

Yang et al. [84] focused on cybersecurity, particularly the development of IDS using ML techniques. They addressed the increasing volume and destructiveness of cyber-attacks in modern networks, the limited availability of public and complete code for ML-based IDSs, and the challenge of effectively detecting both known and zero-day attacks. The objectives include developing IDS-ML, an open-source code repository for IDS development, providing solutions to the general process of IDS development, demonstrating how ML algorithms can be used to design different types of IDSs, and improving intrusion detection performance with advanced techniques such as ensemble learning, Transfer Learning (TL), and Hyper-Parameter Optimization (HPO). The experimental setup involves utilizing IDS-ML, implementing various ML algorithms and techniques, and evaluating IDS performance using relevant metrics such as accuracy, precision, recall, F1-score, Area Under Curve (AUC), and Receiver Operating Characteristic (ROC), considering detection rates for different types of cyber-attacks.

The study [85] focused on IDS within distributed cloud computing, aiming to improve security through hybrid clustering and classification methods. Key challenges included the need to enhance IDS detection accuracy in distributed cloud setups and the limitations of traditional IDS models in identifying both known and unknown attacks effectively. To address these issues, the research proposed using ML-based hybrid models to improve IDS accuracy and implementing anomaly-based IDS with hybrid clustering and classification techniques such as K-Means clustering and Gaussian Mixture Model (GMM) and Random Forest (RF). Experiment results demonstrated significant enhancements in overall accuracy, detection rate, and false alarm ratio compared to traditional IDS models, showcasing improved performance in detecting various types of intrusions.

Bakro et al. [86] focused on enhancing IDS within cloud security, addressing concerns about data privacy and security in cloud environments amidst increasing cyber threats. By leveraging ML models, the proposed system classified network packets accurately to identify intrusions and preserve user data efficiently. Key contributions included integrating the Synthetic Minority Over-Sampling Technique (SMOTE) to handle imbalanced data, utilizing a hybrid feature selection approach combining Information Gain (IG), Chi-Square (CS), and Particle Swarm Optimization (PSO) for optimal feature subset selection, and employing the Random Forest (RF) model for attack detection. Experimental results demonstrated high accuracies exceeding 98% and 99% in multi-class classification scenarios, outperforming existing approaches. The results also showcased high detection rates and low false alarm rates, indicating the efficacy of the proposed system.

The research [87] explored intrusion detection in cloud computing, with a focus on identifying anomalies in time series data using ML techniques. It addressed concerns such as the susceptibility of cloud systems to attacks due to their open nature, as well as challenges related to privacy and security critical for cloud computing success. The solutions proposed involved leveraging IDS to safeguard cloud envi-

ronments, introducing time series anomaly detection as a viable solution, and integrating ML for enhanced anomaly detection and security measures. The results encompassed performance evaluations based on metrics like Dynamic Time Warping (DTW), Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Percentage Error (MAPE), Median Absolute Percentage Error (MdAPE). However, the proposed system showcased improved performance in detecting and preventing security threats in cloud computing environments.

Attou et al. [88] research focused on addressing the challenges associated with the detection of intrusions in cloud-based environments by proposing an innovative model that combines the Random Forest algorithm (RF) with feature engineering techniques. The study aimed to enhance security in cloud networks, considering issues of precision, scalability, and adaptability faced by conventional IDS and ML-driven IDS. The model exhibits commendable performance, achieving high accuracy, precision, and recall outperforming established solutions.

In research [89] Vashishtha et al. focused on developing a Hybrid Intrusion Detection Model (HIDM) for cloud-based healthcare systems, aiming to address the challenges of high detection rates for known attacks, the inability to detect new unknown attacks, and increased false alarm rates for unidentified or new attacks. The proposed model contributes by offering a hybrid approach that combines signature-based and anomaly-based detection methods, enabling the detection of both known and unknown attacks. The experimental setup involves evaluating performance based on accuracy and efficiency metrics. Results showed the proposed HIDM outperformed other models in terms of accuracy, with performance metrics including accuracy rates and security metrics focusing on the ability to detect known and unknown attacks.

The study [90] addressed cybersecurity, particularly focusing on constructing IDS tailored for cloud environments using bio-inspired feature selection algorithms in conjunction with a Random Forest (RF) model. The primary objectives were to develop a cloud-IDS utilizing hybrid bio-inspired feature selection algorithms alongside an RF model and to tackle the challenges associated with dataset development and feature selection in the realm of intrusion detection systems while showcasing enhanced performance and effectiveness compared to existing methodologies. Results from the experiments indicated improved performance in accuracy, recall, and false alarm rate.

B. IDS ANOMALY BASED ON DL - EXISTING RESEARCH WORKS

The research [91] focused on enhancing IDS within cloud computing environments to address cybersecurity challenges. It proposed a Fuzzy Min-Max Neural Networks-based IDS (FMMNN-IDS) to detect diverse network attacks, such as denial of service (DoS) attacks and malware infections. The FMMNN-IDS operated by processing network traffic data through hyperbox expansion and contraction stages to accurately detect intrusions. It demonstrated superior performance in accuracy and detection rates compared to existing approaches.

The study [92] developed an efficient IDS for cloud computing, aiming to address security vulnerabilities and mitigate overfitting. It employed a hybrid DL technique, integrating Improved Heap Optimization (IHO) for data preprocessing and Chaotic Red Deer Optimization (CRDO) for feature selection. The proposed deep Kronecker Neural Network (DKNN), named EOS-IDS, enhanced intrusion detection and classification accuracy. Through rigorous testing on benchmark datasets, EOS-IDS demonstrated competitive performance against state-of-the-art classifiers. Evaluation metrics such as accuracy, true positive rate (TPR), true negative rate (TNR), precision, and f-measure were used to evaluate the IDS in cloud computing environments. Notably, the EOS-IDS model offered significant contributions, achieving high accuracy rates of 97.221% for DARPA IDS datasets and 97.118% for CSE-CIC-IDS2018 datasets.

Pandey et al. [93] research focused on intrusion detection within the realm of big data in cloud computing, addressing the limitations of traditional IDS in countering external attacks affecting network behavior. It aimed to enhance network security through an Exponential Shuffled Shepherd Optimization Algorithm (ExpSSOA)-based deep maxout network for intrusion detection, integrating Exponentially Weighted Moving Average (EWMA) and Shuffled Shepherd Optimization Algorithm (SSOA) for improved performance. By utilizing information from big data sources like the Internet of Things (IoT) and Apache web server data. Experimental evaluation using the Apache web server dataset showcased superior accuracy, F-measure, precision, and recall compared to established methods like Multilayer Perceptron MLP, and Long-Short Term Memory LSTM+Spark.

The research [94] focused on presenting a new intelligent IDS model utilizing DL algorithms for enhancing cloud computing security. It aimed to tackle the difficulties of improving intrusion detection in cloud environments and optimizing feature selection to accurately identify evolving threats. The objectives involved introducing a novel IDS model that merged the Radial Basis Function Neural Network (RBFNN) and Random Forest (RF) to enhance accuracy and efficiency in intrusion detection. However, the research utilized performance metrics in the intelligent intrusion detection system to identify malicious activities in cloud computing, such as accuracy, precision, recall, and Matthew correlation coefficient. The model efficiently identified intrusions, demonstrating its ability to accurately detect and classify malicious activities, and indicating its potential to improve cybersecurity in cloud-based systems.

The research [95] aimed to improve the performance of IDS in cloud settings by employing Deep Neural Networks (DNN), backpropagation, and Particle Swarm Optimization (PSO) algorithms. It sought to address existing literature gaps, conduct a detailed analysis of the CSE-CIC-IDS-

2018 dataset, and compare the proposed models with prior approaches. The objectives included conducting an extensive empirical investigation on IDSs using multi-layer perceptron (MLP) and backpropagation MLP-BP and MLP with PSO techniques to enhance performance metrics in cloud environments. The results of the experiments showed enhanced performance metric scores, including accuracy, and precision.

The research [96] addressed various challenges encountered in cloud computing environments, including the increasing incidence of intrusions, security breaches in the virtual enterprise layer, limitations of conventional intrusion detection systems, and the necessity for enhanced architecture in distributed computing settings. Its objectives involved the development of Filter-Based Ensemble Feature Selection (FEFS) and DL Model (DLM) for intrusion detection in cloud computing. DLM is a combined approach of Recurrent Neural Network (RNN) and Tasmanian Devil Optimization (TDO). Performance evaluation utilized metrics like F-measure, specificity, sensitivity, and accuracy to evaluate the effectiveness of the proposed strategy. The results from the research demonstrated the efficacy of the proposed approach in improving security measures for intrusion detection in cloud computing environments.

Maheswari et al. [97] research examined challenges associated with improving security in cloud computing environments and enhancing the performance of IDS. Its aims include introducing a hybrid approach combining Teacher Learning optimization with Deep Recurrent Neural Networks (TL-DRNN) for IDS, employing Modified Manta-Ray Foraging Optimization (MMFO) for feature selection, and validating the proposed method using standard datasets. Results indicated enhanced performance concerning false positive rate, false negative rate, accuracy, precision, recall, specificity, and F-measure when compared to existing IDS approaches.

The research [98] focused on addressing several challenges related to cybersecurity in IoT-cloud systems, including their susceptibility to cyberattacks due to widespread connectivity and the critical need for robust security measures to safeguard IoT devices and cloud services. To tackle these issues, the study proposed solutions such as utilizing Swarm intelligence algorithms combined with Deep Neural Networks (DNN) for efficient intrusion detection, employing DNN to extract optimal features from IoT IDS data, and introducing a feature selection technique based on the Capuchin search algorithm (CapSA) to enhance intrusion detection capabilities. The results of the experiments included performance metrics such as average accuracy, average recall, average precision, and performance improvement rate, along with comparisons of the CNN-CapSA model with other optimization algorithms, ultimately concluding on the competitive performance of the proposed approach across various datasets.

The research [99] aimed to enhance IDS for cloud computing security, addressing issues like privacy, confidentiality, and availability in cloud systems, as well as detecting new intrusion types and mitigating quantum computing attacks. The proposed Ensemble intrusion detection model for cloud computing using deep learning (EICDL) focused on improving accuracy and efficiency in intrusion detection. It analyzed the drawbacks of existing IDS, introduced an accuracy enhancement model, and compared EICDL performance with modern ML methods and existing IDS. The system preprocessed input data, extracted features, classified using DL models like Gated Recurrent Units (GRU) and Convolutional Neural Network (CNN), and provided predictions. Evaluation metrics included accuracy, precision, recall, and F1 score across datasets. The study compared EICDL performance with other algorithms, consistently demonstrating higher precision, accuracy, and recall.

The article [100] discussed applying intrusion detection in online music education using Deep Neural Networks (DNN) on public cloud networks. The research aimed to tackle the challenges of detecting intrusions in this domain. The proposed framework involved fuzzy logic-based feature selection, optimization using the Salp Swarm algorithm, integration of Gated Recurrent Unit (GRU), and Convolutional Neural Network (CNN). Evaluation metrics included accuracy, precision, recall, and F1 score across datasets. The results indicated higher accuracy in detecting intrusions with the proposed models.

The research [101] tackled intrusion detection in computer networks within network security, focusing on challenges like the rising complexity of network attacks and the limitations of traditional firewalls. The aim was to develop an optimization-enabled DL model Rat Swarm Hunter Prey Optimization-Deep Maxout Network (RSHPO-DMN) to address intrusion detection issues. This involved tasks such as preprocessing data, Conventional Neural Network (CNN) -based feature extraction, utilizing DMN for intrusion detection, and enhancing performance through RSHPO optimization. The evaluation demonstrated the superior performance of RSHPO-DMN over other methods concerning accuracy, precision, recall, and F1-score.

Joraviya et al. [102] investigated several key issues, including addressing security challenges arising from containerization in cloud settings and improving the efficacy of intrusion detection systems for monitoring and identifying attacks within containerized environments. The proposed solutions involve employing DL methods, specifically Convolutional Neural Networks (CNNs), for anomaly detection in system call sequences and images derived from these calls. Results from the experimental assessment of the DL-based Host Intrusion Detection System DL-(HIDS) encompasses comparisons of detection accuracy, false positive rate, and false negative rate with existing methods, along with analyzing the impact of varying image sizes, system call parameters, and CNN architectures on detection performance. Furthermore, the evaluation assesses the system's capability to detect both known and unknown attacks in containerized cloud environments, ultimately aiming to implement DL-HIDS to improve security in such environments.

TABLE 5. IDS anomaly based in cloud network using ML.

REFERENCES	PROBLEM	SOLUTIONS	RESULTS	ADVANTAGES	DISADVANTAGES	DATA SOURS	YEAR
[79]	Log-based intrusion detection.	DT, NN, and ensemble meta-algorithms	NN with the highest accuracy of 98.47%	Minimal time overhead in performance	Dependency on Log quality	Web application logs	2020
[80]	Enhancing intrusion detection accuracy	hybrid FCM-SVM	High accuracy	Low false alarm rates	Scalability	NSL-KDD	2020
[81]	Improving IDS	Rough set theory and Bayes theorem	Accuracy of 0.97958	Enhanced detection rate	Manual preprocessing	CICIDS2017	2020
[82]	IDS to secure data	GA and SVM	Accuracy rate of 99.3	Scalability and Adaptability	Access to real Data for government sectors	CICIDS2017, KDD CUP 99	2021
[83]	Cloud IDS	SCAE + SVM	Highest accuracy with 5- class 97.87%	Efficient feature extraction.	Need for further optimization of the SVM	KDD Cup 99 and NSL-KDD	2022
[84]	IDS development	IDS-ML	Improved detection of cyber attacks	Open-source availability	Interpretability	CICIDS2017	2022
[85]	IDS	Clustering and classification models	Highest accuracy of 99.85%	Comparative Analysis	Threshold sensitivity	NSL-KDD and KDDcup99	2023
[86]	Cloud IDS	RF	Highest accuracy of 99%	Balanced Datasets	Overfitting risk	UNSW-NB15 dataset and the Kyoto dataset	2023
[87]	Cloud IDS	Time series anomalies detection and ML	Enhanced accuracy	Novel technique based on time series anomalies	Generalizability of the proposed method	CSE-CIC-IDS2018	2023
[88]	intrusions in cloud environments	RF	99.99% accuracy on NSL-KDD	Execution time	Enhancement is needed in the aspect of recall.	Bot-IoT and NSL-KDD	2023
[89]	Intrusion detection	HIDM	Highest accuracy of 99.8 %	High accuracy	Results on UNSW-NB15 and CICIDS need improvement.	UNSW-NB15, CICIDS2017 and NSL-KDD	2023
[90]	Cloud Intrusion Detection System	hybrid Bio-Inspired Feature Selection - RF	Highest accuracy of 99%	Utilization of the latest datasets	Algorithms complexity	UNSW-NB15, CIC-DDoS2019, and CIC Bell DNS EXF 2021	2024

VIII. RESEARCH GAP

Based on the extensive list of research articles provided, several research gaps and areas for further investigation in the field of Distributed Denial of Service anomaly (DDoS) and Intrusion Detection Systems (IDS) can be identified. Firstly, there is a notable gap in real-world testing and validation of detection methods, with many studies primarily focusing on development and evaluation using simulated or benchmark datasets like NSL-KDD, CICIDS, and KDD Cup, thus lacking extensive validation in real-world cloud computing environments or with live network traffic data. Secondly, scalability concerns persist, particularly in large-scale cloud environments warranting exploration into scalable intrusion detection techniques capable of efficiently handling increasing data volume and network traffic. Thirdly, there is a need for IDS that can adapt to dynamic threats, as many studies address known attack types but fall short in detecting emerging and evolving attack patterns. Additionally, while many detection methods achieve high accuracy rates, there is room for improvement in terms of computational efficiency and resource utilization. Moreover, there is a gap in developing IDS robust against evasion techniques employed by attackers to bypass detection mechanisms, highlighting the need for research focusing on evasion-resistant detection methods. Additionally, as organizations deploy multiple security solutions, there is a need for research on interoperability and seamless integration between IDS and other security tools to enhance overall threat detection and response capabilities. Finally, addressing privacy concerns and ethical considerations related to data collection, processing, and sharing in IDS development is imperative, underscoring the importance of developing privacy-preserving IDS techniques prioritiz-

TABLE 6. IDS anomaly based in cloud network using DL.

REFERENCES	PROBLEM	SOLUTIONS	RESULTS	ADVANTAGES	DISADVANTAGES	DATA SOURS	YEAR
[91]	Cloud IDS	FMMNN-IDS	High accuracy > 90	Capacity for nonlinear class boundaries	Training time	NSL-KDD	2022
[92]	Cloud IDS	DKNN	Highest accuracy of 97.221 % with DARPA IDS datasets	Hybrid classifier	Complexity	DARPA IDS and CSE-CIC-IDS2018	2022
[93]	Cloud Intrusion Detection Method	Deep Maxout network trained with ExpSSOA	Accuracy of 0.883	Integration of big data in intrusion detection:	Performance requires enhancement	MQTT-IOT-IDS2020 and Apache Web Server dataset	2023
[94]	IDS	RBFNN	High accuracy >94%	Effective detection	Feature selection	Bot-IoT and NSL-KDD	2023
[95]	IDS	DNN, PB, and PSO	Highest accuracy of 98.97%	Detailed analysis and comparison	Limited exploration of alternative algorithms	CSE-CIC-IDS2018	2023
[96]	IDS	RNN+ TDO	High accuracy 95%	Comparison with Conventional Techniques	Real-time performance	KDDCup-99 and NSL-KDD	2023
[97]	IDS	MMFO-TL-DRNN	The highest accuracy of 97.96% with CICIDS-2017	Applied to different datasets	Computational resources	DARPA LLS DDoS-1.0, CICIDS-2017, and CSIC-2010.	2023
[98]	Intrusion detection approach for cloud and IoT environments	CNN-CapSA	High accuracy >99%	Integration of DL and Swarm Intelligence	Convergence of CapSA was slow	NSL-KDD, BoT-IoT, KDD99, and CIC2017.	2023
[99]	IDS	EICDL	Highest accuracy of 97.88688% with KDDcup 1999	Leveraging DL	Time-consuming	KDDcup 1999, UNSW-NB15, and NSL-KDD	2023
[100]	Intrusion detection in online music education	GRU-CNN	Highest accuracy 98.89 %	Utilization of cloud resources for real-time intrusion detection	High computational demands	NSL-KDD and CICIDS2017	2024
[101]	IDS	RSHPO-DMN and CNN	High accuracy 90.88 %	Feature Extraction with CNN	Lack of real-world testing	NSL-KDD, CICIDS 2018, and BoT-IoT	2024
[102]	HIDS	CNN	High accuracy 98.12 %,	Enhanced detection capabilities	Quality and diversity of the dataset	LIDDS-2019.	2024

ing user privacy while maintaining effective threat detection. Addressing these research gaps can contribute significantly to the advancement of DDoS prevention and IDS technologies, ultimately enhancing the security posture of cloud computing and networked systems.

IX. SCOPE OF IMPROVEMENT

The field of Machine Learning (ML) holds extensive potential, especially concerning anomaly detection in cloud networks, with ongoing advancements in several key areas. These include improving data quality and quantity for training robust anomaly detection models, enhancing model interpretability for better understanding decision-making processes, addressing bias, and ensuring fairness in algorithms to prevent discriminatory outcomes, and refining transfer learning capabilities to leverage knowledge from related domains while ensuring scalability and efficiency for large-scale deployment in cloud environments.

Human-machine collaboration is crucial for refining anomaly detection systems, while AutoML solutions accelerate technology adoption. In the realm of Deep Learning (DL), progress is focused on architectural innovations, interpretability, transfer learning, efficiency, robustness, security, and continual learning. Exploring Quantum ML represents an innovative frontier for pushing anomaly detection capabilities in cloud networks further. These developments collectively contribute to the ongoing evolution of anomaly detection methodologies, ensuring continual enhancement in cloud environments. On the other hand, Large Language Models (LLMs) can be used effectively for anomaly detection by taking advantage of their advanced abilities in natural language processing. They can analyze text data and recognize patterns that are different from what is typically expected. Furthermore, integration of the LLM-powered anomaly detection system with existing cloud monitoring and security settings to provide comprehensive defense against cyber threats is essential for increasing the reliability of cloud infrastructures in the face of increasing security threats. However, LLM serves as an additional protection, complementing traditional rule-based or statistical anomaly detection methods. For example, Ali et al. [103]proposed solutions involve integrating LLMs and developing the HuntGPT prototype, which combines ML-based anomaly detection with explainable AI to provide actionable insights for threat responders. The system chatbot responses offer technical cybersecurity knowledge and clear explanations for detected anomalies, catering to users with limited cybersecurity experience. Additionally, time series analysis can be used efficiently to identify anomalies, contributing to the detection and prevention of anomalous behaviors in cloud environments. Moreover, integrating LLMs with time series analytic techniques can provide a more comprehensive solution to anomaly detection by taking advantage of the complimentary features of both methods. This integration can result in improved accuracy and efficacy of anomaly detection systems. Liu et al. [104] research addressed time series anomaly detection challenges by proposing AnomalyLLM, which used to extract knowledge from a trained LLM. AnomalyLLM outperforms state-of-the-art approaches, showing LLM effectiveness in improving time series anomaly identification.

X. CONCLUSION

This paper addresses the challenges and security threats encountered by cloud networks and suggests using ML/DL techniques as a solution. It discusses the prevalence of Distributed Denial of Service (DDoS) attacks in cloud computing, the limitations of current security measures, and the necessity for advanced security solutions. The proposed solutions involve ML/DL techniques for anomaly detection in cloud networks, specifically through an intrusion detection system (IDS) that combines multiple ML/DL algorithms for accurate threat detection and classification. The paper introduces an innovative security model, enhancing categorization accuracy and demonstrating the effectiveness of the proposed systems. However, it also highlights research gaps that provide opportunities for future studies to enhance anomaly detection in cloud environments, ultimately contributing to strengthening cloud network resilience against evolving cyber threats and safeguarding critical data and services.

REFERENCES

[1] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[2] A. Fatani, M. A. Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, "IoT intrusion detection system using deep learning and enhanced transient search optimization," *IEEE Access*, vol. 9, pp. 123448–123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[3] S. M. Kasongo, "An advanced intrusion detection system for IIoT based on GA and tree based algorithms," *IEEE Access*, vol. 9, pp. 113199–113212, 2021, doi: 10.1109/ACCESS.2021.3104113.

[4] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, Feb. 2017, doi: 10.1016/j.jnca.2016.11.027.

[5] Aws Amazon. *Summary of the Amazon S3 Service Disruption in Northern Virginia (U.S.-EAST-1) Region*. Accessed: Feb. 28, 2024. [Online]. Available: https://aws.amazon.com/message/41926/

[6] Ben Lovejoy. (2024). *Global Meta Outage: What Do We Know, and What Was the Likely Cause*. Accessed: Feb. 28, 2024. [Online]. Available: https://9to5mac.com/2024/03/06/global-meta-outage-what-happened/

[7] Z. Ji, Y. Wang, K. Yan, X. Xie, Y. Xiang, and J. Huang, "A space-embedding strategy for anomaly detection in multivariate time series," *Expert Syst. Appl.*, vol. 206, Nov. 2022, Art. no. 117892, doi: 10.1016/j.eswa.2022.117892.

[8] M. Hu, X. Feng, Z. Ji, K. Yan, and S. Zhou, "A novel computational approach for discord search with local recurrence rates in multivariate time series," *Inf. Sci.*, vol. 477, pp. 220–233, Mar. 2019, doi: 10.1016/j.ins.2018.10.047.

[9] A. Iqbal and R. Amin, "Time series forecasting and anomaly detection using deep learning," *Comput. Chem. Eng.*, vol. 182, Mar. 2024, Art. no. 108560, doi: 10.1016/j.compchemeng.2023.108560.

[10] Z. He, P. Chen, X. Li, Y. Wang, G. Yu, C. Chen, X. Li, and Z. Zheng, "A spatiotemporal deep learning approach for unsupervised anomaly detection in cloud systems," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 4, pp. 1705–1719, Apr. 2023, doi: 10.1109/TNNLS.2020.3027736.

[11] M. M. Belal and D. M. Sundaram, "Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9102–9131, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.035.

[12] A. Shajan and S. Rangaswamy, "Survey of security threats and countermeasures in cloud computing," *United Int. J. Res. Technol.*, vol. 2, no. 7, pp. 201–207, 2021.

[13] A. S. Rumale and D. N. Chaudhari, "Cloud computing: Software as a service," in *Proc. 2nd Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Feb. 2017, pp. 1–6, doi: 10.1109/ICECCT.2017.8117817.

[14] M. Yassin, H. Ould-Slimane, C. Talhi, and H. Boucheneb, "Multi-tenant intrusion detection framework as a service for SaaS," *IEEE Trans. Services Comput.*, vol. 15, no. 5, pp. 2925–2938, Sep. 2022, doi: 10.1109/TSC.2021.3077852.

[15] S. K. Sowmya, P. Deepika, J. Naren, and # B Tech. (2014). *Layers of Cloud-IaaS, PaaS and SaaS: A Survey*. [Online]. Available: www.ijcsit.com

[16] B. Habib and F. Khursheed, "REST-API based DDoS detection using random forest classifier in a platform as a service cloud environment," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 1075–1089, Sep. 2023, doi: 10.12785/ijcds/140184.

[17] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, Jul. 2017, doi: 10.1109/TCC.2015.2415794.

[18] S. A. Varma and K. G. Reddy, "A review of DDoS attacks and its countermeasures in cloud computing," in *Proc. 5th Int. Conf. Inf. Syst. Comput. Netw. (ISCON)*, Oct. 2021, pp. 1–6, doi: 10.1109/ISCON52037.2021.9702388.

[19] J. Snehi, M. Snehi, A. Bhandari, V. Baggan, and R. Ahuja, "Introspecting intrusion detection systems in dealing with security concerns in cloud environment," in *Proc. 10th Int. Conf. Syst. Model. Advancement Res. Trends (SMART)*, Dec. 2021, pp. 345–349, doi: 10.1109/SMART52563.2021.9676258.

[20] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison," *Bull. Electr. Eng. Informat.*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[21] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Netw.*, vol. 44, no. 5, pp. 643–666, Apr. 2004, doi: 10.1016/j.comnet.2003.10.003.

[22] Cisco. (2023). *Cisco Annual Internet Report (2018–2023) White Paper*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[23] C. Kruegel, F. Valeur, and G. Vigna, *Intrusion Detection and Correlation: Challenges and Solutions*, vol. 14. Cham, Switzerland: Springer, 2004.

[24] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," *Nat. Inst. Standards Technol.*, vol. 800, p. 94, Feb. 2007.

[25] A. Momand, S. U. Jan, and N. Ramzan, "A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy," *J. Sensors*, vol. 2023, pp. 1–18, Feb. 2023, doi: 10.1155/2023/6048087.

[26] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6, doi: 10.1109/CISDA.2009.5356528.

[27] (2017). *Intrusion Detection Evaluation Dataset (CIC-IDS2017)*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[28] 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.

[29] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[30] (2019). *DDoS Evaluation Dataset (CIC-DDoS2019)*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html.

[31] (2018). *CSE-CIC-IDS2018 on AWS: A Collaborative Project Between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC)*. Accessed: Mar. 11, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html.

[32] O. Osanaiye, H. Cai, K.-K.-R. Choo, A. Dehghantanha, Z. Xu, and M. Dlodlo, "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 1–10, Dec. 2016, doi: 10.1186/s13638-016-0623-3.

[33] Y. Freund and R. E. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," *J. Comput. Syst. Sci.*, vol. 55, no. 1, pp. 119–139, Aug. 1997, doi: 10.1006/jcss.1997.1504.

[34] *Traffic Data From Kyoto University's Honeypots*. Accessed: Mar. 11, 2024. [Online]. Available: https://www.takakura.com/Kyoto_data/

[35] 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.

[36] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, Feb. 2020, Art. no. 105124, doi: 10.1016/j.knosys.2019.105124.

[37] G. S. Kushwah and V. Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102532, doi: 10.1016/j.jisa.2020.102532.

[38] S. Sambangi and L. Gondi, "A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression," *Proceedings*, vol. 63, no. 1, p. 51, 2020, doi: 10.3390/proceedings2020063051.

[39] R. Abubakar, A. Aldegheishem, M. F. Majeed, A. Mehmood, H. Maryam, N. A. Alrajeh, C. Maple, and M. Jawad, "An effective mechanism to mitigate real-time DDoS attack," *IEEE Access*, vol. 8, pp. 126215–126227, 2020, doi: 10.1109/ACCESS.2020.2995820.

[40] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "RETRACTED ARTICLE: Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 3, pp. 3609–3619, Mar. 2021, doi: 10.1007/s12652-019-01611-9.

[41] 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.

[42] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102260, doi: 10.1016/j.cose.2021.102260.

[43] S. Sachdeva and A. Ali, "Machine learning with digital forensics for attack classification in cloud network environment," *Int. J. Syst. Assurance Eng. Manage.*, vol. 13, no. S1, pp. 156–165, Mar. 2022, doi: 10.1007/s13198-021-01323-4.

[44] M. M. G. Alam, S. J. N. Kumar, R. U. Mageswari, and T. F. M. Raj, "An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment," *Comput. Netw.*, vol. 215, Oct. 2022, Art. no. 109138, doi: 10.1016/j.comnet.2022.109138.

[45] 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.

[46] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, p. 1095, May 2022, doi: 10.3390/sym14061095.

[47] S. Sambangi, L. Gondi, and S. Aljawarneh, "A feature similarity machine learning model for DDoS attack detection in modern network environments for Industry 4.0," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107955, doi: 10.1016/j.compeleceng.2022.107955.

[48] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, Sep. 2022, Art. no. 100229, doi: 10.1016/j.array.2022.100229.

[49] S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach," *Concurrency Computation, Pract. Exper.*, vol. 34, no. 27, Dec. 2022, Art. no. e7334, doi: 10.1002/cpe.7334.

[50] 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.

[51] S. V. J. Rani, I. Ioannou, P. Nagaradjane, C. Christophorou, V. Vassiliou, S. Charan, S. Prakash, N. Parekh, and A. Pitsillides, "Detection of DDoS attacks in D2D communications using machine learning approach," *Comput. Commun.*, vol. 198, pp. 32–51, Jan. 2023, doi: 10.1016/j.comcom.2022.11.013.

[52] Y. Shang, "Prevention and detection of DDOS attack in virtual cloud computing environment using naive Bayes algorithm of machine learning," *Meas., Sensors*, vol. 31, Feb. 2024, Art. no. 100991, doi: 10.1016/j.measen.2023.100991.

[53] H. Setia, A. Chhabra, S. K. Singh, S. Kumar, S. Sharma, V. Arya, B. B. Gupta, and J. Wu, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Secur. Appl.*, vol. 2, Jan. 2024, Art. no. 100037, doi: 10.1016/j.csa.2024.100037.

[54] 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.

[55] F. Talpur, I. A. Korejo, A. A. Chandio, A. Ghulam, and M. S. H. Talpur, "ML-based detection of DDoS attacks using evolutionary algorithms optimization," *Sensors*, vol. 24, no. 5, p. 1672, Mar. 2024, doi: 10.3390/s24051672.

[56] S. Dasari and R. Kaluri, "An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques," *IEEE Access*, vol. 12, pp. 10834–10845, 2024, doi: 10.1109/ACCESS.2024.3352281.

[57] S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired deep belief network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Gener. Comput. Syst.*, vol. 110, pp. 80–90, Sep. 2020, doi: 10.1016/j.future.2020.03.049.

[58] 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.

[59] N. Mishra and R. K. Singh, "DDoS vulnerabilities analysis and mitigation model in cloud computing," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 2, pp. 535–545, Feb. 2020, doi: 10.1080/09720529.2020.1729503.

[60] S. Velliangiri, P. Karthikeyan, and V. Vinoth Kumar, "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks," *J. Experim. Theor. Artif. Intell.*, vol. 33, no. 3, pp. 405–424, May 2021, doi: 10.1080/0952813x.2020.1744196.

[61] J. B. Dennis and M. S. Priya, "Deep belief network and support vector machine fusion for distributed denial of service and economical denial of service attack detection in cloud," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 1, Jan. 2022, Art. no. e6543, doi: 10.1002/cpe.6543.

[62] M. Almiani, A. Abughazleh, Y. Jararweh, and A. Razaque, "Resilient back propagation neural network security model for containerized cloud computing," *Simul. Model. Pract. Theory*, vol. 118, Jul. 2022, Art. no. 102544, doi: 10.1016/j.simpat.2022.102544.

[63] D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Comput. Secur.*, vol. 118, Jul. 2022, Art. no. 102748, doi: 10.1016/j.cose.2022.102748.

[64] 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, Jul. 2022, Art. no. 102725, doi: 10.1016/j.cose.2022.102725.

[65] A. A. S. Aliar, M. Agoramoorthy, and Y. Justindhas, "An automated detection of DDoS attack in cloud using optimized weighted fused features and hybrid DBN-GRU architecture," *Cybern. Syst.*, pp. 1–42, Jan. 2023, doi: 10.1080/01969722.2022.2157603.

[66] A. Agrawal, R. Singh, M. Khari, S. Vimal, and S. Lim, "Autoencoder for design of mitigation model for DDOS attacks via M-DBNN," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–14, Apr. 2022, doi: 10.1155/2022/9855022.

[67] M. Varghese and M. Victor Jose, "An optimized radial bias function neural network for intrusion detection of distributed denial of service attack in the cloud," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 27, Dec. 2022, Art. no. e7321, doi: 10.1002/cpe.7321.

[68] G. S. R. E. Selvan, 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, Feb. 2023, Art. no. 110132, doi: 10.1016/j.knosys.2022.110132.

[69] S. Balasubramaniam, C. Vijesh Joe, T. A. Sivakumar, A. Prasanth, K. S. Kumar, V. Kavitha, and R. K. Dhanaraj, "Optimization enabled deep learning-based DDoS attack detection in cloud computing," *Int. J. Intell. Syst.*, vol. 2023, pp. 1–16, Feb. 2023, doi: 10.1155/2023/2039217.

[70] 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," *Meas., Sensors*, vol. 28, Aug. 2023, Art. no. 100828, doi: 10.1016/j.measen.2023.100828.

[71] Z. Liu, C. Guo, D. Liu, and X. Yin, "An asynchronous federated learning arbitration model for low-rate DDoS attack detection," *IEEE Access*, vol. 11, pp. 18448–18460, 2023, doi: 10.1109/ACCESS.2023.3247512.

[72] S. A. Varma and K. G. Reddy, "An AI based IDS framework for detecting DDoS attacks in cloud environment," *Inf. Secur. J., Global Perspective*, pp. 1–13, Nov. 2023, doi: 10.1080/19393555.2023.2279535.

[73] S. Dalal, P. Manoharan, U. K. Lilhore, B. Seth, D. M. Alsekait, S. Simaiya, M. Hamdi, and K. Raahemifar, "Extremely boosted neural network for more accurate multi-stage cyber attack prediction in cloud computing environment," *J. Cloud Comput.*, vol. 12, no. 1, p. 14, Jan. 2023, doi: 10.1186/s13677-022-00356-9.

[74] 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, May 2024, Art. no. 122544, doi: 10.1016/j.eswa.2023.122544.

[75] J. Arango-López, G. Isaza, F. Ramirez, N. Duque, and J. Montes, "Cloud-based deep learning architecture for DDoS cyber attack prediction," *Expert Syst.*, Jan. 2024, Art. no. e13552, doi: 10.1111/exsy.13552.

[76] M. Ouhssini, K. Afdel, E. Agherrabi, M. Akouhar, and A. Abarda, "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 36, no. 2, Feb. 2024, Art. no. 101938, doi: 10.1016/j.jksuci.2024.101938.

[77] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 870–875, doi: 10.1109/AICAI.2019.8701238.

[78] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," 2017, *arXiv:1701.02145*.

[79] J. Fontaine, C. Kappler, A. Shahid, and E. De Poorter, "Log-based intrusion detection for cloud Web applications using machine learning," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 14th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2019) 14*. Springer, 2020, pp. 197–210.

[80] A. N. Jaber and S. U. Rehman, "FCM–SVM based intrusion detection system for cloud computing environment," *Cluster Comput.*, vol. 23, no. 4, pp. 3221–3231, Dec. 2020, doi: 10.1007/s10586-020-03082-6.

[81] M. Prasad, S. Tripathi, and K. Dahal, "An efficient feature selection based Bayesian and rough set approach for intrusion detection," *Appl. Soft Comput.*, vol. 87, Feb. 2020, Art. no. 105980, doi: 10.1016/j.asoc.2019.105980.

[82] A. Aldallal and F. Alisa, "Effective intrusion detection system to secure data in cloud using machine learning," *Symmetry*, vol. 13, no. 12, p. 2306, Dec. 2021, doi: 10.3390/sym13122306.

[83] 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 Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, Jul. 2022, doi: 10.1109/TCC.2020.3001017.

[84] L. Yang and A. Shami, "IDS-ML: An open source code for intrusion detection system development using machine learning," *Softw. Impacts*, vol. 14, Dec. 2022, Art. no. 100446, doi: 10.1016/j.simpa.2022.100446.

[85] K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," *Meas., Sensors*, vol. 25, Feb. 2023, Art. no. 100612, doi: 10.1016/j.measen.2022.100612.

[86] M. Bakro, R. R. Kumar, A. Alabrah, Z. Ashraf, M. N. Ahmed, M. Shameem, and A. Abdelsalam, "An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier," *IEEE Access*, vol. 11, pp. 64228–64247, 2023, doi: 10.1109/ACCESS.2023.3289405.

[87] A.-R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *J. Cloud Comput.*, vol. 12, no. 1, p. 127, Aug. 2023, doi: 10.1186/s13677-023-00491-x.

[88] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-based intrusion detection approach using machine learning techniques," *Big Data Mining Anal.*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/BDMA.2022.9020038.

[89] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "HIDM: A hybrid intrusion detection model for cloud based systems," *Wireless Pers. Commun.*, vol. 128, no. 4, pp. 2637–2666, Feb. 2023, doi: 10.1007/s11277-022-10063-y.

[90] M. Bakro, R. R. Kumar, M. Husain, Z. Ashraf, A. Ali, S. I. Yaqoob, M. N. Ahmed, and N. Parveen, "Building a cloud-IDS by hybrid bio-inspired feature selection algorithms along with random forest model," *IEEE Access*, vol. 12, pp. 8846–8874, 2024, doi: 10.1109/ACCESS.2024.3353055.

[91] A. Kumar, R. S. Umurzoqovich, N. D. Duong, P. Kanani, A. Kuppusamy, M. Praneesh, and M. N. Hieu, "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," *Optik*, vol. 270, Nov. 2022, Art. no. 170044, doi: 10.1016/j.ijleo.2022.170044.

[92] M. Mayuranathan, S. K. Saravanan, B. Muthusenthil, and A. Samydurai, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique," *Adv. Eng. Softw.*, vol. 173, Nov. 2022, Art. no. 103236, doi: 10.1016/j.advengsoft.2022.103236.

[93] B. K. Pandey, S. Ahmad, C. Rodriguez, and D. Esenarro, "ExpSSOA-deep maxout: Exponential shuffled shepherd optimization based deep maxout network for intrusion detection using big data in cloud computing framework," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102975, doi: 10.1016/j.cose.2022.102975.

[94] H. Attou, M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour, A. Alabdultif, and N. Almusallam, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Appl. Sci.*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[95] S. Alzughaibi and S. El Khediri, "A cloud intrusion detection systems based on DNN using backpropagation and PSO on the CSE-CIC-IDS2018 dataset," *Appl. Sci.*, vol. 13, no. 4, p. 2276, Feb. 2023, doi: 10.3390/app13042276.

[96] C. Kavitha, M. Saravanan, T. R. Gadekallu, K. Nimala, B. P. Kavin, and W. C. Lai, "Filter-based ensemble feature selection and deep learning model for intrusion detection in cloud computing," *Electronics*, vol. 12, no. 3, p. 556, Jan. 2023, doi: 10.3390/electronics12030556.

[97] K. G. Maheswari, C. Siva, and G. Nalinipriya, "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.*, vol. 202, pp. 145–153, Mar. 2023, doi: 10.1016/j.comcom.2023.02.003.

[98] M. A. Elaziz, M. A. A. Al-Qaness, A. Dahou, R. A. Ibrahim, and A. A. A. El-Latif, "Intrusion detection approach for cloud and IoT environments using deep learning and capuchin search algorithm," *Adv. Eng. Softw.*, vol. 176, Feb. 2023, Art. no. 103402, doi: 10.1016/j.advengsoft.2022.103402.

[99] D. B. Salvakkam, V. Saravanan, P. K. Jain, and R. Pamula, "Enhanced quantum-secure ensemble intrusion detection techniques for cloud based on deep learning," *Cognit. Comput.*, vol. 15, no. 5, pp. 1593–1612, Sep. 2023, doi: 10.1007/s12559-023-10139-2.

[100] J. Zhang, J. D. Peter, A. Shankar, and W. Viriyasitavat, "Public cloud networks oriented deep neural networks for effective intrusion detection in online music education," *Comput. Electr. Eng.*, vol. 115, Apr. 2024, Art. no. 109095, doi: 10.1016/j.compeleceng.2024.109095.

[101] A. Parameswari, R. Ganeshan, V. Ragavi, and M. Shereesha, "Hybrid rat swarm hunter prey optimization trained deep learning for network intrusion detection using CNN features," *Comput. Secur.*, vol. 139, Apr. 2024, Art. no. 103656, doi: 10.1016/j.cose.2023.103656.

[102] N. Joraviya, B. N. Gohil, and U. P. Rao, "DL-HIDS: Deep learning-based host intrusion detection system using system calls-to-image for containerized cloud environment," *J. Supercomput.*, pp. 1–29, Feb. 2024, doi: 10.1007/s11227-024-05895-3.

[103] T. Ali and P. Kostakos, "HuntGPT: Integrating machine learning-based anomaly detection and explainable AI with large language models (LLMs)," 2023, *arXiv:2309.16021*.

[104] C. Liu, S. He, Q. Zhou, S. Li, and W. Meng, "Large language model guided knowledge distillation for time series anomaly detection," 2024, *arXiv:2401.15123*.

AMIRA MAHAMAT ABDALLAH received the B.S. degree in computer science from Taibah University, Saudi Arabia, in 2018. She is currently pursuing the M.S. degree in information security with United Arab Emirates University, United Arab Emirates. Her research interests include cloud security, intrusion detection systems, and artificial intelligence.

AYSHA SAIF RASHED OBAID ALKAABI is currently pursuing the B.Sc. degree in information security with United Arab Emirates University, United Arab Emirates. Her research interests include cloud security, intrusion detection systems, and artificial intelligence.

GHAYA BARK NASSER DOUMAN ALAMERI is currently pursuing the B.Sc. degree in Computer Science with United Arab Emirates University, United Arab Emirates. Her research interests include cloud security, intrusion detection systems, and artificial intelligence.

SAIDA HAFSA RAFIQUE received the B.Sc. degree in cellular and molecular biology from United Arab Emirates University (UAEU), United Arab Emirates, in 2019, and the first M.Sc. degree in forensic science from the University of Strathclyde, U.K., in 2020. She is currently pursuing the second M.Sc. degree in information security with UAEU. Her research interests include cloud security, the IoT security, artificial intelligence, digital forensics, and forensic science.

NURA SHIFA MUSA received the bachelor's degree in computer engineering from Qatar University (QU), Qatar, and the master's degree in information security from the College of Information Technology, United Arab Emirates University (UAEU), United Arab Emirates. She is currently a Senior Laboratory Supervisor with the College of Engineering, Al Ain University (AAU), United Arab Emirates. Demonstrating a profound dedication to advancing cyber security measures, her research interests include developing innovative solutions to enhance digital security, investigating cyber threats, exploring cloud computing technology, and conducting digital forensic investigations. She received awards and honors.

THANGAVEL MURUGAN (Senior Member, IEEE) received the B.E. degree (Hons.) in computer science and engineering from the M. A. M. College of Engineering, Trichy, India, under Anna University, Chennai, India, the M.E. degree (Hons.) in computer science and engineering from the J. J. College of Engineering and Technology, Trichy, under Anna University, and the Ph.D. degree from Madras Institute of Technology (MIT) Campus, Anna University. He is currently an Assistant Professor with the Department of Information Systems and Security, College of Information Technology, United Arab Emirates University. He also holds more than 11 years of teaching and research experience from various academic institutions. He has published more than ten articles in international journals, more than 15 book chapters in international publishers, more than 25 in the proceedings of international conferences, and three in the proceedings of national conferences/seminars. His academic and research interests include information security, high-performance computing, ethical hacking, cyber forensics, blockchain, cybersecurity intelligence, and educational technology.