Anomaly Detection in Cloud Network: A Review

Amer Al-Mazrawe[1*] and *Bahaa* Al-Musawi[2]

[1,2] Faculty of Education, University of Kufa, Najaf, Iraq

Abstract. Cloud computing stands out as one of the fastest-growing technologies in the 21st century, offering enterprises opportunities to reduce costs, enhance scalability, and increase flexibility through rapid access to a shared pool of elastic computing resources. However, its security remains a significant challenge. As cloud networks grow in complexity and scale, the need for effective anomaly detection becomes crucial. Identifying anomalous behavior within cloud networks poses a challenge due to factors such as the voluminous data exchanged and the dynamic nature of underlying cloud infrastructures. Detecting anomalies helps prevent threats and maintain cloud operations. This literature review examines previous works in anomaly detection in the cloud that employ various strategies for anomaly detection, describes anomaly detection datasets, discusses the challenges of anomaly detection in cloud networks, and presents directions for future studies.

1 Introduction

In the rapidly evolving landscape of contemporary IT, cloud computing emerges as a highly dynamic and ubiquitous concept. It intricately connects data and applications from diverse geographic locations, harnessing the power of emerging Internet technologies. Often considered an advanced iteration of utility computing, cloud computing continually evolves, presenting operators with both enhanced capabilities and challenges. Cloud services are delivered from data centres across various global locations, ensuring widespread accessibility and robust, scalable solutions for businesses and individuals. To meet different user needs, cloud providers present three main service models: Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). Cloud computing may be employed in public, private, hybrid, and community clouds, providing businesses and individuals with a new means of accessing and utilizing these resources while reducing cost, improving scalability, and increasing flexibility [1].

Cloud computing is utilized in various industries, including big data analytics, IoT applications, content delivery, and disaster recovery. Its applications include e-commerce, healthcare, and education, showcasing its flexibility, scalability, and efficiency. Cloud services enable scalable hosting, efficient payment processing, secure data storage, and telemedicine support while enhancing collaboration and learning management systems. According to a survey conducted by IEEE, Cloud computing ranked as the second most important technology following artificial intelligence [2]. Indeed, despite the numerous advantages that cloud computing offers, security concerns persist as a prominent issue for many organizations. In 2020, a Fugue and Sonatype survey revealed that 36% of companies encountered a substantial breach or loss of cloud security data [3].

This apprehension comes from cloud characteristics like the shared nature of cloud environments and introduces the concerns of data breaches or loss of control over data. Cloud service providers heavily invest in security measures and offer robust tools to secure data and applications. While security concerns persist, they are often outweighed by the benefits of cloud computing, leading many organizations to adopt cloud solutions while addressing security as a top priority [4].

To address security issues in cloud computing effectively, organizations should adopt a comprehensive strategy that includes thorough risk assessments, classification of data sensitivity, robust authentication, access controls, and encryption—advanced security strategies like analysing attacker activity and identifying the early stages of attacks. Anomaly detection strategies are primary methods that focus on data analysis and pattern recognition [5].

Various techniques, such as statistical analysis, machine learning, deep learning, and hybrid approaches, are utilized in numerous studies to deal with different forms of abnormalities. Different forms of anomalies include individual anomalies, contextual abnormalities, and collective abnormalities.

Anomaly detection enhances cloud computing security by allowing providers to monitor systems for suspicious activities and respond promptly to potential threats. It helps detect unknown attacks, early warning systems, and stealthy attacks, adapt to evolving threats, and reduce false positives [4].

* Corresponding author: amiersame@gmail.com

The primary contributions of this survey can be brief as follows:

- We delve into the examination of the commonly used datasets for evaluating cloud network anomaly detection techniques, shedding light on their strengths and weaknesses. Additionally, we spotlight the distinctive characteristics of the next generation of cloud network datasets.
- We examine cloud anomaly detection techniques, reviewing their approaches, and the datasets employed, and outlining both their strengths and weaknesses.
- We identify challenges and outline essential criteria to guide future solutions in the domain of cloud anomaly detection.

The paper is organized as follows: Section 2 presents a brief description of cloud computing and cloud security issues while Section 3 looks closely at benchmark datasets in the cloud computing domain. Section 4 investigates several studies on cloud security to consider anomaly detection. Section 5 summarizes anomaly detection challenges and provides key specifications for upcoming cloud anomaly detection systems. Section 6 introduces conclusions and future directions.

2 Cloud Computing Overview

Cloud computing security refers to a set of measures, practices, and technologies designed to protect data, applications, and resources within cloud computing environments from unauthorized access, data breaches, data loss, and other potential threats and vulnerabilities [6]. The National Institute of Standards and Technology (NIST) defines cloud computing as a model composed of five key characteristics, three service models, and four deployment models. The key characteristics refer to on-demand self-service, broad network access, dynamic resource pooling, rapid elasticity, and measured service. Cloud computing offers various service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models are deployed either as a public cloud, a private cloud, a hybrid cloud, or a community cloud. Each of these models has its own control, security, and management options to meet organizational needs [7]. Figure 1 illustrates the framework for defining cloud computing models by NIST.

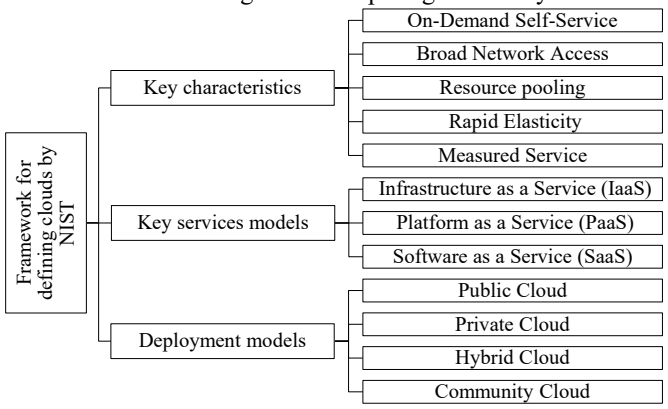

Fig. 1. Framework for defining clouds by NIST.

Cloud computing faces eleven security concerns, as outlined in NIST's document and illustrated in Figure 2 [8]. Including unauthorized access, data breaches, service traffic hijacking, insecure interfaces and APIs, denial-of-service attacks, and loss of confidentiality, security, availability, and integrity. These risks can lead to data breaches, service traffic hijacking, and disruption of cloud services. Confidentiality and integrity are the most vulnerable characteristics of cloud computing. Researchers have developed cloud security systems to mitigate these risks, ensuring the security of all cloud services. These systems aim to protect against data breaches, hijacking, insecure interfaces, APIs, and denial-of-service attacks [9].

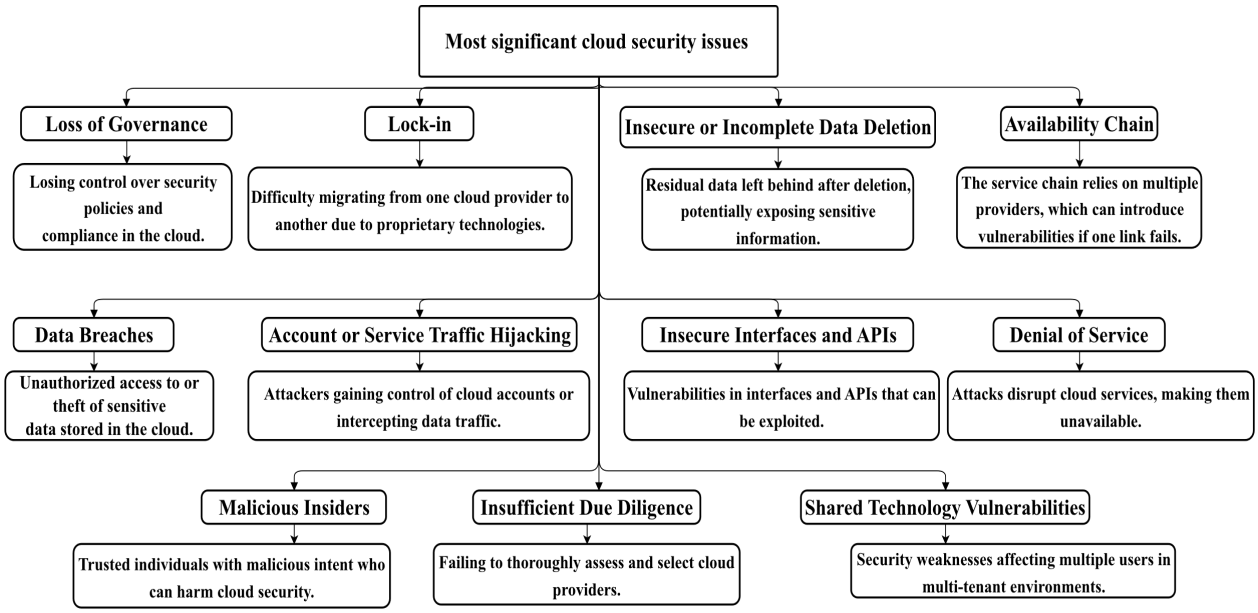

Fig. 2. Most significant cloud security issues by NIST

Microservices, data susceptibility, and auto-scaling functionalities lead to collaborative measures by service providers and customers that are essential to reaching the highest security standards in cloud security. To instill trust and align with business regulatory requirements, organizations must grasp the intricacies of security issues and optimize their governance and policy frameworks. The overarching domains of security can be further subdivided into specific areas, as illustrated in Figure 3 [9].

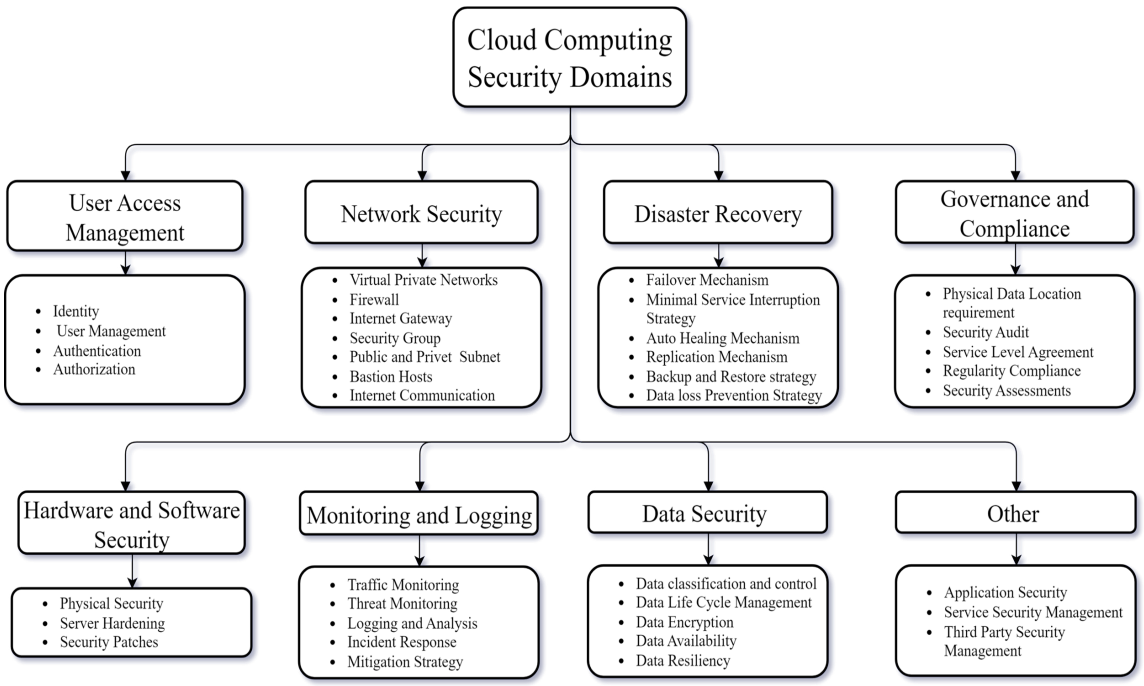

Fig. 3. Cloud computing security domains

Cloud security encompasses several critical facets, including identity and access management (IAM), which ensures that the right individuals have proper access to resources. Data security is another vital concern. Disaster recovery strategies focus on data restoration objectives. Additionally, network security requires optimized configuration and security measures to safeguard applications in the cloud. Governance and compliance demand adherence to recognized standards like ISO/IEC 27001, along with stringent audit and assessment requirements. Hardware and software security, monitoring, and logging round out these core security practices. Also, the management of service security for microservices, third-party tool and

software oversight, application-level security, and the integration of security practices throughout the software development process These elements collectively establish a robust security posture in the cloud, ensuring the protection of data, applications, and resources [10].

3 Cloud Computing Datasets

Cloud anomaly detection datasets are crucial for researchers to evaluate techniques, assess their effectiveness, and benchmark different approaches. These datasets include normal and abnormal instances, representing various cloud-related events and scenarios. They provide a realistic sample of cloud data, ensuring anomaly detection methods can perform well in real-world environments. The availability and diversity of these datasets contribute to advancing the capabilities of anomaly detection techniques, confirming the security and reliability of cloud-based techniques.

To develop an effective anomaly detection system in the dynamic cloud environment, it is essential to consider into account the features of the dataset, including its content, source, and format, and to adapt the approach suitably. Selecting an appropriate dataset for anomaly detection in the cloud is a difficult task due to the constantly evolving system characteristics and data patterns, the infrequency and numerous anomalies, and the requirement for organized filtering and pre-processing.

The optimal choice of datasets is crucial to introducing accurate approaches. For example, to evaluate time series analysis approaches, we must prioritize datasets with many characteristics, such as realism, the inclusion of recent attacks, timestamp format, and others, to maximize the efficacy of the proposed methods. Table 1 explores the symbols used for the types of attacks in selected datasets. Table 2 presents the most widely used datasets in cloud computing, focusing on their characteristics such as data type, number and types of attacks, and number of extracted features.

Table 1. The symbols used for the types of attacks in selected datasets.

Attack Types	Symbol	Attack Types	Symbol	Attack Types	Symbol
Probing attacks	AT-1	Information Theft	AT-22	botnet	AT-43
DoS	AT-2	Ports can	AT-23	Weaponization	AT-44
R2L	AT-3	Ping Scan	AT-24	Exploitation	AT-45
U2R	AT-4	Web Scanning	AT-25	Lateral Movement	AT-46
Data attack	AT-5	Ransomware	AT-26	Command &Control	AT-47
Code-Red	AT-6	Injection	AT-27	Exfiltration	AT-48
Code-Red II	AT-7	Directory/Path Traversal	AT-28	Tampering	AT-49
Anomaly Score	AT-8	Cross-site Scripting (XSS)	AT-29	Crypto Ransomware	AT-50
Fuzzers	AT-9	SQL Injection	AT-30	RDoS	AT-51
Worms Analysis	AT-10	HTTP Flood DoS	AT-31	Recon	AT-52
Backdoors	AT-11	DNS amplification DoS	AT-32	Web-Based	AT-53
Exploits	AT-12	Ports and Network scanning	AT-33	Spoofing	AT-54
Generic	AT-13	Unclassified (unsolicited traffic)	AT-34	Mirai	AT-55
Reconnaissance	AT-14	Cryptojacking	AT-35	Password Cracking	AT-56
Shellcode	AT-15	UDP Flood DoS	AT-36	Synflood DoS	AT-57
Heartbleed	AT-16	Insider threat	AT-37		
Brute force	AT-17	Trojan Horse	AT-38		
DDOS	AT-18	Steppingstone	AT-39		
Web Attack	AT-19	Brute Force FTP	AT-40		
Infiltration					
Attack	AT-20	SSH	AT-41		

Table 2. A brief of the most widely used datasets for detecting anomalies in cloud computing.

No.	Dataset Name	Year	Data Type	Host resources / Network traffic	Attacks	No. of Features
1	Code Red worm [11]	2001	Real	Host Resources	AT-6, AT-7	2
2	KDD Cup 1999 [12]	2007	Real	Network traffic	AT-1, AT-2, AT-3, AT-4	41
3	NSL-KDD [13]	2009	Real	Network traffic	AT-1, AT-2, AT-3, AT-4	41
4	NAB [14]	2015	Real	Host and Network Traffic	AT-8	58

5	UNSW_NB15 [15]	2017	Hybrid	Network traffic	AT-2, AT-9, AT-10, AT-11, AT-12, AT-13, AT-14, AT-15	49
6	CICIDS 2017 [16]	2017	Real	Network traffic	AT-2, AT-16, AT-17, AT-19, AT-20, AT-40, AT-41	80
7	CIDDS 001 [17]	2017	Real	Network traffic	AT-23, AT-2, AT-17, AT-24	14
8	BoT IoT [18]	2018	Real	Network traffic	AT-1, AT-18, AT-22	10
9	ISOT CID [19]	2018	Real	Host and Network Traffic	AT-2, AT-9, AT-17, AT-25, AT-28, AT-29, AT-30, AT-31, AT-32, AT-33, AT-34, AT-35, AT-36, AT-37, AT-38, AT-39, AT-57	17
10	CIC-DdoS2019 [20]	2019	Real	Network traffic	AT-18	80
11	TON_IoT [21]	2020	Real	Host and Network Traffic	AT-2, AT-11, AT-18, AT-25, AT-26, AT-27, AT-29, AT-56	22
12	RARE [22]	2020	synthetic	Host Resources	AT-42	1
13	X-IIoTID [23]	2021	Real	Host and Network Traffic	AT-13, AT-14, AT-44, AT-45, AT-46, AT-47, AT-48, AT-49, AT-50, AT-51	67
14	CICIoT2023 [24]	2023	Real	Network traffic	AT-2, AT-18, AT-17, AT-52, AT-53, AT-54, AT-55	48

Each dataset has limitations and strengths, for instance, the KDD Cup99 dataset has the limitation of the imbalanced dataset. Another example is the CICIDS 2017 dataset. Although it contains the most frequent attacks, the CICIDS 2017 contains recurrent features and null values. The X-IIoTID dataset includes new protocols, device behaviors, and attack types; however, it contains some null values. The CICIoT2023 dataset has modern scenarios of network attacks. It lacks other resources such as hosts and system logs. Choosing the best datasets for detecting cloud anomalies depends on the approach used. For instance, the timestamps characteristic is a primary feature for time series analysis, monitoring, and detecting anomalies in cloud networks. The following classes of cloud computing datasets should prioritize realism, recent attacks, a balanced ratio of benign instances to attacks, proper labeling, and all possible features.

4 A Review of Cloud Anomaly Detection Approaches

In this section, we examine current studies regarding the detection of anomalies in cloud networks, utilizing a variety of approaches, including machine learning, deep learning, statistical analysis, and hybrid methods.

4.1 Statistical Analysis-Based Approach

Statistical analysis enables cloud providers to identify anomalies in their cloud environment, allowing timely interventions and minimizing disruptions to ensure a secure and efficient service. The following are some of the significant works of this approach:

Wang et al**.** in [25] proposed a method to monitor cloud computing. The method is based on correlation analysis and predicting anomalies probability using principal component analysis (PCA). The method was evaluated using the TPC-W and Bench4Q datasets. Even though the approach improved the accuracy and detection delay, the technique yielded a high rate of false alarms.

Guigou et al. in [26] presented a system called SCHEDA, which mixes three algorithms to estimate Euclidean anomaly scores, for anomaly detection in a data cloud. These algorithms are employed to calculate the anomaly score for real-time handling. The author's experiment with a private dataset shows that SCHEDA outperforms other anomaly detection systems in real-time, processing data points without buffering, and providing low false alarms. However, the proposed method was not evaluated with well-known datasets.

Khatibzadeh et al. in [27] applied the catastrophe theory to detecting anomalies in cloud traffic. Because of the dynamic nature of the cloud, this theory works well at illustrating abrupt changes in the network using entropy as one of the control variables. The authors employed the DARA dataset to evaluate the efficacy of the catastrophe theory. Although the suggested approach achieved a superior detection rate and reduction in false positive rates, the proposed method requires more evaluation with well-known datasets.

Schmidt et al. in [28] presented an unsupervised anomaly detection approach in cloud networks based on online Autoregressive Integrated Moving Average (ARIMA). The approach was evaluated on a dataset powered by the OpenStack cloud environment. The results demonstrated excellent rates of detection and minimal false alarms. Nonetheless, the proposed method was not evaluated with realistic datasets and was not tested to detect different types of cloud anomalies.

Table 3 provides a summary of cloud anomaly detection techniques based on statistical analysis. It is noted that none of these techniques have been evaluated with new versions of cloud computing datasets or can detect anomalies in near real-time.

Table 3. A Summary of Approaches Based on Statistical Analysis

Ref.	Year	Methods	Strengths	Limitations	Datasets
[25]	2018	PCA	Near real-time detection. Minimal computing cost.	High-rate false alarms. Not detect all types of cloud anomalies.	TPC-W, Bench4Q datasets
[26]	2019	SCHEDA	Minimal computing cost. Near real-time detection.	Not evaluated with a well-known dataset. Not detect all types of cloud anomalies.	private datacenter dataset
[27]	2019	Catastrophe theory	Near real-time detection. Minimal computing cost.	Not evaluated with a well-known dataset. Not detect all types of cloud anomalies.	DARA dataset
[28]	2019	ARIMA	Near real-time detection. Minimal computing cost.	Not evaluated with a well-known dataset. Not detect all types of cloud anomalies.	OpenStack dataset

4.2 Machine Learning-Based Approach

Machine learning algorithms offer a sophisticated approach to detecting anomalies in vast data, here are some notable works of this approach.

Huang et al. in [29] suggested a Relaxed Linear Programming SVDD (RLPSVDD) method to overcome a significant false-positive rate in Support Vector Data Description (SVDD). The RLPSVDD works to create a flexible data description and then employs linear programming to identify anomalies in time series data. Although the RLPSVDD method has proven effective in identifying anomalies in cloud networks, it requires more effort to tune parameters.

Din et al. in [30] employ the Discrete Cosine Transform (DCT) to recognize, visualize, and classify attacks in these frames. This technique is based on taking network traffic data as a series of frames or videos and then using image-process techniques to classify different types of attacks in cloud computing. The presented technique efficiently detects anomalies when evaluated with the Abilene and GÉANT datasets, which demonstrates the effectiveness of using the proposed method to detect anomalies in cloud networks and identify hidden abnormal behavior. Nevertheless, the method did not support real-time detection.

Yasarathna et al. in [31] employed an Autoencoder and One-class Support Vector Machine (OCSVM) to pinpoint abnormalities in cloud network data. The evaluation of the proposed method with two datasets YAHOO and UNSW-NB15 demonstrated the performance of the OCSVM and Autoencoder. The results showed the Autoencoder outperformed the OCSVM. However, it is crucial to mention that the presented method was unable to identify various types of anomalies.

Islam et al. in [32] presented a cloud anomaly detection approach that relies on a gated recurrent unit autoencoder model which monitors multivariate time series data captured from cloud network traffic. The evaluation of proposed methods on the NAB dataset has proved its ability to detect anomalies. However, it exhibited a fairly low accuracy rate of 70%, and a false alarm rate was not discussed.

Ntambu et al. [33] introduced a proactive monitoring model aimed at detecting abnormalities in the cloud. Two machine learning techniques were employed in the model: isolation forest and OCSVM, which were trained and evaluated on a sampled workload trace. The evaluation reveals that the proposed model accounted for about 97% of the F1-score rate for hourly time-series data. However, the false alarm rate was not discussed.

Parameswarappa et al. in [34] employed machine learning tools to present a novel firewall strategy to enhance secure cloud-based computing. The proposed approaches predict the final categorization of attacks by merging historical node judgments with the current decision made by the machine learning algorithm, a technique referred to as the ‘most frequent decision. The proposed approach was evaluated using the UNSW-NB-15 dataset, achieving an accuracy and F1-score of 97.68%. However, it has incurred high computing costs.

Jiang et al. in [35] proposed an algorithm known as Adaptive Ensemble Random Fuzzy (AERF) to identify anomalies within cloud networks. AERF employs a random fuzzy rule-based approach to select samples randomly, enhancing the diversity of base classifiers and more effectively addressing disruptions arising from atypical data distributions. It leverages

fuzzy classifier ensembles, along with a dynamic weighting method, to enhance processing efficiency and abnormality detection precision. Experimental results used five benchmark datasets to demonstrate AERF's performance, achieving 99.9% accuracy and a 99.3% F1-score with the HTTP dataset. However, the proposed method did not discuss false alarm rates and required parameter tuning.

Table 4 shows a summary of cloud anomaly detection approaches based on ML algorithms. It is noted that none of these approaches showed their ability to detect cloud anomalies with low-rate false alarms.

Table 4. A Summary of Approaches Based on ML

Ref.	Year	Methods	Strengths	Limitations	Datasets
[29]	2017	RLPSVDD	Detect various anomalies. Low-rate false alarms.	Requires parameters tuning	Iris and Yahoo datasets
[30]	2018	DCT	Identify some types of cloud attacks.	The false alarm rate is not discussed. High computing cost.	Abilene and GÉANT datasets
[31]	2020	OCSVM and Autoencoder	Fast in parameter tuning.	Failed to Identify various anomalies. The false alarm rate is not discussed	UNSW-NB15 and Yahoo datasets
[32]	2020	GRU-based model	Low computing cost. Fast in parameters tuning	Failed to Identify various anomalies. The false alarm rate is not discussed	NAB dataset.
[33]	2021	OCSVM and RF	Fast in parameter tuning.	The false alarm rate is not discussed	A private dataset
[34]	2023	ML tools	Low-rate false alarms.	High computing cost. Requires parameters tuning	UNSW-NB-15 dataset
[35]	2023	AERF	Low computing cost. Identify various anomalies.	The false alarm rate is not discussed. Requires parameters tuning	SMD and EMOS Cloud Datasets

4.3 Deep Learning Based Approaches

Deep learning algorithms improve anomaly detection in cloud computing by learning complex patterns, enabling rapid response, mitigation, and cost-efficiency, and cultivating a secure, dependable, and cost-effective cloud environment. Below there are numerous notable works of this approach.

Saljoughi et al. in [36] proposed a novel method based on artificial intelligence techniques to detect anomalies in cloud networks. This approach uses multilayer perceptron neural networks for attack classification and implements the particle swarm algorithm to optimize and enhance classifier accuracy. To evaluate the performance of this proposed method, the NSL-KDD and KDD-CUP datasets were employed. The results of the evaluation yielded a 99.4% accuracy rate with KDDcup99 and 98.08% with NSL-KDD. However, it is worth noting that the proposed method requires parameter tuning.

Zhu et al. in [37] introduced the LogNL technique, which finds abnormalities in cloud platform logs. The fundamental components of LogNL are long-short-term memory (LSTM) and natural language processing (NLP). The NLP is applied to extract the feature vector from each log template and embed the semantic information of the login into the vector. Then LSTM uses the feature vector for anomaly detection. The evaluation with HDFS and OpenStack datasets achieves 98.4% accuracy and a 97.7% F1 score. However, it is worth noting that the proposed method requires parameter tuning.

Girish et al. in [38] utilized stacked and bidirectional LSTM to detect cloud abnormalities from time-series textual records. The suggested technique comprises three units: a data gathering unit, a data preprocessing unit, and an anomaly detection unit. The suggested model achieved 94.61% detection accuracy when evaluated on data gathered from the OpenStack environment. Once again, the presented technique demands parameter tuning.

Khalaf et al.in [39] introduced a method based on graph-based layer-driven learning (GLLD). Separately, the agent executes a graph-based, layered learning-driven (GLLD) network in a cooperative domain, considering the connections between various parts of the cloud network. The evaluation of the presented approach with the Code Red worm attack dataset and the BoT IoT dataset achieved 91.0% accuracy with various traffic allotments. However, it failed to detect various kinds of anomalies.

Song et al. in [40] suggested a method based on deep learning for cloud anomaly detection. The approach examines the correlations between attributes and time in multivariate time series. First, work to capture connections between nodes using parallel graph neural networks. Then it improved the accuracy of anomaly detection by using multi-head self-attention and

GRU mechanisms. The proposed method has been evaluated using the Server Machine Dataset (SMD), gaining a precision of 83.9% and an F1-score of 85.3%. However, it required parameter tuning.

Table 5 shows a summary of different deep learning techniques to detect anomalies in cloud computing. It is noted that none of these approaches have been evaluated with new versions of cloud computing datasets.

Table 5. A Summary of Approaches Based on Deep Learning

Ref.	Year	Methods	Strengths	Limitations	Datasets
[36]	2017	MLP	Detect various kinds of attacks. Low-rate false alarms.	Requires parameter tuning. Not dependent on both physical and virtual features.	NSL-KDD and KDD-CUP datasets
[37]	2020	NLP+LSTM	Detect various anomalies. Low-rate false alarms.	Requires parameter tuning. Not dependent on both physical and virtual features.	HDFS and OpenStack datasets
[38]	2021	LSTM	Handle the distributed nature of the cloud. Dependent on both physical and virtual features.	Requires parameter tuning. Has a remarkable false alarm rate. Not detect various kinds of anomalies.	OpenStack dataset
[39]	2022	Graph-Based Model	Low-rate false alarms. Fast in parameter tuning.	Not dependent on both physical and virtual features Not detect various kinds of anomalies.	BoT IoT Code Red worm attack datasets
[40]	2023	(CGNN-MHSA-AR)	Identify the anomaly source.	Not detect various kinds of anomalies. Low False alarm rate.	Server Machine Dataset

4.4 Hybrid Method Based Approached

Garg et al. in [41] introduced a novel model called “HyClass” for cloud abnormality detection. The system starts with preprocessing and feature selection using the Boruta algorithm. Then it categorizes characteristics into significant and non-significant based on the Z-score value. The features are then given as input to the suggested hybridized classification approach using differential evolution (DE), support vector machines (SVM), and chaotic optimization (CO). The evaluation of the HyClass scheme with the KDD'99 dataset achieved 99.42% accuracy. The results show that the introduced technique efficiently identifies abnormalities in real-time scenarios. However, it has a high rate of false alarms.

Ding et al. in [42] introduced a real-time detection method called RADM that detects anomalies in multivariate time series data based on hierarchical temporal memory (HTM) and Bayesian networks (BN). The HTM is used to detect anomalies, and the BN is utilized for validation. The evaluation of the proposed method with the NAB dataset achieved 77% accuracy. However, it has a high rate of false alarms.

Lou et al. [43] presented an approach based on distance and support vector data description named Max-Min for anomaly detection in cloud systems. Several features that were taken from cloud components, like network traffic, CPU consumption, memory usage, and others, are captured to detect anomalies. The proposed method of evaluation with ten monitored servers achieved a 95.0% accuracy rate. However, the false alarm rate was not discussed.

Yang et al. in [44] Suggested a novel method for anomaly detection in cloud network traffic. The proposed method was based on a hybrid information entropy of network traffic features. After normalizing features, Support Vector Machines (SVM) is exploited to detect anomalous network behaviors. The evaluation of the suggested technique with the KDDcup99 and NSL-KDD datasets achieved about 95.1% accuracy in both datasets. However, it has a significant rate of false alarms.

Chiba et al. in [45] proposed a novel method called ANIDS BPNN-IGA for cloud anomaly detection using BPNN and IGA in a cloud environment. Firstly, the authors employed a backpropagation neural network (BPNN) to detect anomalies. Then IGA is used to find optimal values for learning rate and momentum, ensuring a high detection degree, accuracy, and low rate of false alarms. The evaluation of the presented technique on the DARPA_KDD dataset achieved 99.96% accuracy and a 99.9% F1 score. However, the suggested method requires parameter tuning.

Zhang et al. in [46] Active Transfer Anomaly Detection (ATAD) is a cross-dataset anomaly detection that detects abnormalities in an unlabeled dataset. To overcome the challenge of obtaining sufficient labeled data for cloud monitoring amidst high volumes and distributed areas. This method combines active learning and transfer learning techniques to selectively label only a limited number of samples from the target dataset. The evaluation of ATAD with the NAB and Yahoo datasets achieved about 99.2% F1-score. However, the proposed method failed to identify types of anomalies.

Yu et al. [47] introduced an anomaly detection method based on the behavioral characteristics of time series networks. The framework has two parts: the DBN-BiGRU algorithm model and the preprocessing scheme. This scheme prepares feature analysis files for use by the DBN-BiGRU algorithm by converting them into time-series records. The structure uses past and future time-series data for anomaly detection. When evaluating the proposed framework's performance on the CICIDS2017 dataset, results show a precision of 99.82% and an F1-score of 99.81%. However, a false alarm rate was not discussed.

Lalotra et al. in [48] presented a technique named an Intelligent Real-Time Anomaly Detection System (iReTADS) for anomaly detection in cloud data. The method employs a data summarization strategy to decrease network traffic and improve network security via a robust real-time neural network. The suggested technique earned a 98.9% detection accuracy when tested on the KDD Cup 99 dataset. However, a false alarm rate was not discussed.

Table 6 shows an overview of cloud anomaly detection techniques using hybrid procedures, indicating that none of these techniques proved the ability to detect various types of abnormalities with a low rate of false alarms.

Table 6. Summaries of Approaches Based on Hybrid Methods

Ref.	Year	Methods	Strengths	Limitations	Datasets
[41]	2018	HyClass	Near real-time detection.	High-rate false alarms. Not detect various kinds of anomalies.	TU and KDD'99 datasets
[42]	2018	RADM	Near real-time detection. Dependent on both physical and virtual features.	High-rate false alarms. Not detect various kinds of anomalies.	NAB dataset
[43]	2019	MMD -SVDD	Near real-time detection. Handle the distributed nature of the cloud. Low computing cost.	False alarm rate is not discussed	Private dataset
[44]	2019	SVM	Identify the anomaly source	High-rate false alarms. Not detect various kinds of anomalies.	KDDcup99, and NSL-KDD datasets
[45]	2019	ANIDS BPNN-IGA	Near real-time detection. Low False alarm rate. Handle the distributed nature of the cloud.	Requires parameter tuning. High computing cost.	DARPA and KDD datasets
[46]	2019	ATAD	Dependent on both physical and virtual features. Handle the distributed nature of the cloud.	Not detect various kinds of anomalies. Not Identify the anomaly source.	NAB and Yahoo datasets
[47]	2020	DBN-BiGRU	Identify the anomaly source. Detect various kinds of anomalies.	Requires parameter tuning. High computing cost.	CICIDS2017 dataset
[48]	2022	iReTADS	Near real-time detection.	False alarm rate is not discussed.	KDDCup99

5 Challenges and Essential Criteria for Future Solutions of Cloud Anomaly Detection

Detecting anomalies in cloud networks is a critical challenge for researchers and network operators. This is due to several factors, including the large volume of traffic, continuous data streams, the need for timely detection, and multi-phase attacks. Below are some of the challenges faced by anomaly detection approaches:

- Real-time detection in cloud computing faces challenges like quick data analysis, scalability, achieving high accuracy, and adapting to infrastructure changes [25].
- Identifying the source of an anomaly poses significant challenges. When an anomaly is detected within a multivariate time series, it is often difficult to quickly pinpoint the specific component responsible for the anomaly [31].
- Managing the distributed nature of the cloud presents challenges such as coordinating and controlling resources spread across geographically dispersed data centers [48].
- Techniques for anomaly detection in cloud computing face complex challenges, including integrating and analyzing data from both virtual and physical aspects with robustness and accuracy in identifying dependencies across both virtual and physical cloud aspects [39].
- Detecting cloud anomalies, like point, contextual, and collective types in time series data, presents unique challenges due to their varying characteristics and patterns, necessitating versatile detection systems [33].
- The dynamic nature of cloud environments adds complexity consequently, conserving system resources in cloud anomaly detection requires optimized algorithms [48].
- The availability of effective datasets is a challenge for proposed approaches to achieving effective cloud anomaly detection models [39].
- Many false alarms in cloud anomaly detection present a significant challenge, impeding the ability to identify anomalies accurately and reliably in cloud computing [41].

We have reviewed a variety of systems, methods, and tools with diverse functionalities for the identification of anomalies in cloud environments. To provide a concise overview, we now offer a comparative summary between these techniques in terms of real-time detection, identifying the source of the anomaly, handling the distributed nature of the cloud, dependency on both virtual and physical cloud attributes, detecting various types of cloud anomalies, conserving system resources, cost-effective training, and low-rate false alarms, which are essential criteria. Table 7 shows that none of these approaches possesses all these capabilities.

Table 7. Reviewed Works and Essential Criteria of Cloud Anomaly Detection

CR1: real-time detection, CR2: identifying source of the anomaly, CR3: handling the distributed nature of the cloud., CR4: dependency on both virtual and physical cloud attributes, CR5: detecting various type of cloud anomalies, CR6: conserving system resources., CR7: cost-effective training, CR8: low-rate false alarms.					
Work	**Year**	**Criteria**	**Work**	**Year**	**Criteria**
[29]	2017	C5, C8	[31]	2020	CR2
[36]	2017	C4	[32]	2020	CR6, CR7
[25]	2018	CR1, CR6, CR8	[37]	2020	CR3, CR5
[30]	2018	C5, C6	[47]	2020	CR2, CR5
[41]	2018	CR6, CR7, CR8	[38]	2021	CR3, CR4, CR8
[42]	2018	CR1, CR4, CR5, CR8	[33]	2021	CR5
[26]	2019	CR1, CR4, CR5, CR6	[39]	2022	CR3, CR4, CR5, CR7, CR8
[27]	2019	CR1, CR4, CR5, CR6, CR8	[48]	2022	CR1, CR3
[28]	2019	CR1, CR2, CR4	[34]	2023	CR5, CR7, CR8
[44]	2019	C2	[35]	2023	CR5, CR6
[46]	2019	C3, C4, C8	[40]	2023	CR2
[43]	2019	CR1, CR3, CR4, CR6			
[45]	2019	CR1, CR3, CR4, CR5, CR8			

6 Conclusion

Cloud computing offers measurable service, quick flexibility, resource pooling, wide network connectivity, and on-request self-service. Detecting anomalies in cloud networks is crucial for enhancing security, protecting critical infrastructure, improving performance, ensuring compliance, and constantly monitoring the system. Anomaly detection methods provide cloud service providers and users with the means to strengthen the security of cloud environments and mitigate potential risks and vulnerabilities associated with cloud computing.

This literature review provides a comprehensive overview of the significant advancements made in anomaly detection within cloud networks that employ various strategies for anomaly detection. Furthermore, the review identifies commonly used public datasets for evaluation purposes. It also introduces some important standards for future solutions in cloud anomaly detection and highlights a variety of interesting open issues and challenges. In future work, we plan to add more datasets and extend essential criteria for future solutions to cloud anomaly detection.

References

1. A. Sunyaev and A. Sunyaev, “Cloud computing,” Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies, pp. 195–236, 2020.
2. N. J. Piscataway, “Artificial Intelligence and Machine Learning, Cloud Computing, and 5G Will Be the Most Important Technologies in 2022, Says New IEEE Study,” IEEE, 2021.
3. M. Frederick, “Risk of Cloud Breaches Rising, Teams Struggling to Address Them, Fugue and Sonatype Survey Finds,” Fugue and Sonatype, 2021. Accessed: Nov. 14, 2023. [Online]. Available: https://www.fugue.co/press/releases/risk-of-cloud-breaches-rising-teams-struggling-to-address-them-fugue-and-sonatype-survey-finds
4. S. B. Sadkhan, “Security of Cloud Networks–Status, Challenges and Future Trends,” in 2022 8th International Engineering Conference on Sustainable Technology and Development (IEC), IEEE, 2022, pp. 247–252.
5. S. M. Alturfi, B. Al-Musawi, and H. A. Marhoon, “An advanced classification of cloud computing security techniques: A survey,” in AIP Conference Proceedings, AIP Publishing, 2020.

6. L. Erhan et al., “Smart anomaly detection in sensor systems: A multi-perspective review,” Information Fusion, vol. 67, pp. 64–79, 2021.
7. P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.
8. W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing,” 2011.
9. E. Geetha Rani and D. T. Chetana, “A Survey of Recent Cloud Computing Data Security and Privacy Disputes and Defending Strategies,” in Congress on Smart Computing Technologies, Springer, 2023, pp. 407–418.
10. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A systematic literature review on cloud computing security: threats and mitigation strategies,” IEEE Access, vol. 9, pp. 57792–57807, 2021.
11. D. Moore, C. Shannon, and K. Claffy, “Code-Red: a case study on the spread and victims of an Internet worm,” in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, 2002, pp. 273–284.
12. K. D. D. Cup, “Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html.” Ocotber, 2007.
13. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in 2009 IEEE symposium on computational intelligence for security and defense applications, Ieee, 2009, pp. 1–6.
14. A. Lavin and S. Ahmad, “Evaluating real-time anomaly detection algorithms--the Numenta anomaly benchmark,” in 2015 IEEE 14th international conference on machine learning and applications (ICMLA), IEEE, 2015, pp. 38–44.
15. N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in 2015 military communications and information systems conference (MilCIS), IEEE, 2015, pp. 1–6.
16. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization.,” ICISSp, vol. 1, pp. 108–116, 2018.
17. M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, “Flow-based benchmark data sets for intrusion detection,” in Proceedings of the 16th European conference on cyber warfare and security. ACPI, 2017, pp. 361–369.
18. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset,” Future Generation Computer Systems, vol. 100, pp. 779–796, 2019.
19. A. Aldribi, I. Traore, and B. Moa, “Data sources and datasets for cloud intrusion detection modeling and evaluation,” Cloud computing for optimization: foundations, applications, and challenges, pp. 333–366, 2018.
20. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,” in 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, 2019, pp. 1–8.
21. A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, “TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems,” Ieee Access, vol. 8, pp. 165130–165150, 2020.
22. F. Lomio, D. M. Baselga, S. Moreschini, H. Huttunen, and D. Taibi, “Rare: a labeled dataset for cloud-native memory anomalies,” in Proceedings of the 4th ACM SIGSOFT International Workshop on Machine-Learning Techniques for Software-Quality Evaluation, 2020, pp. 19–24.
23. M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, “X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things,” IEEE Internet Things J, vol. 9, no. 5, pp. 3962–3977, 2021.
24. E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment,” 2023.
25. T. Wang, J. Xu, W. Zhang, Z. Gu, and H. Zhong, “Self-adaptive cloud monitoring with online anomaly detection,” Future Generation Computer Systems, vol. 80, pp. 89–101, 2018.
26. F. Guigou, P. Collet, and P. Parrend, “SCHEDA: Lightweight euclidean-like heuristics for anomaly detection in periodic time series,” Appl Soft Comput, vol. 82, p. 105594, 2019.
27. L. Khatibzadeh, Z. Bornaee, and A. Ghaemi Bafghi, “Applying catastrophe theory for network anomaly detection in cloud computing traffic,” Security and Communication Networks, vol. 2019, 2019.
28. F. Schmidt, F. Suri-Payer, A. Gulenko, M. Wallschläger, A. Acker, and O. Kao, “Unsupervised anomaly event detection for cloud monitoring using online arima,” in 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), IEEE, 2018, pp. 71–76.
29. C. Huang, G. Min, Y. Wu, Y. Ying, K. Pei, and Z. Xiang, “Time series anomaly detection for trustworthy services in cloud computing systems,” IEEE Trans Big Data, vol. 8, no. 1, pp. 60–72, 2017.
30. M. F. Din and S. Qazi, “A compressed framework for monitoring and anomaly detection in cloud networks,” in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, 2018, pp. 1–7.

31. T. L. Yasarathna and L. Munasinghe, “Anomaly detection in cloud network data,” in 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), IEEE, 2020, pp. 62–67.
32. M. S. Islam and A. Miranskyy, “Anomaly detection in cloud components,” in 2020 IEEE 13th international conference on cloud computing (CLOUD), IEEE, 2020, pp. 1–3.
33. P. Ntambu and S. A. Adeshina, “Machine learning-based anomalies detection in cloud virtual machine resource usage,” in 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), IEEE, 2021, pp. 1–6.
34. P. Parameswarappa, T. Shah, and G. R. Lanke, “A Machine Learning-Based Approach for Anomaly Detection for Secure Cloud Computing Environments,” in 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), IEEE, 2023, pp. 931–940.
35. J. Jiang et al., “AERF: Adaptive ensemble random fuzzy algorithm for anomaly detection in cloud computing,” Comput Commun, vol. 200, pp. 86–94, 2023.
36. A. S. Saljoughi, M. Mehrvarz, and H. Mirvaziri, “Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms,” Emerging Science Journal, vol. 1, no. 4, pp. 179–191, 2017.
37. B. Zhu, J. Li, R. Gu, and L. Wang, “An approach to cloud platform log anomaly detection based on natural language processing and lstm,” in Proceedings of the 2020 3rd International Conference on Algorithms, Computing and Artificial Intelligence, 2020, pp. 1–7.
38. L. Girish and S. K. N. Rao, “Anomaly detection in cloud environment using artificial intelligence techniques,” Computing, vol. 105, no. 3, pp. 675–688, 2023.
39. O. I. Khalaf, K. A. Ogudo, and S. K. B. Sangeetha, “Design of graph-based layered learning-driven model for anomaly detection in distributed cloud IoT network,” Mobile Information Systems, vol. 2022, pp. 1–9, 2022.
40. Y. Song, R. Xin, P. Chen, R. Zhang, J. Chen, and Z. Zhao, “Identifying performance anomalies in fluctuating cloud environments: A robust correlative-GNN-based explainable approach,” Future Generation Computer Systems, vol. 145, pp. 77–86, 2023.
41. S. Garg, K. Kaur, N. Kumar, S. Batra, and M. S. Obaidat, “HyClass: Hybrid classification model for anomaly detection in cloud environment,” in 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–7.
42. N. Ding, H. Gao, H. Bu, and H. Ma, “RADM: Real-time anomaly detection in multivariate time series based on Bayesian network,” in 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE, 2018, pp. 129–134.
43. P. Lou, Y. Yang, and J. Yan, “An anomaly detection method for cloud service platform,” in Proceedings of the 2019 4th International Conference on Machine Learning Technologies, 2019, pp. 70–75.
44. C. Yang, “Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment,” Cluster Comput, vol. 22, pp. 8309–8317, 2019.
45. Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida, “New anomaly network intrusion detection system in cloud environment based on optimized back propagation neural network using improved genetic algorithm,” International Journal of Communication Networks and Information Security, vol. 11, no. 1, pp. 61–84, 2019.
46. X. Zhang et al., “Cross-dataset time series anomaly detection for cloud systems,” in 2019 USENIX Annual Technical Conference (USENIX ATC 19), 2019, pp. 1063–1076.
47. X. Yu, T. Li, and A. Hu, “Time-series network anomaly detection based on behaviour characteristics,” in 2020 IEEE 6th International Conference on Computer and Communications (ICCC), IEEE, 2020, pp. 568–572.
48. G. S. Lalotra, V. Kumar, A. Bhatt, T. Chen, and M. Mahmud, “iReTADS: an intelligent real-time anomaly detection system for cloud communications using temporal data summarization and neural network,” Security and Communication Networks, vol. 2022, pp. 1–15, 2022.