REVIEW Open Access

A systematic literature review on intrusion detection techniques in cloud computing

Shamma Shabnam Nasim[1], Prashant Pranav[1*] and Sandip Dutta[1]

*Correspondence:
Prashant Pranav
prashantpranav19@gmail.com
[1]Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Jharkhand, India

Abstract
Intrusion Detection and Prevention Systems (IDPS) play a key role in protecting networks by keeping an eye out for suspicious activity, spotting threats, and taking action to stop them. These systems were originally designed for traditional, fixed networks, but they struggle to keep up with the fast-paced and constantly changing nature of cloud computing environments. Cloud computing has revolutionized technology, bringing many innovations in how organizations operate. Organizations rely heavily on the use of cloud storage to store and retrieve their sensitive data. Security issues in the cloud computing environment are a big challenge as, despite various protection measures, the cloud environment is vulnerable to security threats. Intrusion Detection and Prevention System (IDPS) is a significant component in securing the cloud environment against emerging threats in cyber-attacks. This paper takes a close look at intrusion detection systems (IDS) that are specifically built for cloud computing. The cloud brings its own set of challenges like constantly changing resources, sharing space between many users, and limited visibility into all the network traffic. Unlike traditional IDS that work in fixed, local networks, cloud-based IDS have to handle traffic that moves between virtual machines and scale up or down quickly. Cloud computing has transformed over time, improving access to scalability while offering vulnerabilities that increase the probability of intrusion or attacks. This review addresses these research gaps by comprehensively surveying state-of-the-art IDPS techniques tailored for cloud computing environments. IDPS is further classified into different categories, such as signature-based, anomaly-based, and hybrid-based. Recently, combining Machine Learning (ML) and Deep Learning (DL) with Intrusion Detection Systems (IDS) has shown to be very effective, as it allows for more precise detection and large-scale use. However, notable challenges include small dataset sizes, imbalanced datasets, and high expenses. These challenges mainly focus on creating adaptive systems that identify intrusions in real time. To tackle this, attention is directed towards ensemble learning and edge computing. The outcomes of these initiatives are being used to create a strong and efficient IDS that fits well with the changing nature of cloud environments. This survey provides a comprehensive analysis of current IDPS methodologies and future perspectives, aiming to contribute to developing robust and efficient cloud security solutions.

Keywords Intrusion detection system, Cloud computing, Machine learning, Deep learning, Cyber security, Cyber security datasets

1 Introduction

Cloud computing has become an integral part of modern IT infrastructure, enabling scalable and on-demand services. However, this transformation also introduces new security challenges, particularly around protecting data and infrastructure from sophisticated cyber threats. This technical revolution has presented amazing possibilities for networking, communication, teamwork, and simple access to far-off equipment. Now, storing and accessing data is simple whether you use a computer, cell phone, or another electronic device. People, businesses, entrepreneurs, and government agencies fervently embrace this changing digital terrain. However, with this significant development, there is also a great responsibility [1]. The internet-based character of cloud computing technology raises the possibility of intrusion and malicious attacks exploiting fresh vulnerabilities created by the change from the traditional and generally used methods of storing, processing, and accessing data, information, and communication in the new environment. Studies reveal that the development of numerous modern technologies, including online services, web browsers, and virtualization, has partly helped to drive cloud-based systems. Therefore, every intrusion, threat, or attack connected to these technologies also affects the cloud; they could be quite more detrimental in this context [2]. Thus, one may define “cloud computing” as “an emerging technology that provides on-demand computing resources and services via the internet”. Built on the Internet, this platform handles data processing, storage, and resource exchange encompassing corporate procedures, software, infrastructure, and applications [3].

The National Institute of Standards and Technology’s (NIST) NIST Special Publication 800 – 145 [4] defines “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction”. There are five fundamental components to this cloud paradigm, three distinct service models, and four different deployment approaches. Figure 1 shows the framework of cloud computing.

The cloud computing paradigm has a service-oriented design that has significantly transformed the provision and management of services. The architecture is three-tiered, including infrastructure, platform, and applications as a service, with each layer being vulnerable to security flaws in its own right. Attackers can compromise the availability, integrity, and confidentiality of resources, data, and virtualized infrastructure included within cloud computing systems. This could result in the introduction of new attack vectors. The issue may escalate and become more severe when a cloud with substantial storage capacity and computational power is compromised by intruders operating inside the cloud environment. Intrusion detection systems (IDS) work within fixed and clearly defined boundaries in traditional network environments. The patterns of user behavior, system configurations, and traffic flow are relatively stable and predictable, which makes it easier to spot unusual activity. However, cloud computing changes that picture completely. Cloud platforms are highly dynamic they scale up and down on demand, rely heavily on virtual machines, and often host multiple users on shared infrastructure.

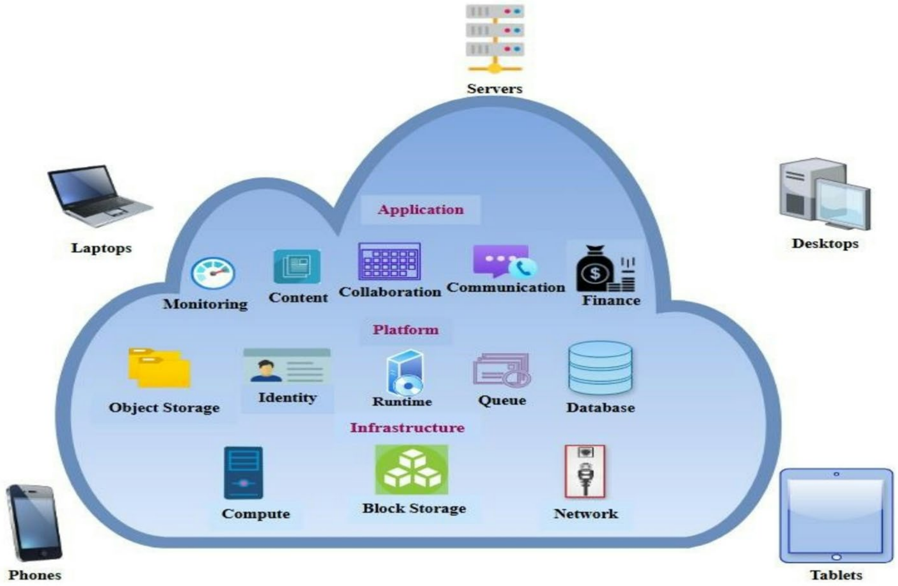

Fig. 1 Architecture of Cloud Computing

Traffic can move internally between virtual systems (so-called east-west traffic), which is harder to monitor using conventional tools. These complexities mean that traditional IDS approaches often fall short. To be effective in the cloud, IDS must be explicitly designed for this environment, with the ability to adapt to constant changes and detect threats that may not even appear in legacy systems.

Moreover, the use of hypervisors and virtual machines in the cloud introduces security vulnerabilities, such as DDoS assaults, due to their susceptibility to attacks at the virtual machine or hypervisor level inside the IaaS framework. In 2017, Equifax, a U.S.-based consumer, had an identity theft incident that affected 145.5 million consumers in the United States. The incident was caused by a cyberattack that was carried out against a credit reporting organization [5]. The hackers stole personally identifying information from consumers, such as their names, social security numbers, and birth dates, but they did not leave any trace of their illegal behavior behind. This incident is regarded as one of the most significant breaches in history, resulting in a loss of $275 million for the corporation. Consequently, in the current age of cyber criminals, it is essential to fortify the system to safeguard resources, infrastructure, and critical data from threats [6]. In cloud computing, the Intrusion Detection System is a crucial component in ensuring the protection of client data and resource assets from potential security breaches. It is a sophisticated security solution designed to safeguard network data from harmful actions [7]. It must be meticulously built and aligned with the characteristics of cloud computing since it differs fundamentally from conventional computer systems. It must also effectively identify cloud-specific threats. Cloud system security presents a significant problem, including a combination of policies, technologies, and procedures to safeguard data, services, and infrastructure. Consequently, the vulnerabilities increase as a result of this amalgamation. Data on the cloud is outsourced to either trustworthy or untrusted service providers, compromising client privacy [8].

Despite the growing number of cloud-based IDS solutions, a significant gap remains in evaluating the practical applicability of machine learning (ML) and deep learning (DL) based hybrid Intrusion Detection and Prevention Systems (IDPS). Many existing surveys fail to assess these systems concerning their adaptability to real-time, evolving threats and the limitations of available datasets.

To address these gaps, this study conducts a comprehensive systematic literature review of cloud-based IDPS, with a focus on ML and DL techniques. The research question is: *How do ML/DL models improve detection accuracy compared to traditional IDPS methods in cloud environments?*

The major contribution of this article is outlined as follows:

- *Evaluates* the effectiveness of ML/DL hybrid models in detecting cloud-specific security threats.
- *Classifies* IDS approaches based on their detection techniques, deployment strategies, and compatibility with cloud environments.
- *Analyzes* the suitability and limitations of commonly used datasets for training and evaluating cloud-based IDS.
- *Identifies* open challenges and proposing future directions for adaptive IDPS frameworks in cloud computing environments.

This review bridges this gap by evaluating adaptive IDPS frameworks for evolving threats. This study primarily focuses on a comprehensive evaluation of Intrusion Detection Systems (IDS) based on their detection methodologies within cloud computing environments. Specifically, it seeks to explore how these systems detect and mitigate emerging security threats. The primary research question guiding this investigation is: How do ML/DL models improve detection accuracy compared to traditional IDPS?

The remainder of this paper is structured as follows: Sect. 2 discusses the methods used to identify and analyze the literature. Section 3 presents an overview of cloud-based intrusion detection. Section 4 describes various IDS methods, categorized into techniques and applications. Section 5 outlines the assessment criteria and datasets commonly used in IDS research. Section 6 highlights the challenges and outstanding issues in the field. Section 7 suggests future research directions. Section 8 concludes the study.

2 SLR methodology

This section outlines a systematic literature review (SLR) process designed to locate, analyze, and synthesize relevant information from emerging research areas. It covers published journal articles from 2017 to 2024 and describes four fundamental processes: formulating a search strategy, establishing selection criteria for research, conducting data extraction, and evaluating the quality of the included studies. The SLR is organized into four steps, as shown in Fig. 2 below.

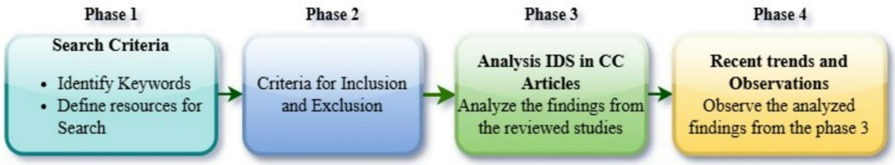
Phase 1
Search Criteria
Identify Keywords
Define resources for Search
Phase 2
Criteria for Inclusion and Exclusion
Phase 3
Analysis IDS in CC Articles
Analyze the findings from the reviewed studies
Phase 4
Recent trends and Observations
Observe the analyzed findings from the phase 3

Fig. 2 The Article Selection Criteria

Establishing selection criteria for research, conducting data extraction, and evaluating the quality of the included studies. The SLR is organized into four steps, as shown in Fig. 2 below.

2.1 Phase 1: search criteria

We selected Google Scholar, Web of Science, and Science Direct as our search engines due to their capabilities to investigate all identified databases. We crafted a search query using relevant keywords for our research. The databases will be searched for the following keywords related to Intrusion Detection Systems (IDS) in Cloud Computing: 'anomaly,' 'intrusion detection system,' 'Cloud Computing,' 'Cloud Security,' 'Machine Learning,' 'Deep Learning,' 'Intrusion Detection,' 'Hybrid IDS,' and 'Cloud Environments,' covering the years from 2017 to 2024. These keywords serve as the most appropriate guidelines for this domain.

2.2 Phase 2: study selection process

To conduct our systematic review, we initially retrieved 577 documents using Google Scholar based on the research title. We focused on journal and conference papers published between 2017 and 2024, targeting studies that explore intrusion detection in cloud computing from various perspectives. Key databases and publishers used for this search included Springer, Elsevier, IEEE Xplore, and Google Scholar. To ensure the relevance and quality of selected studies, we defined specific inclusion and exclusion criteria. The inclusion criteria targeted peer-reviewed publications written in English that explicitly addressed intrusion detection systems (IDS) within the context of cloud computing. Eligible studies included original research featuring case studies, simulations, or empirical evaluations; proposals of novel IDS approaches (e.g., machine learning, deep learning, or hybrid techniques); performance assessments using appropriate metrics; and detailed methodological and technical descriptions. We also considered studies discussing real-world implementation, deployment challenges, and future research directions in IDS for cloud environments.

Conversely, exclusion criteria were applied to eliminate studies not directly aligned with our research objectives. We excluded papers that focused on general network security without specific emphasis on IDS in cloud computing, as well as duplicate publications, papers lacking sufficient methodological detail, non-English publications, and studies published prior to 2017.

After applying the above criteria and removing duplicates, 170 studies were selected for in-depth analysis.

2.3 Phase 3: data collection

To effectively extract data for IDS in cloud computing, it is essential to gather specific details from each study, including the author (s) and year of publication, and the type of research conducted (review, empirical study, simulation, theoretical analysis, reviewer meta-analysis). Additionally, it is essential to note the type of cloud environment involved (public, private, or hybrid) and the IDS techniques utilized (signature-based, anomaly-based, or hybrid). Furthermore, key findings including performance metrics such as accuracy, false positive rate, and scalability. Evaluation methods and datasets used (NSL-KDD, CICIDS2017, UNSW-NB15).

These data points were essential for categorizing and comparing the studies, identifying trends, and assessing the practical effectiveness of various IDS approaches within cloud environments.

2.4 Phase 4: synthesis and analysis

In the final phase 115 paper included in qualitative synthesis, we analysis systematically categorized intrusion detection system (IDS) techniques based on three key dimensions: detection methodology (signature-based, anomaly-based, and hybrid), deployment type (network-based, host-based, hypervisor-based, and distributed), and technology layer (machine learning-based, deep learning-based, and traditional rule-based systems). Within each category, representative studies were critically examined to highlight their technical contributions, limitations, and comparative performance.

Although benchmark datasets play a critical role in facilitating consistent evaluation and comparison of IDS techniques, they often lack the complexity and dynamic nature inherent in real-world production environments. In operational cloud settings, intrusion detection systems must contend with evolving threat landscapes, unlabeled and imbalanced data, and system-specific behaviors typically absent from standardized datasets. To enhance the practical applicability of IDS solutions, future research should focus on developing adaptive learning models capable of fine-tuning on live or proprietary data streams, and explore transfer learning approaches to improve generalization across diverse cloud infrastructures.

3 An overview of cloud based intrusion detection system

This section classifies and analyses various intrusion detection attacks and intrusion detection types. In this work, we have classified IDS techniques based on their types and attacks.

3.1 Cloud-based IDS attack

An intrusion may be defined as anything that potentially cause damage to a system or network. The most prevalent cloud-related attacks are listed below in the following sub section.

3.1.1 Virtual machine attacks

Attackers compromise the hypervisor to take over virtual computers. SubVir, BLUEPILL, and DKSM, which let hackers run the host over the hypervisor are the main attacks aimed against the virtual layer. Zero-day vulnerabilities in virtual machines can be readily used by attackers to get access, hence possibly compromising multiple websites kept on virtual servers [9].

3.1.2 User-to-root (U2R) attacks

The attacker may hack a password to get access to a legitimate user's account, allowing him to collect information about the system by exploiting weaknesses. This assault violates the integrity of cloud-based systems.

3.1.3 Insider attacks

The threat of insiders knowing the whereabouts of an organization has remained a prominent challenge in government as well as the private sectors. Vigilant permission management is clearly important since the attackers may be authorized users attempting to use their given rights or those denied to them [10].

3.1.4 Denial of service (DoS) attacks

In cloud computing, attackers may inundate virtual machines with excessive requests, rendering them inaccessible to legitimate users, a phenomenon known as a DoS assault. This assault aims to compromise the accessibility of cloud resources. Intrusion Detection Systems (IDSs) are critical techniques, whether software or hardware-based, used to identify and prevent intrusions on computer systems. Sensors, consoles, and a central engine are some of the components of these systems. Sensors identify security events, and the console monitors these events in real-time. The central engine stores the events captured by the sensors in a database and uses a set of predefined rules to produce alerts depending on detected security incidents. The essential function of IDSs is to monitor and detect any unauthorized or malicious activity carried out by connected nodes or users that might imperil system resources. By keeping a close eye on user applications, networks, or their combinations, IDSs strive to identify both known and undiscovered attacks, thereby improving system security. Intrusion detection systems offer the following essential features [11]:

- *Monitoring and analyzing user activity*: IDSs continually monitor and analyze user behaviors to detect any unusual or suspicious behavior that might signal a security threat. *Auditing system configuration and vulnerabilities*: To find any flaws or incorrect settings that an attacker may exploit, intrusion detection systems (IDSs) regularly audit system configurations and vulnerabilities.
- *Evaluating the integrity of data files and critical systems*: IDSs assess the integrity of crucial systems and data files by comparing their present state to a predefined baseline and issuing alerts if any deviations are discovered.
- *Examining operating system activity*: Intrusion detection systems (IDSs) examine operating system activity to find any irregularities or illegal activity that might indicate a security breach.

Intrusion detection involves monitoring events inside a computer system or network and evaluating them for indications of intrusions, which are defined as efforts to undermine confidentiality, integrity, or availability or to circumvent the security systems of a computer or network. Intrusions occur when attackers access systems over the Internet, when authorized users seek to get unauthorized rights, or when approved users abuse their granted privileges. Intrusion Detection Systems (IDS) are software or hardware solutions that automate the monitoring and analyzing processes [12].

3.2 Monitoring data sources and feature selection in cloud IDS

In cloud environments, the effectiveness of IDS and IPS systems heavily depends on the type of monitoring data available and how it's collected. Unlike traditional on-premises solutions, cloud-based IDS often draws from a wide range of data sources, such as virtual machine logs, cloud storage access records, API call logs, authentication logs, network flow data (like AWS VPC Flow Logs or Azure NSG Logs), and even telemetry from the hypervisor layer. Monitoring can be done by installing agents directly on virtual machines, containers, or serverless functions or by deploying passive probes within the cloud provider's virtual network infrastructure. The choice between agents or network-based probes plays a significant role in what you can see, the latency introduced, and the types of threats you can detect. Agent-based systems typically offer more profound insight into operating system-level activities. At the same time, network probes provide broader visibility into traffic moving between services often called east-west traffic [13].

When applying machine learning or deep learning techniques in cloud-based IDS, the features you extract from monitoring data become critical to achieving high detection accuracy. Standard features include network flow characteristics (like packet size, flow duration, and the number of connections), system metrics (such as CPU, memory, and disk I/O usage), user behavior patterns (for example, login times and shifts in geographic location), and application-level metrics (like API request rates and error rates). To build robust IDS models, it's essential to focus on features that reflect the cloud's unique properties such as dynamic scaling, multi-tenancy, and its inherently distributed nature. Feature engineering explicitly tuned for cloud environments helps reduce false positives and ensures that detection models can keep up with constantly changing workloads and resource configurations [14].

3.3 Survey of existing intrusion detection system in cloud computing environment

The background of cloud-based intrusion detection shows a rapid transition from conventional signature-based approaches to hybrid and anomaly-based approaches.

3.3.1 Signature based intrusion detection system

In signature-based intrusion detection systems (IDS), identifying new attacks is facilitated by existing threats that the system has previously detected and recognized. This method involves comparing incoming network patterns to known signatures. If the incoming pattern matches a signature, it is classified as an intrusion.

One of the primary advantages of this detection system is its simplicity; once the characteristics of network behavior are understood, the system is easy to design and comprehend. It also demonstrates high accuracy in identifying known attacks and tends to produce a low rate of false positives.

Traditional signature-based IDS were made for fixed, on-premises networks and have trouble adapting to the changing nature of cloud environments. In the cloud, resources come and go quickly, network boundaries are not fixed, and traffic usually moves between services instead of through specific points. Attacks often target cloud-specific features like APIs or containers, which older signatures may not detect. Even small changes in attack patterns, especially against cloud services, can go unnoticed if the IDS isn't updated with the latest cloud-related threats.

Additionally, new signatures can be added to the database without the need to update or modify the existing ones [15].

However, the primary limitation of this approach is that it cannot detect new or unknown attack types. Even minor changes in patterns or variations may allow the attacks to bypass detection. Figure 3 illustrates the typical architecture of signature-based

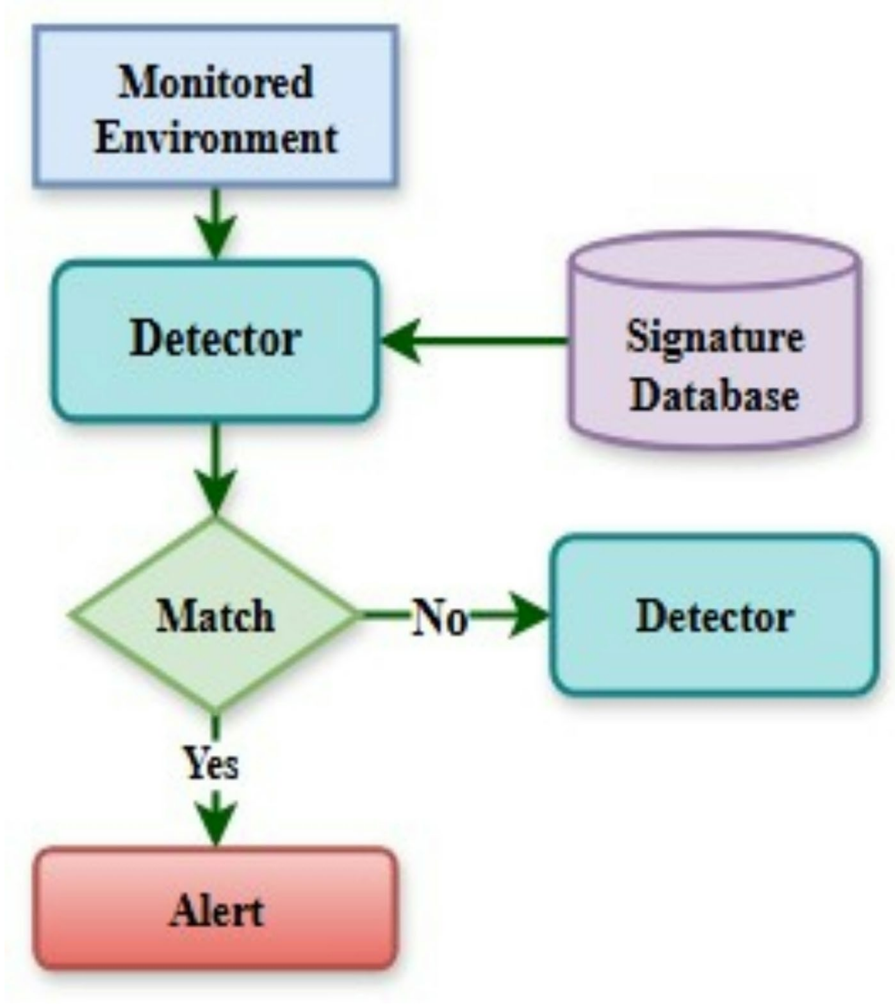

Fig. 3 Signature-based IDS Architecture

intrusion detection systems. Here are some examples of similar studies that utilized signature-based IDS.

In [16] the authors developed a signature-based Intrusion Detection System (IDS) algorithm aimed at improving network security. This system effectively mixed model recorded packets sent across the network and matched the traffic against a known attack signature database. It managed the given RAM resources and so safeguarded the network. Signature-based intrusion detection systems have a drawback, too: they cannot identify fresh or unknown threats without human involvement to update the signature database for every new intrusion.

One research [17] concentrated on using signature-based intrusion detection systems to find intrusions within virtual machine instances inside clouds as well as at the network level. This study using port mirroring for intrusion detection looked at traffic flow inside provider and self-service provider network architectures in an OpenStack context. The results examined the CPU and memory performance measures of the IDS and evaluated its response to alerts created by both benign and malicious traffic at different speeds.

3.3.2 Anomaly based intrusion detection system

By identifying user behaviour as either normal or abnormal, anomaly-based intrusion detection systems (IDS) are meant to find illegal access or deviations in cloud settings. This is accomplished by gathering data on normal user activity over a given period and subsequently performing a statistical analysis to see whether the observed actions fit the behaviour of an average user. Figure 4 shows the usually used structure of an anomaly-based IDS.

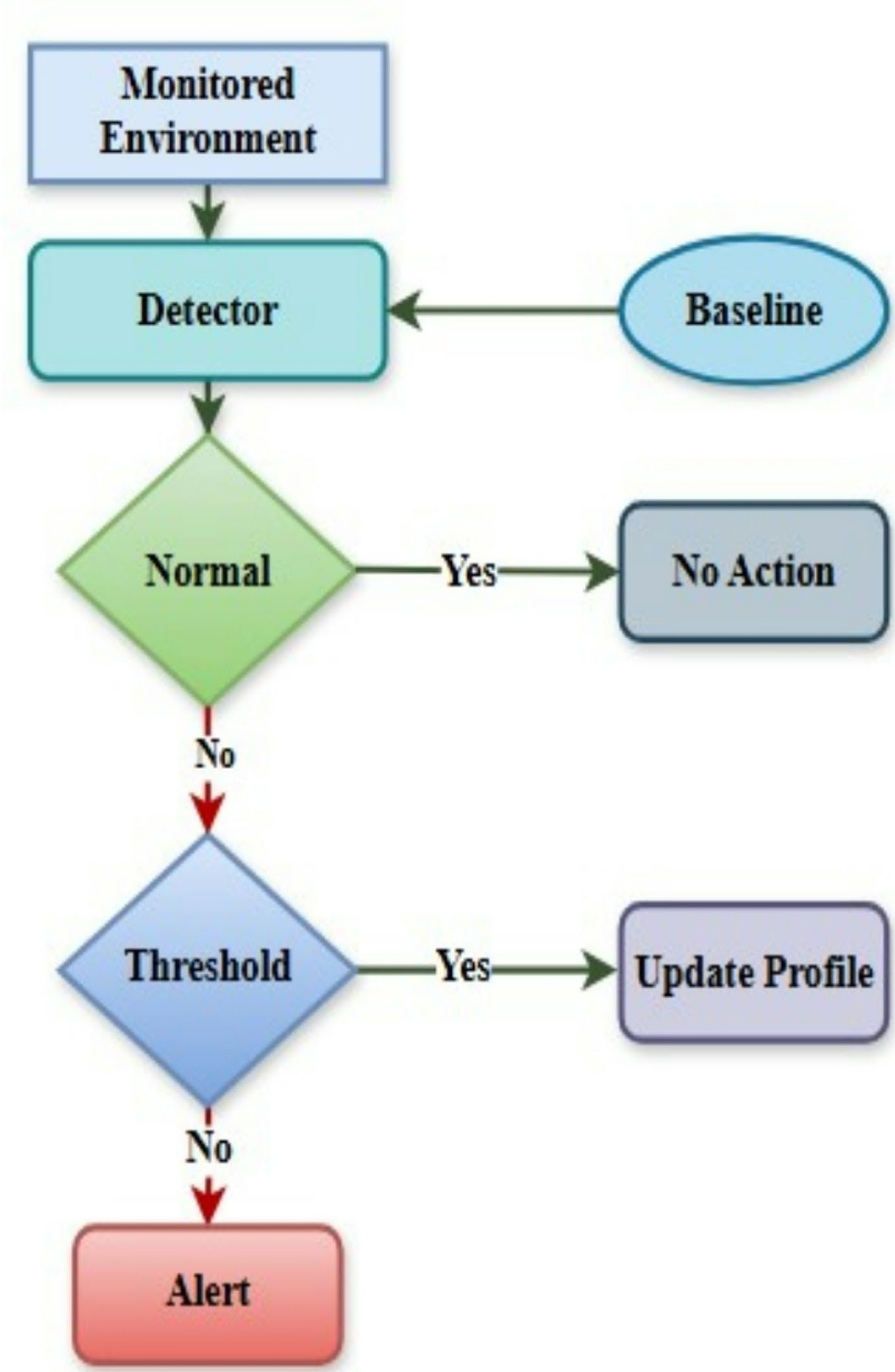

Fig. 4 Anomaly-based IDS Architecture

One major obstacle with these systems is that frequently changing them causes the loss of data used for training past versions. Moreover, these algorithms usually have poor identification accuracy, which results in a lot of false positives. Some current studies on anomaly-based IDS will be discussed in the following sections together with some approaches meant to improve anomaly detection in cloud-based Intrusion Detection Systems.

In [18], a distributed architecture was put out to help counteract DDoS assaults. This architecture lets many virtual machines (VMs) share detection responsibilities via a coordinator so they may cooperate in spotting coordinated threats. In a related work [19], an artificial bee colony optimization method was integrated with neural networks to improve DDoS detection accuracy in cloud systems.

Another approach in [20] combined particle swarm optimization with an adaptive neural network design at the hypervisor level, hence introducing a detection mechanism. With great detection accuracy and few false positives, our method proved successful in categorizing traffic between virtual machines and lowering anomalies associated with DDoS assaults. Emphasized the need for network traffic analysis and the dangers resulting from cost efficiency and dynamic resource movement [21]. The authors created HyClass, an ensemble model functioning in two stages: feature selection based on the Boruta method and classification using a support vector machine improved by chaotic optimization and differential evolution in order to reduce these hazards. HyClass demonstrated efficiency in identifying abnormalities while preserving privacy when evaluated on both benchmark and real-world datasets.

In [22] authors suggested an intrusion detection system (IDS) combining anomaly detection with feature selection to increase intrusion detection still more. The requirement of sophisticated optimization techniques to raise model accuracy was underlined in the work. Furthermore, employing a stacked bidirectional Long Short-Term Memory (LSTM) network, studies done in [23] concentrated on spotting anomalies inside OpenStack settings. Optimized with the binary cross-entropy loss function, the model examined ten distinct features taken from OpenStack logs and obtained detection accuracies of 94.61% in training and 93.98% in testing.

These studies highlight the importance of adjusting anomaly detection methods to fit the cloud's flexible and distributed environment. Unlike traditional IDS/IPS, which are designed for fixed, on-premises networks, cloud-based anomaly detection needs to handle dynamic scaling, the variety of cloud services, and complex traffic patterns that move internally between cloud resources.

3.3.3 Hybrid intrusion detection system

Using a hybrid detection technique combining signature-based and anomaly-based methods can greatly increase the efficacy of Intrusion Detection Systems (IDS) in cloud environments. Using approaches from every detection method, this integration detects known and undiscovered hazards.

Usually, Fig. 5 shows a hybrid strategy that includes three different techniques. The first method assesses the current surroundings before forwarding data to the second and third approaches, therefore producing a more strong and efficient system, especially in dynamic cloud settings [24].

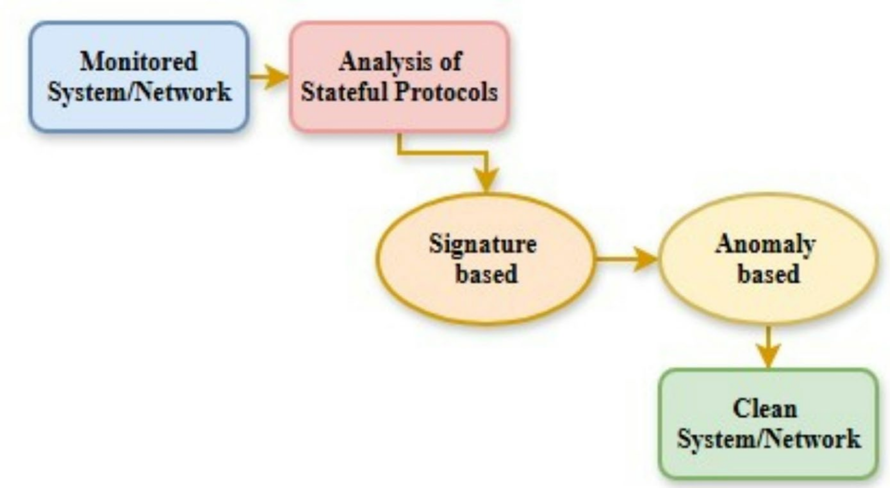

Fig. 5 Hybrid-based IDS Architecture

Aiming to safeguard cloud services, researchers in [25] concentrated on creating hybrid systems for intrusion detection. They used a combination of anomaly detection and signature-based intrusion detection and prevention systems (IDS/IPS). Using signature techniques, this hybrid solution efficiently detects current threats and vulnerabilities; concurrently, it detects new and unknown attacks by means of anomaly detection techniques, therefore augmenting the identification of vulnerabilities.

To enhance task scheduling in cloud computing, the work in [26] offers a method combining the Genetic Algorithm (GA) with the Multi-Verse Optimizer (MVO). While the GA improves this distribution by methods including selection, crossover, and mutation, the MVO helps virtual machines (VMs) distribute their work efficiently. This combined approach seeks to lower running time and enhance resource control. MATLAB simulations show that this method beats either the MVO or GA taken by itself.

In [27] put forth a cooperative architecture for cloud-based intrusion detection. Three elements define this architecture: a preprocessing module, a data capture and logging module, and a decision engine using a finite mixture model with an attack threshold. Still, this hybrid system has restrictions. For example, it calls for the attack information to be shared among distributed IDS nodes upon threat signature or anomaly identification. It also has limitations connected to both anomaly detection and signature-based approaches.

Moreover [28], presented a network-based anomaly detection system coupled with the Cloud Hypervisor level integration. This method improves the accuracy of the anomaly detection mechanism by means of a hybrid model comprising K-means clustering with SVM classification. Using the UNSW-NB15 dataset, the suggested strategy was assessed; the outcomes were then compared with earlier research. Although the K-means clustering approach showed somewhat greater accuracy than other supervised learning methods, the SVM method's performance remained insufficient. Table 1 provides a comparative analysis of various Intrusion Detection System (IDS) techniques in both traditional and cloud computing environments.

Finally [29], presented a hybrid approach known as HIDCC, which successfully detects and stops intrusions in systems of cloud computing. Their deployment resulted in

Table 1 Comparison of IDS techniques in cloud environments

IDSs	Normal Environment Capability	Cloud-Specific Capability	Strengths in Cloud Context
Signature-Based IDS	Performs well in static, well-defined network topologies; relies on known attack patterns	Limited in recognizing new attacks in dynamic, virtualized environments	Effective for identifying frequent attacks quickly; low false positives
Anomaly-Based IDS	Detects deviations from established norms; adaptable to new threats with training.	Must adapt to rapid changes in workload, traffic, and container deployments	Effective in detecting novel threats, adaptable to dynamic environments
Hybrid Techniques for IDS	Integrates multiple detection methods for comprehensive security coverage.	Enables layered security across distributed cloud services.	Enhances accuracy and resilience through multi-layer detection.
Machine Learning-Based IDS	Learns static behavior and patterns from labeled datasets.	Capable of ingesting and learning from large-scale telemetry (e.g., API calls, logs)	Scales with cloud data; adjusts to evolving attack strategies
Deep Learning-Based IDS	Deep analysis of traffic and system data for complex pattern recognition	Excels at modeling dynamic cloud workloads and VM-to-VM communication	Captures subtle and complex threats; scales with cloud traffic

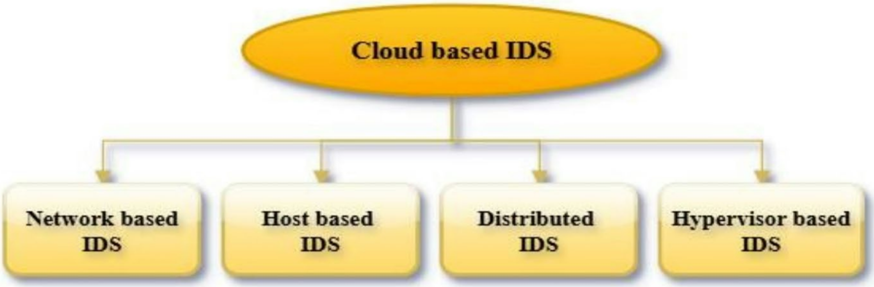

Fig. 6 Types of Cloud-based Intrusion Detection Systems

notable improvements in intrusion coverage, detection accuracy, dependability, and system availability, as well as considerably reduced false alarms.

Cloud-based Intrusion Detection Systems may be categorized into four kinds. The categories shown in Fig. 6 will be described in the subsequent subsections.

3.3.4 Network based intrusion detection system

Network-based intrusion detection systems (NIDS) function by analyzing traffic throughout a complete network infrastructure to identify harmful patterns, such as denial-of-service (DoS) assaults, unauthorized port scanning, and attempts at privilege escalation. These systems generally analyze metadata from IP and transport layer protocols, such as packet headers, to detect anomalies in anticipated communication standards. Detection strategies include two approaches: signature-based analysis, which combines actual traffic with established threat signatures, and anomaly-based monitoring, which creates baseline profiles of typical behavior to identify statistical anomalies.

In cloud environments, Network-based Intrusion Detection Systems (NIDS) face unique operational challenges due to the dynamic, virtualized nature of cloud infrastructure. Traditional NIDS rely on visibility into network traffic at key physical points, such as routers or firewalls. However, in cloud platforms, particularly public or hybrid clouds, network traffic between virtual machines (east-west traffic) may occur within the hypervisor or virtual switches, bypassing physical sensors entirely [30]. These deficiencies highlight the necessity for supplementary security solutions to tackle evolving attack surfaces. The Network-Based Intrusion Detection System (NIDS) depicted in Fig. 7 analyzes network data for signs of intrusion or malicious activity. This type of Intrusion Detection System (IDS) is deployed on a network device, such as a firewall or router. It is responsible for monitoring all traffic that passes through that device. NIDS functions by analyzing traffic and comparing it against a repository of known malware signatures.

Network Intrusion Detection Systems (NIDS) may use anomaly detection methodologies to recognize atypical behaviors or patterns within the traffic. NIDS can manage all network traffic, rendering it exceptionally proficient in identifying external threats or assaults originating from outside the corporation. Secondly, NIDS is less resource-demanding than HIDS since it does not need installation on each host. NIDS is less susceptible to attacks since it is deployed on a network device rather than directly on the host system. Nevertheless, NIDS has several drawbacks [31]. NIDS may provide several false positives, leading to time-consuming and expensive investigations. Secondly, NIDS may exhibit reduced efficacy in identifying insider threats or threats that arise from inside the company. NIDS may be less effective in detecting novel or acknowledged threats that lack an established attack signature.

Previous research [32] demonstrates that NIDS may proficiently guarantee cloud security. It aids in thwarting network assaults and identifying weaknesses inside the Cloud, like unprotected networks or obsolete software. Another advantage is its capacity to safeguard a company's critical data via its alert system. NIDS facilitates real-time monitoring, enabling security workers to react promptly to cloud assaults. In [33], an anomaly-based network intrusion detection system (NIDS) is used for monitoring and analyzing cloud-targeted network traffic flow. The system uses a Support Vector Machine (SVM) as a classifier and binary-based Particle Swarm Optimization (BPSO) to select relevant network features. The system is evaluated using the benchmark NSL-KDD dataset, achieving high detection accuracy and low false alarm rates. Network administrators are notified to block intrusive network connections.

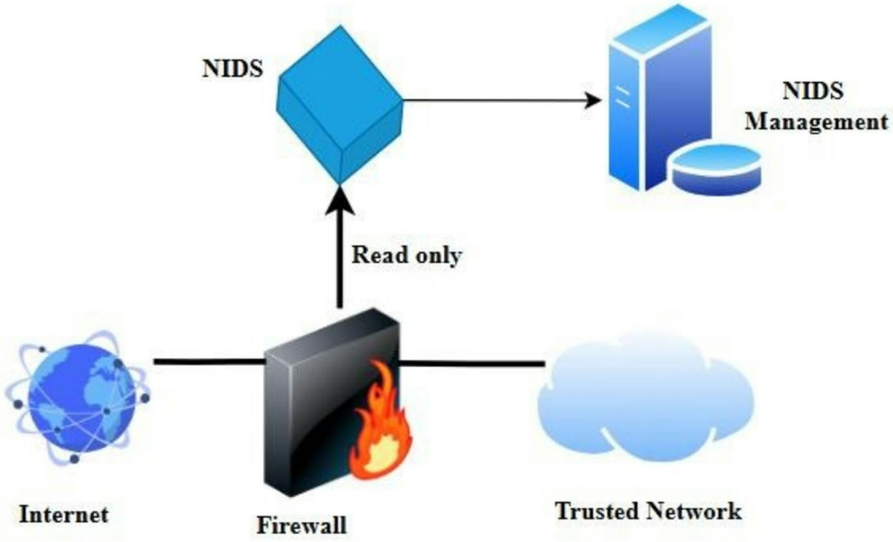

Fig. 7 Network-based intrusion detection systems (NIDS)

3.3.5 Host based intrusion detection system

Host-based intrusion detection systems (HIDS) monitor activities on specific hosts or endpoints, as illustrated in Fig. 8. This IDS is deployed on a single system or device and is responsible for monitoring its behavior. HIDS detects possible security issues by analyzing system logs, file changes, user activity, and other system events. HIDS detection techniques include signature-based detection, anomaly-based detection, and heuristics. Compared to NIDS, HIDS offers various benefits. To begin with, HIDS successfully detects insider threats or attacks that originate within an organization. This is because HIDS is installed directly on the host machine and can monitor any activities there. In addition, HIDS can give precise information on host system behavior, making it more straightforward to detect and react to possible security risks. However, HIDS is not without its drawbacks. For starters, HIDS may be resource-intensive, particularly if distributed across many hosts. Second, if the system hosting the application or data is hacked, HIDS may be subject to attack. Finally, HIDS is less successful at identifying external threats or assaults that originate from outside the host system [34].

3.3.6 Distributed intrusion detection system

The proposed Distributed Intrusion Detection System (IDS) consists of multiple IDSs spread across an extensive network, offering significant advantages such as enhanced network monitoring, event analysis, and real-time attack information [35]. One study introduced a distributed IDS that incorporates a binary segmentation change point detection technique aimed at identifying optimal time intervals for transmitting attack data to various nodes within the distributed system. This approach utilizes a parallel Stochastic Gradient Descent method combined with a Support Vector Machine (SGD-SVM) to improve the efficiency of distributed detection. The system was implemented using Apache Spark and tested with the NSL-KDD benchmark dataset for

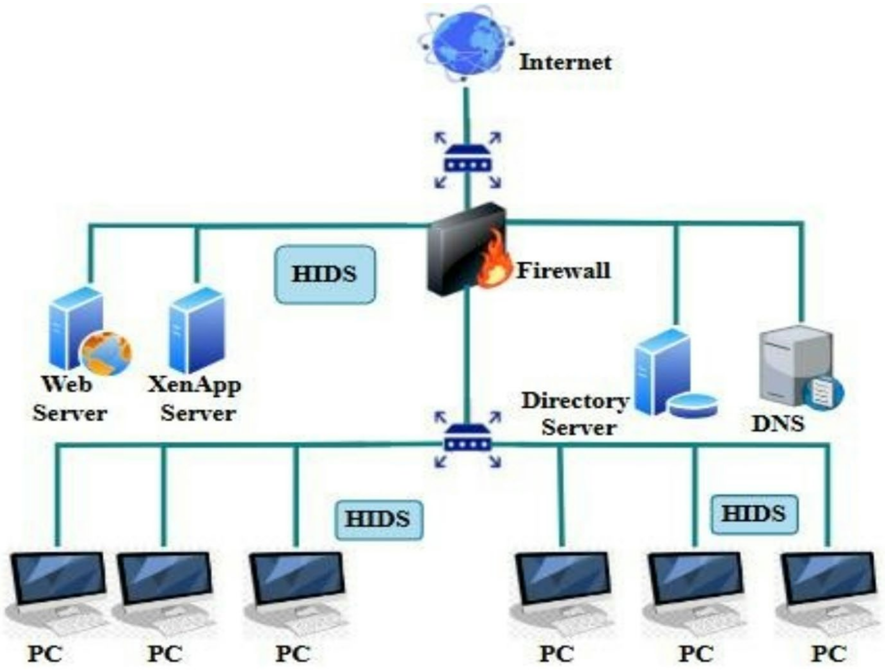

Fig. 8 Host-based Intrusion Detection System

intrusion detection. Experimental results indicated that our distributed IDS approach outperforms existing solutions in cloud computing environments. The distributed IDS improves resource management for incident analysis by aggregating attack information, enabling analysts to quickly identify emerging trends, patterns, and vulnerabilities across multiple network segments [36]. In [37], another distributed IDS for cloud computing was proposed, which detects distributed attacks using Neural Networks in conjunction with the Bat algorithm. Another study developed an efficient, reliable, and secure Distributed Intrusion Detection System (DIDS) employing a multi-agent technique to identify and respond to unique and complex malicious attacks. Evaluations were conducted to assess the effectiveness of this methodology. Figure 9 illustrates the Distributed Intrusion Detection System (DIDS) [38].

3.3.7 Hypervisor based intrusion detection system

Hypervisors offer a structure for running virtual machines (VMs). Operating within the hypervisor layer, intrusion detection systems based on hypervisors enable data monitoring and analysis to spot unusual activities and events. Interactions between the VMs and the hypervisor, interactions among several VMs, and internal communication within the hypervisor-based virtual network constitute the several communication levels from which this data is gathered. Within a cloud network, the hypervisor, also referred to as the Virtual Machine Manager (VMM), is the hardware or program in charge of building and running virtual machines. Virtual machine instances, under the control of hypervisors, can be attacked.

Designed to find and reduce intrusions in hypervisors inside virtualized cloud settings [39], presented the Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS). Combining components from past approaches and constantly observing behaviour to stop suspicious behaviour, the VMHIDS helps to reduce assaults connected to the hypervisor. Furthermore, a new method has been suggested that uses Bayesian inference and a trust-based maximin game to let hypervisors create trust-based interactions with guest virtual machines (VMs). This approach helps virtual machines distribute detection tasks fairly, hence enhancing the efficiency of real-time DDoS assault

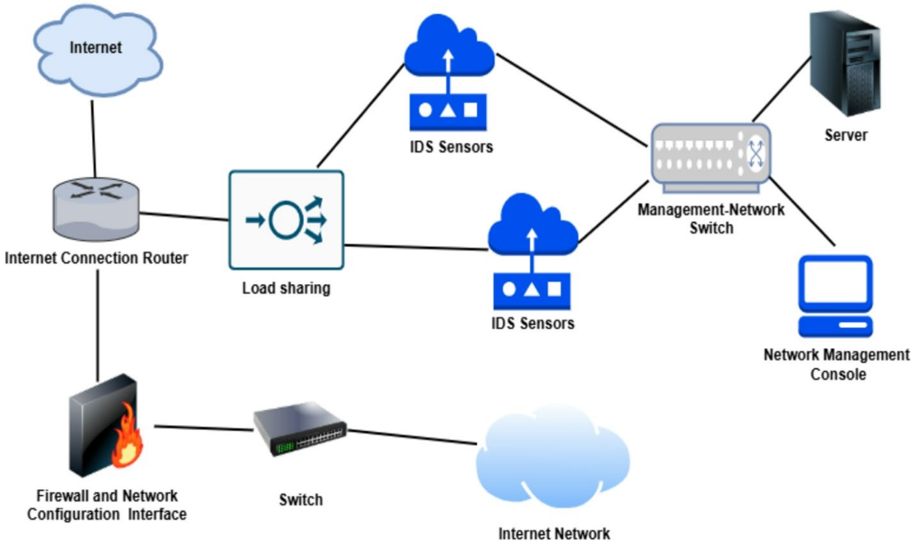
Internet
IDS Sensors
Server
Management-Network Switch
Internet Connection Router
Load sharing
IDS Sensors
Network Management Console
Firewall and Network Configuration Interface
Switch
Internet Network

Fig. 9 Distributed Intrusion Detection System

detection. Using Least Squares Support Vector Machine classification helps the method to have better detection rates [40].

3.4 The evolution of cloud based intrusion detection system

Various researchers have implemented Traditional Intrusion Detection Systems (IDS) in cloud environments to detect anomalies. For example [41], created a security architecture using Virtual Machine Introspection (VMI) for detailed monitoring of virtual machines and identifying known attacks. Zero-day attacks represent a significant threat to cloud security, as noted by [42]. Artificial neural networks are often used for their effectiveness with incomplete datasets.

The significance of machine learning for intrusion detection in the cloud is acknowledged for its scalability and flexibility [43]. Techniques such as genetic algorithms and particle swarm optimization are used to distinguish between network attack packets and legitimate traffic [44]. A study in [45] evaluated four IDSs with the NSL-KDD and UNSW-NB15 datasets and found that a hybrid support vector machine classifier outperformed existing methods. Another study introduced a cuckoo optimization method for preprocessing network traffic to improve IDS detection accuracy [46].

The primary goal of cloud IDS is to detect malicious activities early. DDoS attacks pose major risks, impacting budgets and service quality. To combat these threats, various detection techniques have been proposed [47] [48]. Introduced a new method for identifying DDoS TCP flood attacks using source and destination IP addresses to pinpoint malicious sources.

4 Classification of intrusion detection system methods

Dependency on conventional signature-based intrusion detection systems that use predefined attack signatures has hindered the identification of creative attacks and zero-day threats. By contrast, machine learning-based anomaly detection systems examine network traffic to find anomalies suggesting possible threats. In [49] the authors proposed a time series-based intrusion detection method for cloud environments. Using the CSE-CIC-IDS2018 dataset, they combined feature selection with anomaly detection and Granger causality, building a Facebook Prophet model that reduced features from 70 to 10 while improving accuracy and efficiency. In [50] the authors have reviewed various ML and DL models for IDS but the paper lacks details on datasets, features, and preprocessing which makes it hard to compare or assess them properly. In [51] the authors present a hybrid intrusion detection system that combines machine learning (XGBoost) and deep learning (CNN-LSTM) methods. It selects key features from four popular datasets (CIC IDS 2017, UNSW NB15, NSL KDD, and WSN-DS) to improve detection accuracy and reduce false alarms. The approach also tackles major IDS challenges like spotting new attacks and dealing with imbalanced data.

The authors in [52] have built a DDoS detection system for cloud environments using a deep neural network optimized with the Bat algorithm. Trained on the CICDDoS2019 dataset, it outperforms other methods like RNN and LSTM in accuracy and reliability. In [53] the authors present Cu-LSTMGRU, a hybrid IDS that combines improved LSTM and GRU models for better cloud-based attack detection. Using the CICIDS2018 dataset and Pearson feature selection, it achieved 99.76% accuracy and a very low false alarm rate, outperforming existing models. In [54] the authors present a cloud intrusion detection system that uses kernel fuzzy clustering and an optimized fuzzy neural network. Tested on the NSL-KDD dataset, it shows better accuracy than existing methods. Two approaches can be used to accomplish intrusion detection: intelligent systems based on learning techniques [55] and conventional signature-based systems that struggle with fresh intrusions.

Experiments using NSL-KDD and UNSW-NB15 datasets show that all three models outperform existing intrusion detection approaches in both accuracy and efficiency.

Intrusion Detection Systems (IDS), often combined with anomaly detection methods, are key to protecting cloud networks [56]. Surveys various cloud-based IDS architectures designed to handle these security challenges. In [57] a scalable intrusion detection system that uses deep learning for feature extraction and SVM for classification within a big data framework. The system is tested on the UNB ISCX 2012 and CICIDS 2017 datasets, achieving high accuracy and low false alarm rates.

4.1 Machine learning based intrusion detection system approaches in cloud computing

In research and engineering fields, machine learning (ML) is used to find optimal solutions for complex problems defined by many non-linear constraints, high dimensionality, and temporal limits. Different properties of machine learning methods help to solve problems in pattern categorization, regression, optimization, and function approximation. Using input or training data [58], this technology lets computers independently learn and grow in performance without explicit human programming. Machine learning's main goal is to produce algorithms competent for independently deducing insights from data without human interaction.

Three categories help to define machine learning algorithms: Supervised machine learning algorithms use given data to project results. Unsupervised machine learning systems identify structures or patterns from unlabeled data that are not immediately obvious. Usually, to enhance training data, semi-supervised machine learning approaches combine aspects of both supervised and unsupervised algorithms.

[59] suggests enhancing cloud security by means of a technique called Sea Horse Optimization with Deep Echo State Network for Intrusion Detection (SHO-DESNID). This approach combines a min-max normalizing technique with the Deep Echo State Network (DESN), designed especially for intrusion detection and classification. The SHO method greatly increases detection rates by helping to identify ideal hyperparameters. Results of simulations derived from a reputable Intrusion Detection System (IDS) database showed that the SHO-DESNID approach outperformed conventional approaches in performance criteria.

To improve detection accuracy in cloud environments [60], presented a novel intrusion detection system combining fuzzy c-means clustering with a support vector machine. Understood using the NSL-KDD dataset, this system showed a low false alarm rate comparable to past methods and improved detection accuracy, therefore highlighting the effectiveness of this hybrid method. Research on the combination of artificial intelligence (AI) and machine learning (ML) to enhance threat detection in cloud infrastructures has focused on [61]. A method consists of qualitative and quantitative assessments of current threat detection systems incorporating contemporary artificial intelligence approaches, including deep learning and reinforcement learning. Apparently reaching a minimum of 30% improvement over traditional techniques, this integrated model has shown a significant increase in anomaly detection accuracy.

Using a particle swarm optimization-based probabilistic neural network (PSO-PNN) [62], developed a new technique enhancing the capacity of cloud service providers to assess customer behavior. This approach uses a multi-layer neural network to detect fraudulent activity and effectively turns user behavior into a more understandable form. With a success rate of 96.4%, validation using the UNSW-NB15 dataset has shown great efficacy in security monitoring and the identification of harmful behavior [63]. looked at machine-learning approaches meant to address security issues in cloud computing and malware threats. The researchers presented a framework evaluating three machine learning models selected for their remarkable accuracy in malware detection.

[64] evaluated intrusion detection systems in mobile cloud environments using computational intelligence approaches in great detail. Apart from an evaluation of security threats in these fields, their study covers a schematic defining cloud computing (CC) and mobile cloud computing (MCC) standards and governance structures.

The machine learning-based intrusion detection system approaches investigated in this systematic literature review are thoroughly compared in Table 2. We proposed a

Table 2 ML-Based IDS in cloud computing

Reference	Objective	Methodology	Algorithm	Datasets	Accuracy
Aljamal et al., [28]	To enhance the accuracy of the anomaly detection system.	Combining K-means clustering with SVM classification to maximize accuracy, the paper presents a hybrid approach for identifying anomalies in network traffic at the Cloud Hypervisor level.	K-means clustering-SVM	UNSW-NB15	77%
Bakro et al., [67]	To detect and Classify Various types of attacks	The work presents an improved cloud IDS for attack detection and classification using a hybrid feature selection technique called SMote and a random forest model.	Random Forest (RF)	UNSW-NB15 Kyoto datasets	98% 99%
Satya & Dittakavi, [68]	To categorize assaults as either harmless or threatening.	The study proposes a dimensionality-reduction based IDS for cloud computing environments to reduce computational costs.	Gradient-Boosting	CSE-CIC-IDS2018	92%
Idhammad et al., [70]	To employ a multi-class classification procedure to identify the kind of each attack.	The work presented a distributed machine learning-based intrusion detection system intended especially for cloud systems.	An ensemble classifier based Random Forest	CIDDS-001 public dataset	97%
Bharati & Tamane [71]	To classify the attacks (benign / malicious) based on the intrusion detection performance.	This paper utilized the CSE-CICIDS-2018 dataset to analyze advanced system threats using an Intrusion Detection System with Machine Learning Based (Random Forest) approach.	Random Forest	CSE-CIC-IDS-2018	99%
Gumaste et al., [72]	To detect DDoS assaults in OpenStack-based Private Cloud	Using machine learning classifiers, a real-time detection system for DDoS attacks was constructed and put on a distributed processing platform. Using the Apache Spark framework, the system was evaluated on a cloud testbed grounded on OpenStack. Its performance was measured against real-time data as well as benchmark sets.	Random Forest	KDDCup 99 datasets Real time data	99.21% 94.40%

novel approach to detect Distributed Denial of Service (DDoS) attacks in cloud computing platforms. In [65], The approach applied Voting Extreme Naive Bayes and K-Means Learning Machine (V-ELM), a machine learning model. Every sample was categorized based on several votes on the type of attack used. The effectiveness of the V-ELM model was confirmed with respect to the NSL-KDD and ISCX intrusion detection datasets. Additionally presented was a cloud-based intrusion detection model using feature engineering and random forest (RF). Developed and included to raise the detection model's accuracy was the RF classifier. Two datasets were used to evaluate the approach and produce accuracy ratings of 98.3% for the Bot-IoT dataset and 99.99% for the NSL-KDD dataset.

In [66], hybrid machine learning approaches were investigated in cloud-based intrusion detection systems (IDS). Using the IDS at the level of the cloud hypervisor showed better detection accuracy. Support Vector Machine (SVM) classification methods, together with k-means clustering, were applied. The study showed that for the identification of known threats, hybrid machine learning approaches attained better detection accuracy than other approaches.

In [69], a method using machine learning to detect DDoS assaults in cloud systems was proposed. The system efficiently classified network traffic using the C4.5 decision tree technique. The technique integrated behavioural analysis with pattern recognition of identified dangers to find abnormal network activity. The strategy was assessed in an OpenStack and Virtual Box environment, where methods including K-Means clustering and Naive Bayes were also examined. The most efficient method for spotting and reducing dangers in cloud systems, the data showed, was the C4.5 algorithm, which attained the fastest detection time and the best accuracy (98.8%).

4.1.1 Supervised learning based techniques for intrusion detection system in cloud computing

In [73] a new dataset for an Intrusion Detection System (IDS) was produced in a private cloud environment utilizing Tor Hammer as the attack tool. The classification used several machine learning techniques like Random Forest, Naïve Bayes, and Support Vector Machine (SVM). Support Vector Machine had 99.7% accuracy; Random Forest had 98.0%; Naïve Bayes had 97.6%.

In another paper [74], a suggested Network Intrusion Detection System (NIDS) applied eXtreme Gradient Boosting (XGBoost) and SVM machine learning models. Hyperparameter tuning of the Crow Search Algorithm was used to improve performance. Moreover [75], a feature selection based on XGBoost enhanced classification precision. Using the NSL-KDD and UNR-IDD datasets, the efficacy of this system was assessed, and it showed better performance than baseline systems. It also encouraged future possibilities for modern NIDS.

Furthermore, another work proposed hybrid models for an anomaly-based IDS combining clustering and classification techniques. Using threshold-based detection techniques, this system seeks to identify several forms of malicious attacks, including regular traffic, Denial of Service (DoS), probing activities, User to Root (U2R), and Remote to Local (R2L). In the experiments, two threshold values-0.01 and 0.5, were investigated. The evaluation was conducted using NSL-KDD and KDDcup99, among other datasets. Along with 98.27% accuracy, 98.12% detection rate, and a mere 0.09% false alarm rate on the NSL-KDD dataset, this novel approach, which combines K-means clustering with

Random Forest classification, achieves noteworthy improvements in classification metrics on the KDDcup99 dataset at both threshold levels [76].

In [77], paper introduces a new approach to detecting intrusions in cloud computing using machine learning. It tackles a common problem where some types of attacks are harder to detect because they appear less often in training data. To solve this, the authors developed a weighted classification method that gives more importance to these rare attack types. By combining machine learning with insights from past network behavior, the system learns to improve its accuracy over time. Tests using the UNSW dataset show that this method performs better than existing solutions, especially in identifying less common threats.

In [78], paper introduces a smart intrusion detection system tailored for cloud computing. It uses a mix of five different techniques to pick out the most important features and combines multiple machine learning models to improve accuracy. The system classifies network traffic as either normal or an attack using a voting strategy. Tests on real-world and benchmark datasets showed it performs better than existing methods, with high accuracy and fewer false alarms.

A machine learning-based hybrid intrusion detection system using SVM and genetic algorithm (GA) approaches was presented in [79]. This algorithm ran in parallel to maximize accuracy in spotting the best characteristics and was tested on a dataset that included typical attacks. Up to 5.74%, the model exceeded standards, including KDD CUP 99 and NSL-KDD. Cloud computing is anticipated to be efficient since it offers a great synergy between information security and attack and harmful intrusion detection.

In [80], anomaly detection and classification are concentrated on publicly available datasets. Two supervised machine learning methods, random forest and linear regression, were used to develop and evaluate assault detection and classification learning models. The outcomes revealed a 93.6% categorization accuracy and almost 99% detection accuracy. Some attacks, however, were not categorized and emphasized the need to include detection and categorization in the contemporary study. Table 3 presents a thorough comparison of machine learning-based supervised learning methods; Fig. 10 shows the proportion of every methodology.

Table 3 ML-based supervised learning techniques

Reference	Techniques	Datasets	Accuracy (%)
Velliangiri, S and Premalatha, J et al. [37]	Radial basis function neural network (RBF-NN)	NSL-KDD data set	99.56
Chkirbene et al. [77]	Weight optimization algorithm	UNSW dataset	99.21
Krishnaveni et al. [78]	SVM, NB, LR, DT	Real-time Honeypot, Kyoto 2006 and NSL- KDD Dataset	98.89
Besharati et al. [81]	Logistic Regression (LR)	NSL-KDD data set	97.51
Zhang et al. [82]	K-Nearest Neighbor (KNN)	NSL-KDD	98.57
Singh, P., &Ranga, V [83].	Boosted tree, bagged tree, subspace discriminant, and RUS Booted	CICIDS 2017 and CloudSim	97.24
Ibrahim, N. M., &Zainal, A [84].	SGD-SVM	NSL-KDD	99.6
Attou et al., [85]	Random forest (RF)	Bot-IoT and NSLKDD datasets	98.3

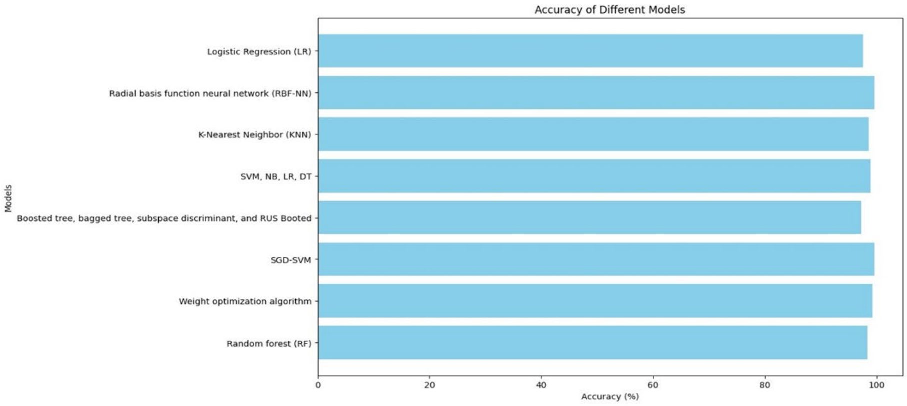

Fig. 10 Comparison of ML based Techniques

4.1.2 Unsupervised learning based techniques for intrusion detection system in cloud computing

In [66] authors showed how to use hybrid machine learning in a cloud-based intrusion detection system (IDS). Implementing the intrusion detection system in a network area at the cloud hypervisor level enhances its accuracy. The system implements a hybrid method that combines k-means clustering with SVM (Support Vector Machine) classification techniques. The investigation demonstrates that ML hybrid technology has a greater detection accuracy than other ML technologies for model creation work that can identify well-known threats.

In [86] proposed a novel integrated method to enhance the security of intrusion detection systems in cloud computing environments. Their technology addresses several security concerns, including the detection of fraudulent identities, the mitigation of data breaches, and protection against phishing attempts. This approach employs a fuzzy-based artificial neural network (ANN) to efficiently cluster anomalies, which is further improved by the spider monkey optimization process. This optimization method streamlines the iterative classification and selection procedures, allowing for automatic updates of fitness values. The use of spider monkey optimization leads to reduced computational time and improved accuracy compared to existing hybridization methods. Additionally, reference [87] introduces an innovative integrated clustering method called Weighted Fuzzy K-means in combination with an Auto Associative Neural Network (WFCM-AANN). This classifier demonstrates significant effectiveness in malware detection, proving capable of accurately identifying abnormalities and surpassing current classification techniques.

4.1.3 Deep learning based techniques for intrusion detection system in cloud computing

In [88] the authors concentrated on building an intelligent deep-learning algorithm for the real-time identification of cloud anomalies in order to increase system resilience. The characteristics obtained from the Transmission Control Protocol (TCP) traces in the simulation offer performance indicators at both the system and network levels, hence guiding the deep learning models. By means of the false alarm rate and detection rate, our suggested method exceeded Support Vector Machines (SVM).

To solve the constraints of conventional neural network models in [89], a deep learning-based intrusion detection system for multi-cloud IoT environments was presented.

The system increased its detection accuracy by optimizing training efficiency. By means of the NSL-KDD dataset, experimental evaluations revealed a detection rate of 97.51%, an accuracy of 96.28%, and a precision of 94.41%, so proving that the model exceeded conventional approaches.

Moreover, a novel deep learning model for cloud security intrusion detection was created in [90], combining recurrent neural networks (RNNs) and convolutional neural networks (CNNs). Trained on the NSL-KDD dataset, this model effectively stopped unwanted traffic from getting to the cloud server. It exceeded earlier methods described in the literature with an amazing accuracy of 99.86% over five classification categories. Additionally performed was a methodical study and comparison of several deep learning-based intrusion detection systems.

In [91], a hybrid deep learning model combining Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks was reported to distinguish between attack and regular traffic. Emphasizing the identification of important traits for DDoS attack detection, this approach employs ensemble feature selection and mutualizing aggregation. By means of the CICIDS 2017 benchmark dataset, the model achieved a success rate of 97.9%, therefore improving security and enabling efficient and automatic DDoS detection. Furthermore, under discussion in [95], a sophisticated Intrusion Detection and Prevention System (IDPS) tracked network traffic using a hybrid LSTM-CNN model to detect intrusions. User data inclusion greatly raised detection accuracy and produced fast alarms. Various performance criteria, including accuracy, precision, recall, and F1 score, showed the system's efficiency with a test accuracy of 99.27%, thereby strengthening security in cloud systems. A deep learning based IDS is found in Table 4.

4.1.4 Deep learning based supervised learning techniques for intrusion detection system in cloud computing

The proposed system [99] utilizes the UNSW-NB15 and BoT-IoT data sets with Bidirectional Long Short-Term Memory (BiLSTM) algorithms to detect network attacks, achieving up to 99% accuracy. It integrates blockchain and smart contracts for enhanced security and privacy while featuring a Cloud Vendor, a Central Coordinating Unit (CCU), and a Collaborative Intrusion Detection System (CIDS). The model trains on 60% of the data, effectively identifying various attacks like DDoS and data theft to secure cloud and IoT networks.

In [100], a Denial of Service (DoS) attack detection system tailored for cloud computing, employing the Oppositional Crow Search Algorithm (OCSA) and a Recurrent Neural Network (RNN), is developed. The methodology includes three key steps: Preprocessing to cleanse the data, and after that, Feature selection using OCSA to identify significant features, enhancing processing efficiency. Classification where the RNN categorizes data as normal or attacked. The system's effectiveness was evaluated based on precision, recall, F-measure, and accuracy, revealing superior performance compared to traditional methods when tested on the KDD Cup 99 dataset.

[101] introduces a system combining a Back Propagation Neural Network (BPNN) with an Improved Genetic Algorithm (IGA) to detect intrusions in cloud networks using the DARPA KDD Cup 1999 data set. The BPNN identifies patterns with enhanced accuracy, while the IGA optimizes performance and resource use. Testing with the CloudSim 4.0 simulator demonstrated that this system outperforms traditional methods, achieving

Table 4 DL-based IDS in cloud computing

Reference	Objective	Methodology	Algorithm	Dataset	Accuracy
Hajimirzaei & Navimipour [44]	To the detection of normal and anomalous packets inside network traffic	Developed a novel intrusion detection system utilizing a multilayer perceptron network and artificial bee colony to identify normal and abnormal network traffic packets.	MLP-ABC	NSL-KDD 99	98.41%
Hizal et al., [90]	To build a novel deep learning model for intrusion detection for cloud security	suggested a convolutional and recurrent layer-based lightweight model for binary and five-class categorisation using the NSL-KDD dataset.	CNN-RNN	NSL-KDD	99.86%
Aljuaid & Alshamrani [92]	To identify cyber-attacks in cloud environments.	The research introduced a deep learning model that utilizes an advanced architecture of convolutional neural networks (CNNs) to effectively identify cyberattacks within cloud environments.	MultiBlocks of CNN	CES-CICIDS2018	98.67%
Attou, Mohyeddine, et al., [93]	To develop and validate a novel Intrusion Detection System (IDS) model using Deep Learning (DL) techniques.	The study presented a novel IDS model using DL algorithms like RBFNN and Random Forest, utilizing Bot-IoT and NSL-KDD datasets for feature selection and intrusion detection.	Random Forest (RF) - Radial Basis Function Neural Network (RBFNN)	Bot-IoT NSL-KDD	99.99% 94.16%
Jisna et al., [94]	To conducted Attack detection and classification simultaneously	This presented a hybrid Stacked Contractive Auto Encoder (SCAE) + Support Vector Machine (SVM) IDS model and compares it to a cloud-based deep learning LSTM IDS model.	DL basedL-STM IDS model	NSL-KDD datasets	99.6%
Arulappan et al., [96]	To detect the intrusion and non-intrusion data	The paper introduced Intrusion Detection Systems and Fully Homomorphic Elliptic Curve Cryptography (IDS-FHECC), utilizing	LSTM-GAN	UNSW-NB15 dataset	99.87%
Mayuranathan et al., [97]	A deep Kronecker neural network (DKNN) is used to identify and classify cloud threats and intrusions.	In this work, a hybrid deep learning method was used to give an effective and optimum security solution for intrusion detection in a cloud computing environment.	DKNN	DARPA IDS CSE-CICIDS2018	97.22% 97.11%
Varun & Ashokkumar [98],	To develop an efficient security framework to enhance cloud security.	This study suggests using a Game Theory Cloud Security Deep Neural Network (GTCSDNN) model to enhance cloud security.	GT-CSDNN	CICIDS – 2017	CI-CIDS2017

Table 5 DL based supervised learning techniques

Reference	Techniques	Datasets	Accuracy (%)
Aljuaid & Alshamrani [97]	Multi-Blocks of CNN	CES-CICIDS2018	98.67%
Alkadi et al. [99]	Bi-LST M	UNSW-BN15 and BoT-IoT data sets	99.79
Sai Sindhu Theja, R., & Shyam, G. K [100]	Recurrent Neural Network (RNN)	KDD cup 99 dataset	94.12
Chiba et al. [101]	Back Propagation Neural Network (BPNN)	CloudSim simulator 4.0 and DARPA's KDD cup datasets	99.16
Alzughaibi & El Khediri [102]	Multi-layer Perceptron (MLP) with backpropagation (BP)	CES-CICIDS2018	98.41%
Prabhakaran, V., &Kulandasamy, A. [103]	Recurrent convolutional neural network (RCNN)	KDD CUP 99 data sets	99.67
Farhan et al., [104]	DNN	CES-CICIDS2018	95%
Garg et al., [105]	GWO and CNN	DARPA'98 and KDD'99	98.42
Chiba et al., [106]	Deep Neural Network (DNN)	CICIDS2017, NSL-KDD	99.93
Pu et al., [107]	CNN& k-means	KDDCUP99 dataset	98.41

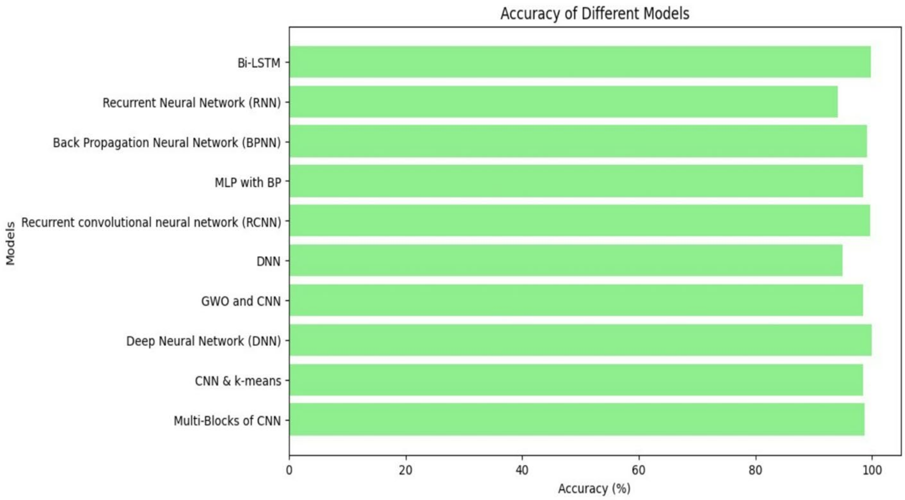

Fig. 11 DL based Supervised Learning Techniques

low false alarm rates and high detection efficiency, thus improving cloud network security. A comparison of deep learning techniques is found in Table 5, with Fig. 11 illustrating each technique's percentage.

4.1.5 Deep learning based unsupervised learning techniques for intrusion detection system in cloud computing

[108] introduces an intrusion detection system that uses deep learning specifically Variational Autoencoders (VAE) and Autoencoders (AE) to spot unusual activity in network traffic. The models are trained only on normal data, helping them recognize unknown or new types of attacks. Tested on the CICIDS2017 dataset, the VAE approach performed better than AE and One-Class SVM at identifying threats. Still, the authors note that some attack types were harder to detect, and more work is needed to lower false alarms

and improve accuracy [109]. showed that they used an unsupervised learning technique called Autoencoder (AE), which can learn without labeled data, a Network Intrusion Detection System (NIDS), which employs. They proposed a heuristic method based on the ratio of anomalous data in the training set to define a reconstruction loss threshold.

In [110] authors presents an innovative method for detecting network intrusions. The authors developed a layered approach that starts by using a genetic algorithm to pick out the most useful features from the data. They then refine these features further with fuzzy C-means clustering. After that, a convolutional neural network is used to extract deeper patterns from the data. Finally, a bagging classifier is applied to make accurate predictions. This combined method was thoroughly tested and showed strong, reliable performance, thanks to the use of 5-fold cross-validation.

[111] introduced a deep learning approach for unsupervised feature extraction that employs a stacked contractive autoencoder (SCAE) to acquire low-dimensional, robust features from network traffic. Their novel cloud intrusion detection system integrates support vector machine (SVM) classification methods with SCAE. Based on the KDD Cup 99 and NSL-KDD datasets, the SCAE + SVM strategy was found to lower analytical overhead and attain improved detection performance over three other approaches.

[112] proposed a deep learning intrusion detection system (IDS) that employs a pre-training strategy involving a deep auto-encoder (PTDAE) and a deep neural network. The model improves detecting performance using hyperparameter tweaking techniques. It was evaluated on the NSL-KDD and CSE-CIC-ID2018 datasets using the DAE technique, which exceeded earlier methods in multiclassification.

5 Datasets for intrusion detection system in cloud computing environment

The first step in building an effective intrusion detection system is selecting the right dataset. It is essential to include both benign and malicious entries to accurately represent the types of records the model will encounter in real-world scenarios. This section outlines some of the most well-known datasets used in this field. The most utilized datasets include KDD Cup 99, NSLKDD, CSE-CIC-IDS2018, UNSW-NB15, and CIDDS, among others. The frequency of use of datasets are shown in Fig. 12.

The intrusion detection datasets generated from actual network traffic traces are presented in Table 6. Researchers have widely used these datasets to evaluate the performance of intrusion detection systems (IDS). These datasets typically include labeled instances of normal behavior as well as various attack vectors, allowing for comprehensive training and validation of IDS models.

5.1 KDD CUP

The KDD CUP dataset is commonly utilized in research into intrusion detection systems. Developing and accessing machine learning models that detect disturbances and cyberattacks inside cloud-based intrusion detection systems depends especially on the KDD CUP 99 dataset. Improving cloud security depends on developing algorithms capable of efficiently filtering network traffic and spotting odd or hostile activity. There are around five million raw records in the KDD CUP 99 dataset, of which about 80% of them are assault data. Attack data and normal traffic are the two primary categories of this collection [113].

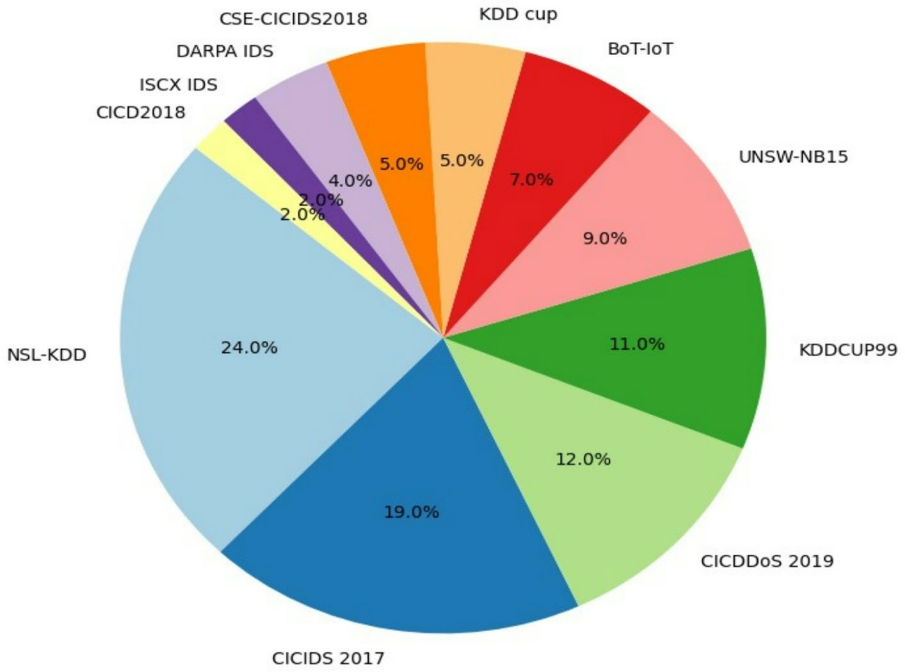

Fig. 12 Dataset usage percentage for IDS

Table 6 Intrusion detection system (IDS) datasets generated from actual network traffic traces

Developed by	Dataset	Attack Detect	Features
University of New South Wales Canberra (UNSW- Canberra)	BoT-IoT	Operating system and service scanning, keylogging, DDoS, DoS, data exfiltration assaults.	BoT-IoT dataset consists 43 features.
University of New South Wales Canberra (UNSW-Canberra)	UNSW-NB15	Attack_cat Which categorize attack into several type Generic, Exploits, Fuzzers, DoS, Reconnaissance, Backdoor.	This dataset comprises 49 features.
Coburg University of Applied Sciences and Arts in Germany.	CIDDS-001	DoS, Port scanning, Ping scanning, Brute Force Attack	14 total attributes in the dataset.
Communications Security Establishment (CSE) of Canada	CSE-CIC-IDS-2018	Brute Force Attacks, DoS, DDoS, Botnet attack, Web attack, Malware attack.	The dataset contains over 80 statistical flow features.
MIT Lincoln Laboratory	KDD-CUP99	DDoS attacks, User to Root, Remote to Local.	Dataset uses 41 features to describe network traffic
University of New Brunswick (UNB) in Canada	NSL-KDD	Dos, Probing or Surveillance, User to Root, Remote to Local.	Dataset includes 41 features.
Canadian Institute for Cybersecurity (CIC)	CICDDoS 2019	Network traffic, DDoS.	Dataset contain total of 83 features particularly in CI/CD environment.
Massachusetts Institute of Technology Lincoln Laboratory (MIT LL).	DARPA IDS	DoS, Remote to Local, User to Root, Probe, and Regular Traffic.	Dataset contains 41 features extracted from network traffic.
Canadian Institute for Cybersecurity (CIC)	ISCX IDS	DoS, Brute force attack, Infiltration, Web based attack.	The dataset contains 20 traffic flow features for each network flow.
Canadian Institute for Cybersecurity (CIC)	CICD 2018	Web assaults, DoS, DDoS, Brute-force, Heartbleed, Botnet, and infiltration	80 network traffic features that were retrieved using CICFlowMeter are included in the dataset.

5.2 NSL-KDD

Developing the NSL-KDD dataset helped the researchers overcome the constraints of the KDD-99 dataset. This new dataset seeks to resample KDD-99 such that the predictions generated by classifiers trained on the original KDD-99 data take front stage. The NSL-KDD dataset still presents difficulties, the researchers point note, especially in underrepresenting low-footprint attacks [114].

5.3 CSE-CIC-IDS2018

The Canadian Institute for Cybersecurity (CIC)'s CSE-CIC-IDS2018 dataset focuses on Amazon Web Services (AWS) cyber defence. By means of its datasets, the CIC and ISCX help to mitigate malware and support worldwide security testing. Seven different attack scenarios brute force attacks, Heartbleed exploits, botnet operations, Denial of Service (DDoS) attacks, Denial of Service (DoS) attacks, Internet assaults, and internal network penetration are included in the most recent CIC dataset.

5.4 ISCXIDS2012

The SCXIDS2012 dataset was developed using profiling techniques and contains intrusion descriptions as well as abstract models that depict the distribution of lower-level network components, protocols, and applications. These profiles are used to create a database inside the necessary testing environment and especially intended to copy user behaviour. The anomalous parts of the dataset are produced by using several scenarios of multi-stage assaults.

5.5 CICIDS2017

The CICIDS2017 dataset contains a large number of records relating to security threats that resemble legitimate traffic data. It produces legitimate and innocuous traffic while analyzing human behaviour using B-Profile technology. This dataset records 25 users' behaviour on several protocols including email, HTTPS, HTTP, SSH, and FTP.It also offers records on security issues including DDoS attacks, Heartbleed, online attacks, brute-force attacks on FTP and SSH.

5.6 UNSW-NB15

The collection includes both abnormal and regular network traffic traces created by the IXIA Perfect Storm tool. Network intrusion detection systems (NIDS) are examined using this tool. In addition to using the most recent attack data from a website that offers information on security vulnerabilities, IXIA can simulate nine different kinds of security attacks.

It's essential to recognize that, while widely used for training and evaluating intrusion detection models, most benchmark datasets are static, well-labelled, and pre-processed. These characteristics make them ideal for research comparisons, but don't fully reflect the conditions found in real-world cloud environments. In practice, data is often unlabelled, imbalanced, and changes over time factors that can limit the performance of models trained only on benchmark data. Future work should focus on building systems that learn continuously, adjust to shifting traffic behaviours, and incorporate real-time data, federated learning, and current threat intelligence to make IDS solutions more practical and effective in production.

6 Challenges of intrsuion detection technqiues in cloud computing environment

The advancement of intrusion detection algorithms in contemporary network systems primarily encounters four challenges are as follows [115]:

6.1 System datasets not available

A primary challenge in the development of effective intrusion detection algorithms is the lack of comprehensive, up-to-date, and diverse datasets. Many proposed approaches in the literature have difficulties in identifying zero-day attacks due to a lack of diversified training on different attack kinds and patterns. An intrusion detection system (IDS) needs to be tested and verified using datasets, including both historical and modern threats if it is to be efficient. Incorporating a broad spectrum of attack definitions into the dataset helps the model to identify fresh trends, hence enhancing its capacity to resist increasingly advanced invasions. The challenge lies not only in the creation of such datasets but also in the continuous updating of these datasets to reflect the evolving threat landscape.

Developing such thorough databases, however, may be expensive and resource-intensive and call for great knowledge. Therefore, the development of current datasets spanning a wide range of attack scenarios becomes one of the main difficulties in intrusion detection system research. Identifying the most recent dangers depends on regular updates to these databases. Hence, it is imperative that this material stays publicly available to facilitate academic study.

6.2 Reduced detection accuracy results from imbalanced datasets

Low-frequency assaults in datasets face challenges due to a lack of sufficient samples, which hinders models' ability to learn their characteristics effectively. This scarcity can reduce detection accuracy and complicate the algorithms' capacity to recognize low-frequency occurrences. Additionally, conventional loss functions, such as cross-entropy, may not effectively address the imbalance created by high-frequency data, leading to a bias that compromises detection effectiveness. To tackle the issue of imbalanced datasets, future research should explore advanced data augmentation techniques, such as the use of GANs to generate synthetic attack samples or hybrid models combining traditional machine learning methods with deep learning to improve accuracy across all attack types. Cost-sensitive learning and anomaly detection techniques could also play a key role in enhancing the performance of IDS in scenarios involving imbalanced datasets.

6.3 Poor performance in real-world environments

Exploring Intrusion Detection Systems (IDSs) is an intriguing endeavor as we assess their performance in real-world environments. Many proposed solutions often use outdated datasets for testing, leading to questions regarding their effectiveness. To develop genuinely robust systems, validating these techniques in real-time scenarios is crucial, ensuring they can thrive in today's dynamic networks. Let us embrace this challenge and collaboratively improve our cybersecurity landscape. Real-world validation is crucial for ensuring that IDS systems can operate effectively in dynamic production environments. Future research should focus on developing adaptive IDS models that can adjust to evolving network behaviors, leveraging techniques such as online learning, anomaly detection, and continuous retraining of models based on live traffic. By prioritizing real-time data collection and model updates, researchers can build more resilient systems capable of handling the challenges posed by modern, complex networks.

6.4 Resources used by complex models

Modern intrusion detection systems (IDS) often rely on intricate algorithms and resource-intensive architectures, which demand considerable computational power and memory allocation. This can strain system resources, creating bottlenecks that hinder real-time threat analysis and degrade the responsiveness of security frameworks. Although leveraging advanced GPU architectures with parallel processing capabilities may accelerate data throughput, such hardware investments often escalate operational expenses, making scalability challenging for resource-constrained environments. To address these limitations, prioritizing streamlined methodologies such as optimized feature extraction becomes imperative. By isolating high-impact network traffic attributes and eliminating redundant data dimensions, this approach minimizes processing latency while preserving detection accuracy, enabling efficient resource utilization without compromising system integrity. To improve the scalability and efficiency of IDS models, future research should prioritize the development of lightweight models that reduce computational complexity without compromising accuracy. Leveraging hardware-accelerated solutions such as GPUs or FPGAs for parallel processing and exploring federated learning or edge computing strategies can provide efficient ways to handle large-scale network traffic while reducing operational costs.

7 Future recommendations

Particularly in domains like automated incident response, image-based malware detection, and cloud-native security, exciting developments in cybersecurity are just around the horizon. Using machine learning methods inside cloud-native environments where these tools can efficiently evaluate and defend apps and services from possible hazards is attracting more and more interest. As cyber threats become increasingly sophisticated, these advanced techniques can provide proactive defense mechanisms, detecting and mitigating attacks before they cause significant harm.

Cloud environments keep expanding; hence, it is imperative to use wiser and more effective techniques for anomaly and intrusion detection. With possible innovations in machine learning and deep learning methods improving our capacity to correlate and react to security events, the future seems bright. One important method is federated learning, which greatly strengthens our defenses in cloud computing by encouraging organizational cooperation [116].

Furthermore, very promising is the idea of multi-task learning. This creative approach lets security models handle several problems at once, hence enhancing resilience against several kinds of threats. The value of edge and fog computing in preserving cloud security cannot be emphasized, given the explosive number of linked devices. Ensuring the security and privacy of edge devices depends on investigating customized machine learning and deep learning methods for these settings. This paradigm shift towards decentralized computing brings security closer to the source, reducing latency and enhancing real-time threat detection.

Eventually, as IoT-driven data processing keeps growing, maintaining safe operations depends on the demand for sophisticated, safe solutions leveraging machine learning and deep learning. There are plenty of chances ahead to build a safer digital environment [117]. Integrating security into the very fabric of IoT systems will be essential to building resilient infrastructures for the future.

8 Conclusion

Intrusion detection in cloud computing is a crucial area for ensuring system integrity, confidentiality, and availability against evolving cyber threats. This review highlights the significance of IDS as a basis of cloud security and provides an overview of signature-based, anomaly-based, and hybrid detection techniques also covers IDS techniques tested on standard datasets, but applying them in real-world settings brings new challenges. In practice, data is often unbalanced, unlabelled, and constantly changing. To make these systems more useful in actual cloud environments, they need to be tested on real traffic, adjusted to specific use cases, and optimized for fast, efficient performance.

The use of machine learning and deep learning techniques has improved the capability of IDS to detect complex and unknown attacks. However, these challenges include the issue of imbalance in datasets, high demands of computational resources, and applicability to real-world applications.

Innovative solutions like federated learning, automated incident response, and edge computing can help overcome some of these issues and pave the way for intrusion detection systems. Future research is expected to target scalable, adaptive, and resource-efficient IDS capable of meeting increasingly sophisticated and diverse cloud environments. Next-generation IDS could potentially deliver much better precision and significantly decreased false positives combined with more aggressive, real-time mitigation of threats due to advances in AI and emergent technologies and would assure high-quality security within the cloud environment.

Author contributions

S.S.M wrote the main manuscript text and prepared the figures under the supervision of P.P. and S.D. All the authors reviewed the manuscript.

Funding

No funding was received for carrying out this work.

Data availability

No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent for publication

No ethical or informed consent was required during this research.

Competing interests

The authors declare no competing interests.

Received: 5 February 2025 / Accepted: 2 June 2025

Published online: 06 June 2025

References

1. Elmasry W, Akbulut A, Zaim AH. A design of an integrated cloud-based intrusion detection system with third party cloud service. Open Comput Sci. 2021;11(1):365–79. https://doi.org/10.1515/comp-2020-0214.
2. Simon A. Intrusion detection system in cloud computing: a review. Int Conf Fac Nat Appl Sci 2022 No July. 2023. https://doi.org/10.5281/zenodo.8121064.
3. Suthar KC. Data security in cloud computing using encryption and obfuscation techniques, 2017.
4. Goggi S, Pardelli G, Bartolini R, Monachini M. Semantic query analysis from the global science gateway. Grey J. 2019;15(3).

5. Federal Trade Commission. Equifax data breach settlement. 2019. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.
6. Equifax Inc. Form 10-K for the fiscal year ended December 31, 2017, U.S. Securities and Exchange Commission. 2018. https://www.sec.gov/Archives/edgar/data/33185/000003318518000007/efx201710-k.htm.
7. A review on intrusion detection in cloud computing. 2023;2(2):207–15.
8. Al Nafea R, Almaiah MA. Cyber security threats in cloud: literature review, 2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc., no. July 2021. 2021. pp. 779–86. https://doi.org/10.1109/ICIT52682.2021.9491638.
9. Eddermoug N, et al. A literature review on attacks prevention and profiling in cloud computing. Procedia Comput Sci. 2023;220:970–7.
10. Al Nafea R, Almaiah MA. Cyber security threats in cloud: literature review. In: 2021 International Conference on Information Technology (ICIT), IEEE. 2021. pp. 1–6.
11. Krishna RH, Selvapriya B. Comprehensive review of intrusion detection systems in cloud computing. 2024;12(3):724–31.
12. Kosamkar VB. Intrusion detection system in cloud computing: an overview. Int J Recent Innov Trends Comput Commun. 2017;4(1):164–7.
13. Sadreazami H, Hashemi S, Movaghar A. A survey on east-west network traffic security challenges in cloud data centers. IEEE Commun Surv Tutorials. 2022;24(3):1953–75. https://doi.org/10.1109/COMST.2022.3196452.
14. Singh M, Sharma R, Thakur R. Deep learning-based IDS in multi-cloud environments: a feature selection perspective. Computers Secur. 2024;108:102321.
15. Aldallal A, Alisa F. Effective intrusion detection system to secure data in cloud using machine learning. Symmetry (Basel). 2021;13(12). https://doi.org/10.3390/sym13122306.
16. Saraniya G. Securing the network using signature based IDS in network intrusion detection systems. 2019.
17. Mahajan V, Peddoju SK. Deployment of Intrusion Detection System in Cloud: A Performance-Based Study. In: 2017 IEEE Trustcom/BigDataSE/ICESS, 2017. pp. 1103–8. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.359
18. Pandey VC, Peddoju SK, Deshpande PS. A statistical and distributed packet filter against DDoS attacks in cloud environment. Sādhanā. 2018;43:1–9.
19. Ali U, Dewangan KK, Dewangan DK. Distributed denial of service attack detection using ant bee colony and artificial neural network in cloud computing. In: Nature Inspired Computing: Proceedings of CSI 2015, 2018. pp. 165–75.
20. Al-hawawreh M. An anomaly-based approach for DDoS attack detection in cloud environment Adnan Rawashdeh * Mouhammd Alkasassbeh and. 2018;57(4):312–24.
21. Garg S, Kaur K, Kumar N, Batra S, Obaidat MS. HyClass: hybrid classification model for anomaly detection in cloud environment. In: 2018 IEEE International Conference on Communications (ICC), 2018. pp. 1–7. https://doi.org/10.1109/ICC.2018.8422481.
22. Aljawarneh S, Aldwairi M, Yassein MB. Anomaly-based intrusion detection system through feature selection analysis and Building hybrid efficient model. J Comput Sci. 2018;25:152–60.
23. Girish L, Rao SKN. Anomaly detection in cloud environment using artificial intelligence techniques. Computing. 2023;105(3):675–88. https://doi.org/10.1007/s00607-021-00941-x.
24. Karande SC, Bhongade PS. Hybrid intrusion detection system for securing cloud based services. In: International Conference on Intelligent Computing and Applications, 2017. pp. 1–4.
25. Vashishtha LK, Singh AP, Chatterjee K. A hybrid intrusion detection model for cloud based systems. No 4 Springer US. 2023;128. https://doi.org/10.1007/s11277-022-10063-y.
26. Abualigah L, Alkhrabsheh M. Amended hybrid multi-verse optimizer with genetic algorithm for solving task scheduling problem in cloud computing. J Supercomputing. 2022;78(1):740–65. https://doi.org/10.1007/s11227-021-03874-4.
27. Moustafa N, Creech G, Sitnikova E, Keshk M. Collaborative anomaly detection framework for handling big data of cloud computing. In: 2017 military communications and information systems conference (MilCIS), 2017. pp. 1–6.
28. Aljamal I, Tekeoglu A, Bekiroglu K, Sengupta S. Hybrid intrusion detection system using machine learning techniques in cloud computing environments. In: Proc - 2019 IEEE/ACIS 17th Int Conf Softw Eng Res Manag Appl SERA 2019. 2019;84–9. https://doi.org/10.1109/SERA.2019.8886794.
29. Hatef MA, Shaker V, Jabbarpour MR, Jung J, Zarrabi H. HIDCC: a hybrid intrusion detection approach in cloud computing. Concurr Comput Pract Exp. 2018;30(3):e4171. https://doi.org/10.1002/cpe.4171.
30. Chiba Z, Abghour N, Moussaid K, El Omri A, Rida M. A survey of intrusion detection systems for cloud computing environment. Stud Comput Intell. 2017;680:139–57. https://doi.org/10.1007/978-3-319-51388-1_6.
31. Rathod G, Sabnis V, Jain JK. Intrusion detection system (IDS) in cloud computing using machine learning algorithms: a comparative study. Grenze Int J Eng Technol. 2024;10(1).
32. Khan M, Haroon M. Detecting network intrusion in cloud environment through ensemble learning and feature selection approach. SN Comput Sci. 2023;5(1):84.
33. Sakr MM, Tawfeeq MA, El-Sisi AB. Network intrusion detection system based PSO-SVM for cloud computing. Int J Comput Netw Inf Secur. 2019;11(3):22–9. https://doi.org/10.5815/ijcnis.2019.03.04.
34. Hami S, Satılmış H, Akleylek S, Tok ZY. Syst Literature Rev host-based Intrusion Detect Syst IEEE Access. 2024;12:27237–66.
35. Ibrahim NM, Zainal A. A distributed intrusion detection scheme for cloud computing. Int J Distrib Syst Technol. 2020;11(1):68–82. https://doi.org/10.4018/IJDST.2020010106.
36. Idhammad M, Afdel K, Belouch M. Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Comput Sci. 2018;127:35–41.
37. Velliangiri S, Premalatha J. Intrusion detection of distributed denial of service attack in cloud. Cluster Comput. 2019;22:10615–23.
38. Achbarou O, El Kiram MA, Bourkoukou O, Elbouanani S. A new distributed intrusion detection system based on Multi-Agent system for cloud environment. Int J Commun Networks Inf Secur. 2018;10(3):526–33. https://doi.org/10.17762/ijcnis.v10i3.3546.
39. Dildar MS, Khan N , Abdullah JB, Khan AS. Effective way to defend the hypervisor attacks in cloud computing. In: 2017 2nd International Conference on AntiCyber Crimes (ICACC), 2017. pp. 154–9. https://doi.org/10.1109/AntiCybercrime.2017.7905282
40. Vetha S, Vimala Devi K. A trust-based hypervisor framework for preventing DDoS attacks in cloud. Concurr Comput Pract Exp. 2021;33(3). https://doi.org/10.1002/cpe.5279.

41. Mishra P, Varadharajan V, Pilli ES, Tupakula U. VMGuard: A VMI-Based security architecture for intrusion detection in cloud environment. IEEE Trans Cloud Comput. 2020;8(3):957–71. https://doi.org/10.1109/TCC.2018.2829202.
42. Rana P, Batra I. Detection of attacks in cloud computing environment–a comprehensive review. In: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021. pp. 496–9.
43. Balamurugan V, Saravanan R. Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation. Cluster Comput. 2019;22:13027–39.
44. Hajimirzaei B, Navimipour NJ. Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express. 2019;5(1):56–9. https://doi.org/10.1016/j.icte.2018.01.014
45. Rana P et al. Intrusion detection systems in cloud computing paradigm: analysis and overview. Complexity. 2022. 2022(1):3999039. https://doi.org/10.1155/2022/3999039.
46. Gnana Singh DAA, Priyadharshini R, Jebamalar Leavline E. Cuckoo optimisation based intrusion detection system for cloud computing. Int J Comput Netw Inf Secur. 2018;10(11):42–9. https://doi.org/10.5815/ijcnis.2018.11.05.
47. Vu L, Nguyen QU, Nguyen DN, Hoang DT, Dutkiewicz E. Deep generative learning models for cloud intrusion detection systems. IEEE Trans Cybern. 2023;53(1):565–77. https://doi.org/10.1109/TCYB.2022.3163811.
48. Sahi A, Lai D, Li Y, Diykh M. An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. IEEE Access. 2017;5:6036–48.
49. Al-Ghuwairi AR, Sharrab Y, Al-Fraihat D, AlElaimat M, Alsarhan A, Algarni A. Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. J Cloud Comput. 2023;12(1):127.
50. Attou H, Guezzaz A, Benkirane S, Azrour M, Farhaoui Y. Cloud-based intrusion detection approach using machine learning techniques. Big Data Min Anal. 2023;6(3):311–20. https://doi.org/10.26599/BDMA.2022.9020038.
51. Sajid M, et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. J Cloud Comput. 2024;13(1):123.
52. Jyothsna V, Manisha C, NanduSri BS. Intrusion detection system for detection of DDoS attacks in cloud environment. 2023.
53. Aldallal A. Toward efficient intrusion detection system using hybrid deep learning approach. Symmetry (Basel). 2022;14(9):1916.
54. Srilatha D, Shyam GK. Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network. Cluster Comput. 2021;24(3):2657–72.
55. Wu P. Deep learning for network intrusion detection: attack recognition with computational intelligence. UNSW Syd. 2020.
56. Sharma P, Sengupta J, Suri PK. Survey of intrusion detection techniques and architectures in cloud computing. Int J High Perform Comput Netw. 2019;13(2):184–98.
57. Mighan SN, Kahani M. A novel scalable intrusion detection system based on deep learning. Int J Inf Secur. 2021;20(3):387–403.
58. Ghanem WAHM, Jantan A, Ghaleb SAA, Nasser AB. An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons. IEEE Access. 2020;8:130452–75.
59. Jansi Sophia Mary C, Mahalakshmi K. Modelling of intrusion detection using sea horse optimization with machine learning model on cloud environment. Int J Inf Technol. 2024;16(3):1981–8. https://doi.org/10.1007/s41870-023-01722-9.
60. Jaber AN, Rehman SU. FCM–SVM based intrusion detection system for cloud computing environment. Cluster Comput. 2020;23(4):3221–31. https://doi.org/10.1007/s10586-020-03082-6.
61. Akinbolaji TJ. Advanced integration of artificial intelligence and machine learning for Real-Time threat detection in cloud computing environments. 2023;6(10):980–91.
62. Rabbani M, Wang YL, Khoshkangini R, Jelodar H, Zhao R, Hu P. A hybrid machine learning approach for malicious behavior detection and recognition in cloud computing. J Netw Comput Appl. 2020;151(May 2019):102507. https://doi.org/10.1016/j.jnca.2019.102507
63. Selamat N, Ali F. Comparison of malware detection techniques using machine learning algorithm. Indones J Electr Eng Comput Sci. 2019;16(1):435–40.
64. Shamshirband S, Fathi M, Chronopoulos AT, Montieri A, Palumbo F, Pescapè A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues. J Inf Secur Appl. 2020;55:102582.
65. Kushwah GS, Ranga V. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. J Inf Secur Appl. 2020;53:102532.
66. Pavan PJ, Sivakumar R. Implementation of hybrid machine learning approach for intrusion detection system. J Adv Res Dyn Control Syst. 2019;11(6 Special Issue):49–55. https://doi.org/10.9756/INT-JECSE/V14I2.128.
67. Bakro M et al. An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. IEEE Access. 2023;11(May):64228–47. https://doi.org/10.1109/ACCESS.2023.3289405
68. Satya R, Dittakavi S. Dimensionality reduction based intrusion detection system in cloud computing environment using machine learning. Int J Inf Cybersecur. 2022. pp. 62–81.
69. Zekri M, El Kafhali S, Aboutabit N, Saadi Y. DDoS attack detection using machine learning techniques in cloud computing environments. Proc 2017 Int Conf Cloud Comput Technol Appl CloudTech 2017. 2017;2018–Janua(no October):1–7. https://doi.org/10.1109/CloudTech.2017.8284731.
70. Idhammad M, Afdel K, Belouch M. Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Comput Sci. 2018;127:35–41. https://doi.org/10.1016/j.procs.2018.01.095.
71. Bharati MP, Tamane S. NIDS-network intrusion detection system based on deep and machine learning frameworks with CICIDS2018 using cloud computing. In: 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020. pp. 27–30. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299584.
72. Gumaste S, Narayan DG, Shinde S, Amit K. Detection of Ddos attacks in openstack-based private cloud using Apache spark. J Telecommun Inf Technol. 2020;4:62–71.
73. Wani AR, Rana QP, Saxena U, Pandey N. Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In: Proc - 2019 Amity Int Conf Artif Intell AICAI 2019. 2019; pp. 870–5. https://doi.org/10.1109/AICAI.2019.8701238.
74. Samriya JK, Kumar S, Kumar M, Wu H, Gill SS. Machine learning based network intrusion detection optimization for cloud computing environments. IEEE Trans Consum Electron. 2024;XX(Xx):1–12. https://doi.org/10.1109/TCE.2024.3458810

75. Samunnisa K, Kumar GSV, Madhavi K. Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods. Meas Sens. 2023;25(September 2022):100612. https://doi.org/10.1016/j.measen.2022.100612
76. Gao Y, Liu Y, Jin Y, Chen J, Wu H. A novel Semi-Supervised learning approach for network intrusion detection on Cloud-Based robotic system. IEEE Access. 2018;6:50927–38. https://doi.org/10.1109/ACCESS.2018.2868171.
77. Chkirbene Z, Erbad A, Hamila R, Gouissem A, Mohamed A, Hamdi M. Machine learning based cloud computing anomalies detection. IEEE Netw. 2020;34(6):178–83.
78. Krishnaveni S, Sivamohan S, Sridhar SS, Prabakaran S. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Comput. 2021;24(3):1761–79.
79. Aldallal A, Alisa F. Symmetry. 2021;13(12). https://doi.org/10.3390/sym13122306. Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning.
80. Akoto J, Salman T. Machine learning vs deep learning for anomaly detection and categorization in Multi-cloud environments. In: Proc - 2022 IEEE Cloud Summit Cloud Summit 2022. 2022;44–50. https://doi.org/10.1109/CloudSummit54781.2022.00013.
81. Besharati E, Naderan M, Namjoo E. LR-HIDS: logistic regression host-based intrusion detection system for cloud environments. J Ambient Intell Humaniz Comput. 2019;10:3669–92.
82. Zhang Z, Wen J, Zhang J, Cai X, Xie L. A many objective-based feature selection model for anomaly detection in cloud environment. Ieee Access. 2020;8:60218–31.
83. Singh P, Ranga V. Attack and intrusion detection in cloud computing using an ensemble learning approach. Int J Inf Technol. 2021;13(2):565–71.
84. Ibrahim NM, Zainal A. A distributed intrusion detection scheme for cloud computing. Int J Distrib Syst Technol. 2020;11(1):68–82.
85. Attou H, Guezzaz A, Benkirane S, Azrour M, Farhaoui Y. Cloud-based intrusion detection approach using machine learning techniques. Big Data Min Anal. 2023;6(3):311–20.
86. Samriya JK, Kumar N. A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing, Mater. Today Proc. 2020. https://doi.org/10.1016/j.matpr.2020.09.614
87. Yadav RM. Effective analysis of malware detection in cloud computing. Comput Secur. 2019;83:14–21. https://doi.org/10.1016/j.cose.2018.12.005.
88. Sreenivasa Chakravarthi S, Jagadeesh Kannan R, Anantha Natarajan V, Gao XZ. Deep learning based intrusion detection in cloud services for resilience management. Comput Mater Contin. 2022;71(2):5117–33. https://doi.org/10.32604/cmc.2022.022351.
89. Selvapandian D, Santhosh R. Deep learning approach for intrusion detection in IoT-multi cloud environment. Autom Softw Eng. 2021;28(2):19. https://doi.org/10.1007/s10515-021-00298-7
90. Hizal S, AKGÜN ÜÇAVUŞOĞLU. A new deep learning based intrusion detection system for cloud security. In: 2021 3rd International Congress on HumanComputer Interaction, Optimization and Robotic Applications (HORA), 2021. pp. 1–4. https://doi.org/10.1109/HORA52670.2021.9461285.
91. Sanjalawe Y, Althobaiti T. DDoS attack detection in cloud computing based on ensemble feature selection and deep learning. Comput Mater Contin. 2023;75(2):3571–88. https://doi.org/10.32604/cmc.2023.037386.
92. Aljuaid WH, Alshamrani SS. A deep learning approach for intrusion detection systems in cloud computing environments. Appl Sci. 2024;14(13). https://doi.org/10.3390/app14135381.
93. Attou H, et al. Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. Appl Sci. 2023;13(17). https://doi.org/10.3390/app13179588.
94. Jisna P, Jarin T, Praveen PN. Advanced intrusion detection using deep learning-LSTM network on cloud environment. In: Proc. 4th Int. Conf. Microelectron. Signals Syst. ICMSS 2021, 2021. https://doi.org/10.1109/ICMSS53060.2021.9673607.
95. Srilatha D, Thillaiarasu N. LSTM-CNN: a deep learning model for network intrusion detection in cloud infrastructures. Int J Crit Infrastruct. 2024;20(6):505–23. https://doi.org/10.1504/IJCIS.2024.142451.
96. Arulappan R, Rose M, Gopalakrishnan A, Vasuki J. Research article deep learning based lstm-gan approach for intrusion detection in. 2024;2(3).
97. Mayuranathan M, Saravanan SK, Muthusenthil B, Samydurai A. An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. Adv Eng Softw. 2022;173:103236. https://doi.org/10.1016/j.advengsoft.2022.103236.
98. Varun P, Ashokkumar K. Intrusion detection system in cloud security using deep convolutional network. Appl Math Inf Sci. 2022;16(4):581–8. https://doi.org/10.18576/amis/160411.
99. Alkadi O, Moustafa N, Turnbull B, Choo K-KR. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet Things J. 2020;8(12):9463–72.
100. SaiSindhuTheja R, Shyam GK. An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. Appl Soft Comput. 2021;100:106997.
101. Chiba Z, Abghour N, Moussaid K, Omri AE, Rida M. New anomaly network intrusion detection system in cloud environment based on optimized back propagation neural network using improved genetic algorithm. Int J Commun Networks Inf Secur. 2019;11(1):61–84.
102. Alzughaibi S, Khediri SE. A cloud intrusion detection systems based on Dnn using backpropagation and Pso on the cse-cic-ids2018 dataset. Appl Sci. 2023;13(4):2276.
103. Prabhakaran V, Kulandasamy A. Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. Comput Intell. 2021;37(1):344–70.
104. Farhan RI, Maolood AT, Hassan NF. Optimized deep learning with binary PSO for intrusion detection on CSE-CIC-IDS2018 dataset. J Al-Qadisiyah Comput Sci Math. 2020. 12(3):16.
105. Garg S, Kaur K, Kumar N, Kaddoum G, Zomaya AY, Ranjan R. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Trans Netw Serv Manag. 2019;16(3):924–35.
106. Chiba Z, Abghour N, Moussaid K, Rida M. Intelligent approach to build a deep neural network based IDS for cloud environment using combination of machine learning algorithms. Comput Secur. 2019;86:291–317.
107. Pu X, Zhang Y, Ruan Q. Optimization of intrusion detection system based on improved convolutional neural network algorithm. Math Probl Eng. 2022(1):6762175.

108. Zavrak S, Iskefiyeli M. Anomaly-based intrusion detection from network flow features using variational autoencoder. IEEE Access. 2020;8:108346–58.
109. Choi H, Kim M, Lee G, Kim W. Unsupervised learning approach for network intrusion detection system using autoencoders. J Supercomput. 2019;75:5597–621.
110. Nguyen MT, Kim K. Genetic convolutional neural network for intrusion detection systems. Futur Gener Comput Syst. 2020;113:418–27.
111. Wang W, Du X, Shan D, Qin R, Wang N. Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE Trans Cloud Comput. 2022;10(3):1634–46. https://doi.org/10.1109/TCC.2020.3001017.
112. Kunang YN, Nurmaini S, Stiawan D, Suprapto BY. Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. J Inf Secur Appl. 2021;58:102804.
113. Scholar PG. Machine-learning-based cloud intrusion detection. Int J Mech Eng Res Technol. 2024;16(3).
114. Li K, Zhang Y, Wang S. An intrusion detection system based on PSO-GWO hybrid optimized support vector machine. In: 2021 International Joint Conference on Neural Networks (IJCNN), 2021. pp. 1–7.
115. Wu Y, Zou B, Cao Y. Current status and challenges and future trends of deep Learning-Based intrusion detection models. J Imaging. 2024;10(10). https://doi.org/10.3390/jimaging10100254.
116. Alzoubi YI, Aljaafreh A. Blockchain-fog computing integration applications: a systematic review. Cybern Inf Technol. 2023;23(1):3–37.
117. Alzoubi YI, Mishra A, Topcu AE. Research trends in deep learning and machine learning for cloud computing security. No 5 Springer Neth. 2024;57. https://doi.org/10.1007/s10462-024-10776-5.

Publisher's note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.