Volume (1) No (9), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Classification Techniques on Network Intrusion Systems

Mr. Himanshu Barhaiya
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Bhopal
himanshub@lnct.ac.in

***Abstract*—Cloud computing's scalability, flexibility, and on-demand resource availability have revolutionized contemporary IT architecture. However, complicated security and privacy issues are brought up by its dynamic, distributed, and multi-tenant nature. When it comes to dealing with these changing threats, conventional rule-based intrusion detection systems (IDS) frequently fail. With an emphasis on proactive and adaptable security measures, this study offers a thorough review of IDS based on machine learning (ML) and deep learning (DL) for cloud settings. The review examines the effectiveness of supervised and unsupervised ML models, as well as advanced DL architectures, in real-time threat detection and anomaly prediction. Behavior-based analysis, feature selection techniques, and predictive models such as Facebook Prophet are highlighted for their role in improving detection accuracy. Key datasets, evaluation metrics, and deployment tools are also discussed to offer practical insights into the implementation of intelligent IDS solutions. Emphasizing a shift from reactive defense to predictive, self-learning strategies, this survey outlines the potential of AI-driven IDS to enhance scalability, accuracy, and resilience in cloud security. The findings aim to support future research and development of next-generation intrusion detection frameworks for secure cloud computing.**

***Keywords*—Cloud computing, Intrusion Detection Systems (IDS), Machine Learning (ML), Deep Learning (DL), Cloud Security, Proactive Threat Detection, Anomaly Detection.**

I. INTRODUCTION

The widespread adoption of cloud computing enables organizations across industries to reap the benefits of unprecedented scalability, operational flexibility, and cost efficiency in deploying and managing IT services. Cloud platforms are essential for contemporary digital businesses because they provide on-demand resource provisioning, effective task allocation, and easy access to processing power and storage [1]. These benefits carry a high and shifting price in terms of security. As enterprises outsource sensitive data and critical workloads to cloud environments, the attack surface expands exponentially and faces an extended range of threats, among them advanced persistent threats (APTs), insider threats, the loss of sensitive data, unauthorized access, and account hijacking [2]. These risks are compounded by the dynamic and dispersed cloud systems, characterized by quick changes in resource placements, service interrelations and access patterns [3]. Their inability to deal with this kind of complexity often leads to a failure of traditional security mechanisms that are generally based on static rules, signature-based detection, and reactive monitoring to provide appropriate protection of vital systems.

In modern-day cloud computing, proactive security has become an important practice, which aims at anticipating, detecting, and preventing security threats prior to their occurrence instead of responding to the security threats after they appear [4]. This is more crucial in cloud scenarios, where reactive defenses are not useful because resources are dynamic, distributed and virtualized. Forward-looking preventive policies comprise behavioral modelling, predictive analytics, and automated enforcement solutions to defend systems prior to attacks being effective and to thwart these impediments. The ProSAS system which analyzes previous cloud activity logs to detect interdependencies between the events and anticipate potential policy violations is one of the best examples of this shift [5]. ProSAS extends the traditional security to avoid threats that are proactive by combining prediction with verification of pre-emptive policies [6]. It can assist businesses to protect cloud infrastructure against sophisticated and dynamic cyberthreats by enhancing the accuracy of their detection and lowering the response time of such threats.

The invention of ML and DL has changed the Intrusion Detection Systems (IDS) scenario. These intelligent models are able to detect complex patterns through big data and therefore, they can experience low false alerts and high anomaly detection accuracy [7]. ML-based frameworks such as Leader Class and Confidence Decision Ensemble (LCCDE) show the effectiveness of the ensemble methods to distinguish different cyberattacks with more precision [8]. Similarly, DL is proving practical significance, most especially in challenging environments like Cyber-Physical Systems (CPS), where hierarchies can be applied in managing the dynamic reaction to attack types [9].

Smart IDS designs are also currently incorporating real-time behavioral analysis and host-based intrusion detection as a way to safeguard endpoints in the cloud [10]. The behavioral sample of the user e.g., logging behavior, typing patterns, or machine usage, is recorded by newer systems to utilize contextual awareness to improve authentication and threat detection. In order to complement these advanced

mechanisms of IDS, it is also critical to choose proper data storage solutions [11]. As data generated from IDS logs and behavioral tracking grows rapidly, hybrid databases combining SQL and NoSQL models offer scalable and flexible back-end infrastructures [12].

This survey presents an extensive examination of IDS strategies based on ML and DL that are suited for cloud environments. It examines detection methodologies, architectural frameworks, benchmark datasets, and evaluation metrics prevalent in current literature. Finally, the paper advocates for the development of proactive, self-adaptive IDS systems that not only detect intrusions but also anticipate and preempt threats paving the way toward intelligent, next-generation cloud security.

A. *Structure of the Paper*

The paper is structured as follows: Section I presents the background and security challenges in cloud computing. Section II reviews cloud security. Section III overview of Intrusion detection system (IDS). Section IV explores ML/DL-based IDS models and evaluation. Section V and Section VI provide comparative insights, and conclude with key findings and future directions.

II. Understanding of Cloud Security

The way that people and organizations store, manage, and process data has been completely transformed by the rapid growth of cloud computing in the last several years. It has gained popularity mainly due to the convenience it promises, its scalability and affordability. The cloud platforms provide high-quality computing at high-performance with the support of various applications such as web hosting, email, and real-time messaging [13]. Such characteristics as the on-demand allocation of resources, the elastic scalability, and pay-as-you-go pricing models have also made cloud solutions particularly popular among businesses of all sizes. Although this has provided many benefits, the growth in the use of cloud infrastructure has raised novel and compound security issues [14]. The risk and consequences (in case of a cyber-attack) have increased as more sensitive and mission-critical data are migrated to the cloud. The rise in cloud-targeted attack frequency, complexity, and efficacy is a glaring example of why significant and ongoing security measures are required.

A. *Evolution of Cloud Computing*

Cloud computing has revolutionized how individuals and businesses store, process, and retrieve data. Through the internet, it offers customers computational infrastructures such as servers, storage, databases, networking, software, and analytics often referred to as "the cloud." John McCarthy initially proposed the notion in the 1960s, when he viewed computer power as a public utility, similar to water or electricity. The foundation of cloud computing was established in the 1970s when virtualization technology was invented, enabling the operation of many operating systems on a single physical server [15]. In 2006, Amazon Web Services (AWS) was introduced, marking a significant advancement by granting on-demand access to cloud-based resources including computing, storage, and databases. This marked a significant shift from traditional IT models, eliminating the necessity for businesses to make investments in and keep up their own physical infrastructure.

B. *Cloud Computing Architecture*

A concept known as cloud computing uses the internet to provide scalable, on-demand resources. The three service types that make up its architecture, IaaS, PaaS, and SaaS are based on layers of networking, storage, virtualization, and data centers. Cloud deployment options, including public, private, hybrid, and community clouds, specify how users may access and share infrastructure. Virtualization and resource pooling enable multi-tenant environments, improving efficiency but also introducing security risks, (as shown in Figure 1).

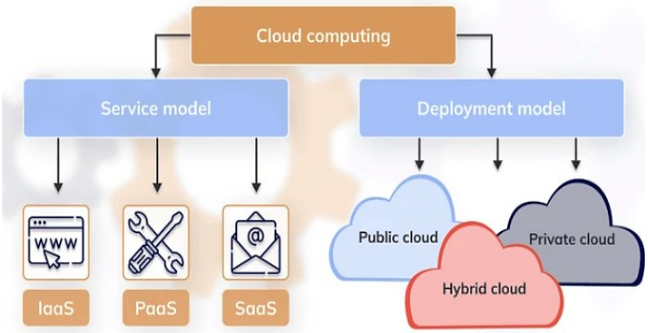

Fig. 1. Cloud Computing Architecture

To discover attack vectors and create efficient intrusion detection systems (IDS), it is imperative to comprehend their architecture:

- **Public Cloud:** Operated by third-party providers, public clouds offer scalable resources like servers and storage over the internet. They support multiple clients and are highly elastic. Examples include AWS, Azure, and Google Cloud.
- **Private Cloud:** Private clouds provide more protection and control and are dedicated to a single organization. They are perfect for regulatory compliance since they stay inside the company's firewall, whether they are hosted on-site or by a provider.
- **Hybrid Cloud:** Enables data and apps to flow across public and private clouds by combining them. Because of its adaptability, companies may grow while maintaining the security of critical processes.

C. *Cloud Service Models*

The three main service models offered by cloud computing are IaaS, PaaS, and SaaS:

1) *Infrastructure as A Service (IaaS):*

The foundational layer of cloud computing, Infrastructure as a Service (IaaS), offers virtualized resources over the internet, such as servers, storage, and networking. Using a pay-as-you-go paradigm gives consumers autonomy and freedom over their IT infrastructure. Operating systems, middleware, and applications are the responsibility of users, while providers oversee the hardware itself. Three well-known IaaS providers are Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS).

2) *Platform as A Service (Paas)*

Platform as a Service (PaaS) builds on the IaaS model by providing a complete development and deployment environment. It provides resources and services for creating, evaluating, and deploying apps without requiring management of supporting infrastructure. By abstracting infrastructure management, PaaS simplifies the development

lifecycle and accelerates deployment [16]. In order to facilitate the quick delivery of applications, providers usually provide a variety of databases, frameworks, and development tools. Amazon Elastic Beanstalk, Google App Engine, and Heroku are top PaaS providers.

3) Software as A Service (SaaS):

A cloud computing approach known as Software as a Service (SaaS) provides software applications online via a subscription mechanism. Through web browsers, users may access the programs, and the supplier maintains distant servers for this purpose. SaaS offers benefits such as lower costs, easy access, automatic updates, and scalability. Users don't have to handle software or hardware upkeep. Google Workspace, Microsoft 365, Salesforce, and Zoom are typical examples.

D. Threat Landscape in Cloud Environments

The cloud threat landscape is rapidly evolving, with cyber-attacks becoming more sophisticated and difficult to detect. Common targets include weak access controls, insecure APIs, and poor authentication mechanisms [17]. The rise of IoT devices further increases risks, as many lack adequate security and can serve as entry points for attackers. Once compromised, these devices can expose sensitive data and critical systems. To counter these threats, a robust security strategy is essential [18]. Protection must span all layers of the cloud, from physical infrastructure to applications and end-user devices. Important measures include multi-factor authentication (MFA), encryption of data both in transit and at rest, and continuous monitoring to find and immediately address vulnerabilities. As cyber threats continue to grow, organizations must remain vigilant to safeguard their cloud environments and digital assets.

E. Security Challenges in Multi-Tenant and Virtualized in Cloud Systems

Multiple users sharing the same physical infrastructure is known as multi-tenancy, and virtualization technologies such as hypervisors introduce unique security challenges in cloud environments [19]. Key issues include:

- Isolation breaches between virtual machines (VMs), potentially resulting in cross-tenant data leakage.
- Side-channel attacks that get private information by taking advantage of shared hardware resources.
- VM escape and hypervisor vulnerabilities, which may allow attackers to access the host or other VMs.
- Resource exhaustion and “noisy neighbor” effects, which degrade service performance and availability.

These challenges highlight the limitations of traditional security models [20]. The demand for sophisticated, flexible intrusion detection systems that can monitor in real time and mitigate threats in dynamic environments is therefore increasing, virtualized environments.

III. Intrusion Detection Systems (IDS)

Businesses can benefit from IDS by limiting the ability of cyberattacks and breaches to access or compromise their network infrastructure. In and of itself, an intrusion undermines and circumvents the CIA of systems' availability, confidentiality, and integrity. As wireless connection makes gadgets more generally available, dangers are expected to arise because wireless devices linked to the IoT are more vulnerable to intrusion than traditional networks [21]. Information security and privacy concerns are also mentioned in relation to IoTs, which emphasizes the necessity of IDS, particularly in IoT contexts, to prevent attacks that attempt to take advantage of weaknesses [22]. To ensure the security of their networks, Security defenses like firewalls and antivirus software are implemented by organizations, and IDS, among others. Nevertheless, these systems have disadvantages and restrictions. Firewalls, for example, guard against illegal access to private networks; they are not immune to malware or viruses.

A. Types of IDS: Host-based, Network-based, Hybrid

The three primary categories of intrusion detection systems (IDS) are based on the data source: network-based IDS (NIDS), which examines traffic across network segments; host-based IDS (HIDS), which keeps an eye on individual systems; and hybrid IDS, which integrates host and network data for a more thorough detection [23]. The following is a categorization of intrusion detection systems:

1) Host-based IDS (HIDS)

Host Intrusion Detection Systems (HIDS) are software programs that are placed on individual workstations or servers and monitor system activities. Such agents monitor the operating system, log events, and trigger an alert when suspicious activity is detected. HIDS would only be able to see what is happening on the particular device the HIDS is installed on and would not see what was going on throughout the network. They are frequently applied to secure important servers against intrusion attempts.

2) Network-based IDS

Network intrusion detection systems, or NIDS, employ a promiscuous NIC to monitor network traffic. They are installed at strategic locations within the network and identify attacks based on the packet information, using known or abnormal signatures. They are also called the packet sniffers and are used to protect all the devices on a segment, and can be deployed on the routers or other active network devices.

3) Hybrid-based IDS

The network-based and host-based IDS warnings are combined via central intrusion detection management. Although they are cheaper and easy to install, NIDS use known attack signatures. This renders them exposed to new and unfamiliar attacks that are difficult to detect.

B. Comparison of Traditional vs. Intelligent Intrusion Detection

Intrusion Detection Systems (IDS) form an essential element of contemporary cybersecurity infrastructures and, in particular, the dynamic and elastic settings of cloud-based computing [24]. The transition between conventional IDS technology and smart systems that rely on learning is a major change that occurred in the process of identifying and eliminating cyber risks.

1) Traditional Intrusion Detection Systems

The customary IDS largely relies on signature-based and rule-based methods. Such systems match inbound traffic or user activity with a pre-determined database of threat signatures of known threats or rules defined by experts. Although they are very useful to detect known attacks with a high probability of success and a low number of false positives, traditional IDSs are static, reactive and cannot be used to detect new or mutating threats like zero-day attacks [25]. The weaknesses of traditional IDS in the cloud include:

- **Inflexibility:** It takes considerable labor to create rules, and signature databases need to be updated often.
- **Scalability issues:** In large-scale cloud infrastructures, traditional IDS frequently have trouble keeping up with the amount and velocity of data.
- **Inability to detect anomalies:** These systems are oblivious to polymorphic assaults and previously unobserved behavior.
- **High False Negative Rate:** Especially common in contexts that are dynamic or dispersed.

2) Intelligent Intrusion Detection Systems

Intelligent IDS uses ML and DL techniques to provide adaptive, data-driven, and proactive threat detection to address the drawbacks of conventional methods. Unlike traditional IDS, these systems learn patterns from historical data and are capable of identifying anomalies, emerging attack vectors, and context-aware threats.

Key advantages of intelligent IDS include:

- Generalization capability: The capacity to identify known and unknown (zero-day) threats.
- Automation: Reduces dependency on manual rule updates by learning from data.
- Scalability: Better suited for high-volume environments typical in cloud computing.
- Real-time adaptation: Models can be updated continuously to adapt to new threats.

The requirement for sizable labelled datasets, the possibility of overfitting, issues with interpretability, and vulnerability to hostile assaults are some of the difficulties that intelligent IDS must overcome. Table I: Comparison of Traditional and Intelligent (ML/DL-based) Intrusion Detection Systems showing the main differences in detection abilities, scalability, and cloud-friendliness, is presented below:

TABLE I. TRADITIONAL IDS VS ML/ DL BASED IDS

Feature	Traditional IDS	Intelligent IDS (ML/DL-Based)
Detection Approach	Signature/Rule-based	Anomaly Detection and Pattern Learning
Novel Threat Detection	Limited	High (Zero-day, Evasive Attacks)
Dependency on Expert Rules	High	Low
Scalability	Poor	Good (Especially with DL)
Adaptability	Manual updates required	Automatic learning and adaptation
Real-time Capability	Moderate	High (with optimized models)
Interpretability	High	Moderate to Low (esp. Deep Learning)
Suitability for Cloud	Low to Moderate	High

The traditional IDSs are effective in detecting known threats, but are not as effective in cloud environments due to their lack of dynamic deployment. As opposed to this, intelligent IDS with the help of ML and DL is more adaptive, scalable, and accurate and suited to proactive cloud security. The transition signifies an approach towards being more automated and resilient cloud cybersecurity in the current cloud systems.

IV. MACHINE LEARNING AND DEEP LEARNING BASED INTRUSION DETECTION IN THE CLOUD

ML and DL enhance cloud intrusion detection because they can detect threats in real-time using an intelligent method. In contrast to conventional techniques, they are able to learn and adapt to changing patterns of attack, discover abnormalities, and minimize false alerts [26]. This suggests that they can flourish in dynamic multi-tenanting systems since they can handle sophisticated cloud data, which means better overall security and responsiveness. Figure 2 shows an example of a cloud-based AI that involves processing input data with neural networks and training models on the cloud, and sending the resulting data back to the processor.

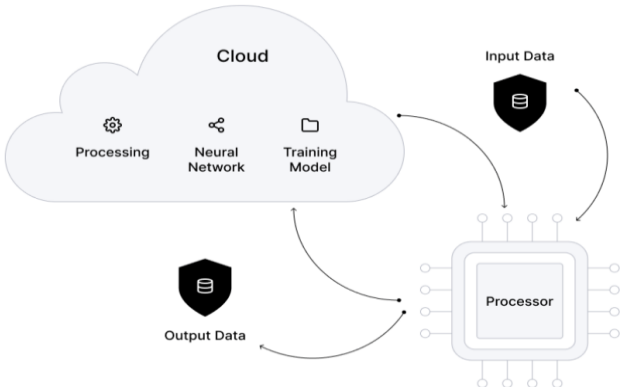

Fig. 2. Role of AI/ML in Cloud Computing

A. Supervised Learning Approaches

Supervised learning is the process of training models using labelled datasets, where the input attributes and corresponding output labels are known. These designations frequently correspond to recognised security events or threat classes in the context of cloud security [27]. With this method, the model may predict new, unknown data by learning patterns associated with particular hazard types or typical behaviour.

The following are common supervised learning techniques in cloud security:

- **Support Vector Machines (SVM):** SVMs are appropriate for analyzing complicated security data because of their exceptional performance in high-dimensional domains. SVMs to identify insecure Docker containers with 97.8% accuracy in detecting cloud infrastructure misconfigurations.
- **Random Forests (RF):** In order to handle complicated, non-linear connections in data and increase prediction accuracy, this ensemble learning technique integrates numerous decision trees.
- **Neural Networks (NN):** In cloud security applications, two DL models that have shown remarkable outcomes are CNN and RNN. Combining CNN and LSTM to identify malware in cloud systems.
- **Logistic Regression (LR):** Despite its ease of use, for cloud security binary classification tasks, LR is still often used. Strong interpretability is one of its key features, especially in security-related applications where rational decision-making is required.

B. Unsupervised Learning Techniques

In the absence of data labels, unsupervised algorithms are used to look for patterns in the unlabeled data. In the realm of

cloud security, where novel and unidentified dangers are always emerging, this is incredibly beneficial. With unsupervised learning, it possible to identify anomalies that deviate from the established pattern, perhaps revealing a new attack vector or zero-day vulnerability.

In the realm of cloud security, popular unsupervised learning techniques include:

1) Clustering Algorithms:

- **K-means:** Collects data points and divides them into k clusters according on how similar they are. It may be applied to cloud security to group comparable user activity and network traffic together.
- **Density-Based Spatial Clustering of Applications with Noise (DBSCAN):** It is very helpful in locating outliers, which might indicate unusual cloud activity.

This example proposes a hybrid clustering approach that combines K-means and fuzzy C-means for cloud system DDoS attack detection [28].

2) Dimensionality Reduction Techniques:

- **Principal Component Analysis (PCA):** It may be used to visualize high-dimensional security data and highlight important features that cause anomalies by reducing the data's dimensionality without sacrificing its variance.
- **t-Distributed Stochastic Neighbor Embedding (t-SNE):** They are especially useful for cloud security when it comes to showing high-dimensional data. Dashboards using graphical analytics.

3) Autoencoders:

Training neural networks to compress and decompress data. They could be applied to cloud security to detect abnormalities, that is, finding those points of data that cannot be successfully replicated.

4) Isolation Forests:

The data space is split randomly in an ensemble model in order to isolate the anomalies. In cloud security logs, it is very useful to detect rare events of infrastructure.

C. Feature Engineering and Selection in Cloud IDS

A very important process in the optimization of ML-based IDS performance and effectiveness is feature engineering. The most commonly used methods of reducing the dimension and retaining the significant features include mutual information, principal component analysis (PCA), and recursive feature elimination (RFE), which enhance the accuracy and computation speed of detection.

D. Deep Learning Architectures in Security

An ML framework known as DL uses multi-layered networks to discover the intricate patterns in very large data automatically. It has done particularly well in the intrusion detection of the cloud, where sophisticated attacks like the advanced persistent threats (APTs) and zero-day attacks can often go undetected by traditional security systems. CNN, RNN, and LSTM networks are DL models that can be used to record network traffic patterns both in space and time. Research indicates that intrusion detection systems using DL have a high accuracy rate of over 95% as compared to the conventional methods used in detecting the subtle and dynamic threats. The models remain relevant as they are always evolving to provide an autonomously increasing protection mechanism that fits the dynamic cloud environment.

E. AI-driven Proactive Threat Detection and Response Mechanisms in Cloud Security

The modern cloud security includes proactive threat detection, which is aimed at detecting possible threats before they become major ones. Unlike the reactive models, AI-based systems monitor cloud environments proactively and detect anomalies through anomaly detection to target abnormal behavior that shows malicious intentions [29]. This strategy is particularly important in the light of distributed and large-scale cloud infrastructures, as the number and sophistication of the threats keep increasing. Besides detection, AI plays a big role in incident response by automating it. These systems have the capacity of responding within a short time, most of the time without human input by completing predetermined procedures depending on the nature of the threat, such as putting under isolation infected systems [30]. AI-based response models may relieve security professionals, improve the effectiveness of cloud threat response, and expedite the process when paired with SIEM (Security Information and Event Management) solutions.

V. Literature Review

This section examines the latest developments in IDS, with a focus on proactive threat mitigation, cloud security, federated learning, and DL. It draws attention to new research issues, datasets, and developing approaches in IDS development.

Hakeem and Kim (2025) Provide a structured survey of the existing approaches to IDS in the V2X security, with particular emphasis on Federated Learning (FL) and Edge AI used to implement privacy-preserving and scalable IDS systems, conduct a systematic analysis and benchmark of IDS, identifying their limitations in terms of detecting zero-day attacks, and discuss the possibility of a more realistic and robust combination of real-world vehicular data and adversarial attack scenarios. One of the main novelties of this work is the discussion of computational complexities of IDS deployment such as sensor fusion strategies, noise elimination algorithms and false alarm mitigation measures and provide a detailed account of post quant cryptography and blockchain integration in increasing the security of the Federated Learning based IDS [31].

Aljuaid and Alshamrani (2024) offer a DL model that efficiently detects cyberattacks in the cloud environment by utilizing the most advanced model architecture in CNN-based model features. Some of the most important steps in the proposed CNN-based IDS include data collection, preparation, the SMOTE balance data strategy, feature selection, model training, testing, and evaluation of results. The proposed plan has shown impressive efficiency in securing cloud networks against different possible threats, as proved through experimentation. The potential of the model to detect and recognize any breach of the network has been found to be precise, accurate and recallable. Based on the comprehensive tests, the model can deploy cloud security and eliminate any risk that comes with changing security threats [32].

R et al. (2024) describe various features of cloud computing with specific reference to the privacy and security concerns that arise in logging and parsing EXIF information

and metatags. Proactive Cloud Security Threat Mitigation also emerges as a very crucial game changer in the contemporary cybersecurity scenario, where its ultimate aim is not only to prevent the immediate threats but also to avoid the forthcoming threats associated with the existence of the EXIF data and the metadata before they become actualized. Such a preemptive stance is enabled by the incorporation of advanced algorithms and predictive analytics in order to enable cloud security experts to have the upper hand over the evolving threats. This paper makes an in-depth analysis that encompasses motivation, purpose, creative solution, size and design of an aggressive cloud security model that is committed to logging and parsing of EXIF and metadata. The proposed system integrates the most up-to-date technologies to make the clouds with threats related to EXIF and metadata-related threats more secure and resilient and keep their integrity [33].

Azam, Islam and Huda (2023) introduce a comprehensive overview of the intrusion detection methods, a new IDS taxonomy and common assessment datasets. To enhance network security, it talks about the evasion methods of attackers and how difficult it is to resist the attacks. One of the attempts to better the capabilities of IDS is to enhance the ability to detect new intrusion activity, minimize false positives and detect the intruders correctly. The use of ML and DL in IDS systems has proven to be effective in detecting the attacker on networks in a short duration of time. challenges and provides a framework that can form the basis of future research capable of mitigating the weaknesses of the approaches. To determine the anomalies in results, including the results of a comparison survey, it is possible to recommend the decision tree as a way to accomplish the task because of its accelerated speed and simplicity. The research will aim at guiding the development of a powerful decision tree-based detection platform [34].

Mayuranathan et al. (2022) The hybrid DL scheme (EOS-IDS) introduced in this paper provides a very good optimum security scheme to detect intrusion in a cloud computing environment. In order to guarantee data quality by removing unnecessary information from the dataset, the IHO technique was used during the preparation stage. provide the chaotic red deer optimization (CRDO) strategy that takes care of the elimination of dimensions induced by the large data to achieve the best feature selection. It is suggested that the deep Kronecker neural network (DKNN) be used to detect and scan for cloud and intrusion assaults. To make sure the suggested EOS-IDS approach is effective, its performance is evaluated on two benchmark datasets, DARPA IDS and CSE-CIC-IDS2018, and contrasted with that of other successful IDS techniques already in use [35].

Adnan et al. (2021) Review IDSs from the perspective of ML. The three primary IDS issues under discussion are concept drift, high dimensionality, and computing complexity of an IDS in general and of an IDS in the IoT in particular. This includes a discussion of the present research dynamics as well as an investigation into solving each of the problems. Besides, in this research, they allocate a specific section in which they provide datasets of an IDS. Specifically, three important datasets have been made available: Kyoto, NSL, and KDD99. The research concludes that the three symmetry properties of idea drift, high-dimensional awareness, and computational awareness must be included in the neural network (NN)-based model of an IoT, IDS [36].

Table II summarizes key studies on AI-based anomaly detection in smart grids, which use approaches like DL, fuzzy logic, and quantum-inspired models to enhance anomaly detection accuracy for issues such as load shifts and unauthorized access.

TABLE II. SUMMARY OF KEY STUDIES ON PROACTIVE CLOUD SECURITY IN ML AND DEEP LEARNING-BASED IDS.

Reference	Study on	Approaches	Key Findings	Challenges	Limitations
Hakeem et al. (2025)	IDS in V2X security with emphasis on FL and Edge AI	Federated Learning, Edge AI, adversarial robustness, blockchain, post-quantum cryptography	Highlights zero-day attack detection gaps, benchmarks IDS datasets, and explores AI-based evasion	Adversarial robustness, scalability, false alarms, and dataset limitations	Lack of real-world vehicular datasets, complex deployment scenarios
Aljuaid et al. (2024)	Deep learning for cloud intrusion detection	CNN-based DL model, SMOTE, feature selection	High performance in attack detection with strong accuracy, precision, and recall	Efficient detection and classification of cyberattacks	Limited to CNN architecture; scalability across diverse cloud setups is not discussed
R et al. (2024)	Proactive security for EXIF and metadata in cloud environments	Predictive analytics, proactive threat mitigation, EXIF logging classification	Proposes a proactive framework using predictive models for metadata security	Anticipating and mitigating metadata-based threats	Focused mainly on EXIF data; generalizability to broader cloud threats is uncertain
Azam et al. (2023)	IDS taxonomy, detection techniques, dataset evaluation	ML/DL models, decision tree analysis, comparative survey	Decision tree suggested for anomaly detection; surveys ML/DL performance	Evasion techniques, false positives, and new threat detection	No empirical evaluation; primarily a theoretical framework
Mayuranathan et al. (2022)	Optimal hybrid IDS for cloud using DL	EOS-IDS using IHO, CRDO, DKNN; tested on DARPA, CIC-IDS2018	Effective feature reduction and classification; superior to existing IDS	High dimensionality, feature selection, and accuracy optimization	Model complexity, computational intensity, and practical deployment have not been validated
Adnan et al. (2021)	IDS in IoT using ML with emphasis on critical challenges	Review of ML models; focus on concept drift, dimensionality, and complexity	Identifies three major challenges; suggests research directions and dataset review	Concept drift, high-dimensional data, and computational complexity	No new IDS proposed; lacks practical implementation evidence

VI. CONCLUSION AND FUTURE WORK

AI-based techniques have become pivotal in strengthening cloud security by enabling proactive, intelligent, and real-time intrusion detection. Both ML and DL models have demonstrated remarkable accuracy in identifying cyber threats and significantly lowering false alarm rates compared to traditional detection methods. This survey highlights that, beyond enhanced threat detection, AI also supports the automation of incident response, allowing for rapid and

effective mitigation of security breaches. However, several challenges continue to hinder the widespread adoption of these technologies. These include the need for efficient handling of large-scale and heterogeneous cloud data, seamless integration with existing cloud infrastructures, and a lack of comprehensive validation in real-world, operational environments. The effectiveness of the development of cloud computing AI-driven intrusion detection systems heavily depends on overcoming these barriers and developing robust, scalable and practically deployable systems.

Further investigation is needed on developing ML/DL models that can be effective and lightweight on a real-time cloud system. It is also important to benchmark on various real-life datasets to assess the model's generalizability. The addition of hybrid AI models and the use of privacy-preserving techniques such as Federated Learning can also enhance the ability to detect and achieve system resilience. Also, it is advisable to focus more on the deployment analysis within practical scenarios such as vehicular networks and edge-cloud systems in order to analyze the operational effectiveness of the AI-based IDSs. In such a manner, the disconnect between research and actual application will be bridged, and an opportunity to see genuinely proactive and resilient cloud security measures will emerge.

REFERENCES

[1] V. Shah, "Managing Security and Privacy in Cloud Frameworks: A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, pp. 1–13, 2022, doi: 10.14741/ijcet/v.12.6.16.

[2] P. Srivastava, S. Singh, A. A. Pinto, S. Verma, V. K. Chaurasiya, and R. Gupta, "An architecture based on proactive model for security in cloud computing," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, 2011, pp. 661–666. doi: 10.1109/ICRTIT.2011.5972392.

[3] A. R. Duggasani, "Scalable and Optimized Load Balancing in Cloud Systems: Intelligent Nature-Inspired Evolutionary Approach," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 5, pp. 2153–2160, May 2025, doi: 10.38124/ijisrt/25may1290.

[4] S. Kabade and A. Sharma, "Cloud-Native AI Solutions for Sustainable Pension Investment Strategies," *Int. J. All Res. Educ. Sci. Methods*, vol. 13, no. 3, pp. 3930–3939, 2025.

[5] V. Shah, "Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks," vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[6] S. Majumdar *et al.*, "ProSAS: Proactive Security Auditing System for Clouds," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2517–2534, 2022, doi: 10.1109/TDSC.2021.3062204.

[7] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 3, pp. 6–18, Mar. 2025, doi: 10.48175/IJARSCT-23902.

[8] L. Yang, A. Shami, G. Stevens, and S. de Rusett, "LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in The Internet of Vehicles," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, IEEE, Dec. 2022, pp. 3545–3550. doi: 10.1109/GLOBECOM48099.2022.10001280.

[9] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA J. Autom. Sin.*, vol. 9, no. 3, pp. 377–391, Mar. 2022, doi: 10.1109/JAS.2021.1004261.

[10] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, 2023.

[11] T. Badgujar and P. More, "An Intrusion Detection System implementing Host based attacks using Layered Framework," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015, pp. 1–4. doi: 10.1109/ICIIECS.2015.7193122.

[12] M. Kaur and P. Garg, "Exploring Behavioral Patterns for Security in Cloud Computing: a Case Study," in *2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2025, pp. 720–725. doi: 10.1109/InCACCT65424.2025.11011337.

[13] A. Mishra, "AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 02, pp. 873–892, 2025.

[14] V. Singh, "Lessons Learned from Large-Scale Oracle Fusion Cloud Data Migrations," *Int. J. Sci. Res.*, vol. 10, no. 10, pp. 1662–1666, 2021.

[15] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[16] A. Joseph, "AI-Driven Cloud Security : Proactive Defense Against Evolving Cyber Threats," *World Acad. Sci. Eng. Technol. Open Sci. Index 209, Int. J. Comput. Inf. Eng.*, vol. 18, no. 5, 2024.

[17] V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," *Tech. Int. J. Eng. Res.*, vol. 11, no. 12, pp. 74–82, 2024.

[18] K. Juaind, "Threat Landscape in Cloud Computing: Cyber-Attacks, Device Vulnerabilities, and Information Security Solutions." 2019. doi: 10.13140/RG.2.2.35854.06726.

[19] D. Prava Sahu and B. L. Raina, "A Security Challenges in Multi-Tenant Cloud Computing: Exploring the Security Challenges of Multi-Tenant Cloud Computing," *J. Adv. Sch. Res. Allied Educ.*, vol. 15, no. 1, pp. 941–946, 2018.

[20] B. Chaudhari, S. C. G. Verma, and S. R. Somu, "Next-Generation Authentication and Authorization Models for Secure Financial Microservices APIs: Challenges, Innovations, and Best Practices," *Int. J. Curr. Sci.*, vol. 14, no. 1, 2024, doi: 10.56975/ijcsp.v14i1.303089.

[21] K. Coulibaly, "An overview of Intrusion Detection and Prevention Systems." 2020. doi: 10.48550/arXiv.2004.08967.

[22] B. K. R. Janumpally, "A Review on Data Security and Privacy in Serverless Computing: Key Strategies, Emerging Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, p. 9, 2025.

[23] K. Rajasekaran and K. Nirmala, "Classification and Importance of Intrusion Detection System," *Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 08, pp. 44–47, 2020.

[24] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," *Meas. Sensors*, vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[25] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[26] N. S. Kharbanda, "Comparative Review of Supervised vs. Unsupervised Learning in Cloud Security Applications," *Int. Res. J. Eng. Technol.*, vol. 11, no. 9, 2024.

[27] R. P. Sola, N. Malali, and P. Madugula, *Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention*. Notion Press, 2025.

[28] H. Kali, "The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[29] D. Patel and R. Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[30] S. Chitraju and G. Varma, "AI-Enhanced Cloud Security : Proactive Threat Detection and Response Mechanisms," no. December 2024, 2025, doi: 10.36948/ijfmr.2024.v06i06.31587.

[31] S. A. A. Hakeem and H. Kim, "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," in *IEEE Transactions on Intelligent Transportation Systems*, 2025, pp. 1–69. doi: 10.1109/TITS.2025.3558849.

[32] W. H. Aljuaid and S. S. Alshamrani, "A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing

Environments," *Appl. Sci.*, vol. 14, no. 13, p. 5381, Jun. 2024, doi: 10.3390/app14135381.

[33] R. V. R, P. KP, D. V. Hemamalini, and M. H. Khan H, "Proactive Cloud Security Threat Mitigation," *SSRN Electron. J.*, 2024, doi: 10.2139/ssrn.4824952.

[34] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[35] M. Mayuranathan, S. K. Saravanan, B. Muthusenthil, and A. Samydurai, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique," *Adv. Eng. Softw.*, vol. 173, p. 103236, Nov. 2022, doi: 10.1016/j.advengsoft.2022.103236.

[36] A. Adnan, A. Muhammed, A. A. Abd Ghani, A. Abdullah, and F. Hakim, "An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges," *Symmetry (Basel).*, vol. 13, no. 6, p. 1011, Jun. 2021, doi: 10.3390/sym13061011.

