Volume 12, No.6, June 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

AI AND MACHINE LEARNING FOR CLOUD SECURITY: A COMPREHENSIVE SURVEY OF IDS AND THREAT DETECTION METHODS

Mrs. Neha Upadhyay[1]

[1] Assistant Professor, Department of Computer Applications, IIS University, Bhopal (M.P.)
neha.upadhyay887@gmail.com

Abstract: Cloud computing becomes central to modern digital infrastructure, ensuring robust security has become paramount, particularly against sophisticated cyber threats targeting dynamic and multi-tenant environments. IDS struggle to meet the demands of cloud ecosystems due to scalability issues and limited adaptability. This study offers a thorough analysis of the use of machine learning and artificial intelligence techniques in enhancing IDS capabilities for cloud security. In order to better detect recognized and unidentified acts of violence, adjust to changing threats, and increase detection accuracy, the study examines unsupervised, supervised, and reinforcement models. It further investigates hybrid models that combine multiple learning paradigms for context-aware and scalable defense mechanisms. Deployment challenges in cloud environments, such as virtualization, real-time monitoring, and integration with orchestration tools, are also examined. Emphasis is placed on AI-driven IDS architectures that support elastic scaling, behavior-based threat analysis, and automated responses. The paper underscores the shift from reactive to proactive defense strategies enabled by intelligent systems. IDS solutions that are bright, flexible, and adaptable are essential as use of clouds increases. This review synthesizes current advancements and identifies future directions, including the development of lightweight models, enhanced explain ability, and secure AI frameworks tailored for cloud-based intrusion detection.

Keywords: Cloud Security, IDS, ML, Threat Detection, Hybrid Models, Real-Time Monitoring

1 INTRODUCTION

Cloud computing offers flexible, scalable, and affordable solutions, it has completely changed the IT environment. But this change also makes vital digital records more vulnerable to increasingly complex security threats. An essential line of defense for protecting cloud environments is provided by intrusion detection systems, or IDS [1]. Yet, traditional signature-based IDS approaches are frequently insufficient in addressing the complex, Cloud systems are changing and expansive.

The rise in cloud adoption has highlighted the limitations of conventional security mechanisms, originally designed for static, on-premises infrastructures [2]. The evolving threat landscape in cloud environments necessitates advanced security approaches ability to identify and react in real-time [3]. In this context, AI and ML have garnered increasing attention for their potential to automate threat detection, recognize unusual patterns and behaviors, and adapt continuously to new and unknown attacks.

Recent developments in detection of breaches using ML and DL and Prevention Systems offer promising capabilities. However, challenges persist, particularly in terms of their real-time adaptability, reliance on outdated or incomplete datasets, and limited evaluation under realistic threat scenarios. Issues for trust and transparency are also raised by the truth that many machine learning algorithms are black-box. Thus, explicable the use of AI has emerged as a key element. with the goal of boosting analysts' trust in model judgments [4]. Furthermore, privacy-preserving techniques such as federated learning are gaining traction by enabling collaborative IDS training without centralizing sensitive data. Simultaneously, the rise of adversarial machine learning where attackers exploit model vulnerabilities through crafted inputs emphasizes the pressing requirement for strong and durable defenses.

Despite the progress, there remains a substantial gap in evaluating the practical deployment and efficiency of IDSs built around machine learning and deep learning in cloud IoT contexts. A comprehensive examination of existing methods [5], their performance, challenges [6], and future directions is essential to bridge this gap and to inform the creation of cloud-based security measures that are smart, safe, as well as flexible.

1.1 Structure of the Paper

The paper is structured as follows: Section 2 discusses the basics of IDS and cloud security. Section 3 explains AI/ML methods for IDS. Section 4 draws attention to implementation issues. Section 5 reviews recent IDS studies, and Section 6 concludes with insights and future directions.

2 FUNDAMENTALS OF CLOUD SECURITY AND INTRUSION DETECTION SYSTEMS

Cloud computing has revolutionized digital infrastructure by offering scalable, on-demand access to resources, but it also introduces complex security challenges [7]. As cloud adoption rises, so do concerns around data breaches, privacy, and insider threats. Traditional security tools often fall short against dynamic and distributed cloud environments. These days, surveillance systems, or IDS, are crucial instruments for identifying both known and unknown threats, particularly those driven by machine learning and artificial intelligence. Understanding cloud architectures, evolving threat landscapes, and IDS classifications, misuse, anomaly, and hybrid detection provides a foundational basis for developing intelligent, adaptive security mechanisms suited for modern cloud infrastructures.

2.1 Cloud Computing Architectures and Security Models

Computer peripherals and assets are now accessible in greater numbers, more powerful, more inventive, more ubiquitous, and easier to reach than ever before due to the general growth in technical innovation and internet usage [8]. As a result, people, companies, businesses, governments organizations and businessmen are adopting these rapidly changing digital infrastructure without taking into account the dangers it presents and sharing their personal and business data not worrying about privacy loss. A structure for granting network users access to a common pool of computer resources that may be reconfigured in an everywhere, accessible, and instant manner. Three kinds of services, four deploying methods, and five key features make up this cloud-based model show Figure 1.

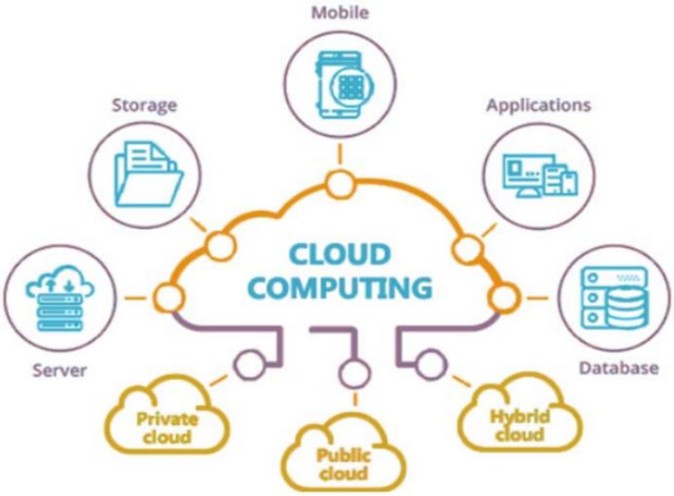

Figure 1: Architecture of Cloud Computing

Instead of using local servers or individual gadgets to manage apps, a cloud-based system shares computer resource. Generally speaking, there are four installation strategies and three service kinds that cloud computing technology may provide. Types of service delivery includes:

- **IaaS:** Digital Ocean, Linode, and Rackspace are a few such, and Amazon [9].
- **PaaS:** These consist of development platforms and management systems. Google App Engine's OpenShift.
- **SaaS:** For example, Microsoft Office 365, Zoom, Drive, Cisco Web-x, and GoToMeeting.

The public, private, communal, and hybrid deployment modes are among them. Each of these models has unique characteristics, and the installation model is determined by the goals of the cloud-based user [10]. The end user is advised to examine the models' safety, dependability, and efficiency concerns prior to agreeing to a model installation.

2.2 Threat Landscape in Cloud Environments

The introduction of cloud-based computing has changed the digital technology environment. This article explores the complex interrelationship between cybersecurity and CC, providing a thorough examination of the changing risk environment and the countermeasures used. Cloud-based settings are crucial, and networks are essential to their security [11], explaining the many methods of cybersecurity used to protect prevent possible threats. The inability of conventional safety precautions to fend off sophisticated attackers has led to the development of anomaly-based systems for intrusion that use machine learning techniques.

Machine learning-based malware identification techniques, explaining how they may learn on their own and adjust to changing risks. The paper highlights the importance of appropriate feature selection techniques to optimize model performance and reduce issues with imbalanced data by evaluating the efficacy of supervised machine learning algorithms in detecting different kinds of assaults [12]. One essential element in guaranteeing the defense of customer information and resource resources against possible security breaches is the intrusion detection system. It is an advanced security solution intended to protect network information from malicious activity.

2.3 Intrusion Detection Systems in Cloud Environments

This is now essential to put in place systems that can recognize and stop illegal activities within networks due to the growing sophistication and prevalence of cyberthreats. Since they offer a proactive line of protection IDS, are essential components of contemporary security designs (shown in Figure 2) [13]. IDSs may actively track and evaluate traffic on the network, identifying trends of odd or unusual behavior that could reveal hazards that are undiscovered or unidentified, in contrast to more traditional preventative measures like antivirus or firewall software, which try to block known threats. and new attacks.

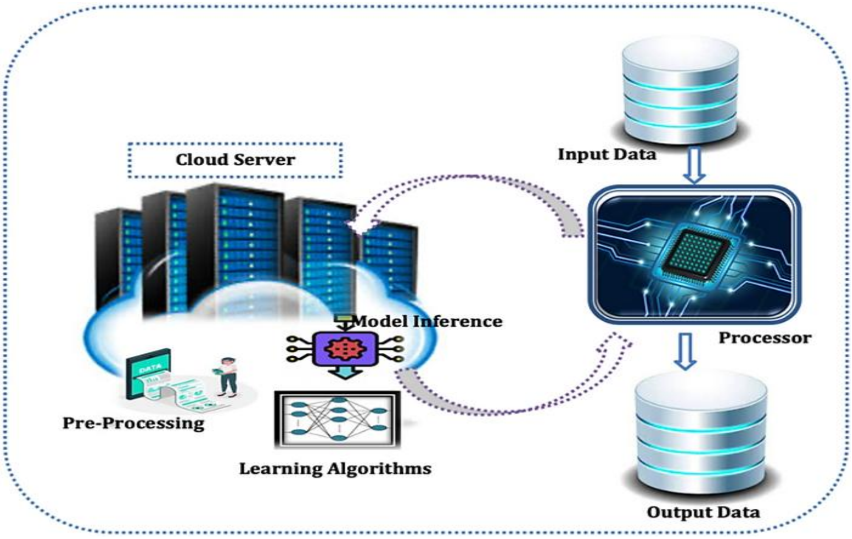

Figure 2: Intrusion Detection Systems

IDS recognition comes in three varieties, which are as follows:

- **Identification of Misuse:** Alternatively referred to as a signature. There are three types of IDS identification, that are outlined below: Re-detection looks for established patterns of network or host infiltration. Every assault has a unique signature, which might be the packet's content, the originating IP address, or a particular header.
- **Identifying Anomalies:** establishes an initial or typical situation for the host or network, from which any change is seen as a possible attack. By looking at regular internet traffic, including the services each host offers, the services each host uses, and the amount of activity throughout the day, Security measures that rely on anomalies can provide a baseline.
- **Hybrid Surveillance:** include the two identifications stated above [14]. It can find novel assaults and often have a lower false finding rate than anomaly approaches.

3 AI AND MACHINE LEARNING TECHNIQUES FOR IDS IN CLOUD

Artificial intelligence. Cloud-based IDS has undergone a revolution because to AI and ML, which make threat detection more intelligent, flexible, and scalable. While reinforcement learning improves IDS flexibility through real-time feedback, Systems for supervised and unsupervised learning can detect both new and established risks [15]. Hybrid models offer accurate identification in dynamic multi-tenant systems by fusing many learning paradigms. IDS is further enabled by deep learning to handle high-dimensional traffic data, increasing accuracy and decreasing false positives. These AI-powered methods are essential for protecting cloud infrastructures from advanced assaults because they represent a change from static detection to proactive protection.

3.1 Supervised and Unsupervised Learning Approaches

Regarding Both of these learning techniques are essential for enhancing IDS efficacy in security in the cloud. Supervised learning refers to the training of a model using labeled data where the type of attacks is known and well identified. This has been an effective method since it has a high rate of accuracy when identifying threats that have been seen before. Popular algorithms are SVM, Decision Tree, Random Forest, and ANNs [16]. Such models can learn rich representations and especially when large well-labeled intrusion data like NSL-KDD, CICIDS2017, and UNSW-NB15 are available.

Unsupervised approaches, as opposed to supervised models, are focused on identifying anomalies in terms of deviation with respect to typical behavior training rather than requiring data with labels. Such methods K-Means Clustering, Separation, automatic encoders, and Principal Component Analysis Forests are often utilized. Such techniques are especially effective in identifying zero-day attacks, malicious insiders, and data exfiltration efforts, where previous examples of these can be non-existent.

The necessity to use both supervised and unsupervised approaches is motivated with the fact that cloud environment is continuously changing with various traffic patterns and new vulnerabilities [17]. Therefore, the hybrid IDS models, integrating both learning paradigms, are beginning to appear as the effective solution. The advantage of these systems is that they have the high detection accuracy associated with supervised learning and the flexibility of unsupervised learning to detect unknown threats.

3.2 Reinforcement Learning and Hybrid Models

The Reinforcement Learning (RL) provides an adaptive learning process to the Intrusion Detection System (IDS) because it interacts with the cloud environment and gets better at threat detection based on reward feedback [18]. RL allows IDS to deal with unfixed and changing attacks in a real time fashion. Supervised, unsupervised, and RL methods are also used together (hybrid models), and deployed to achieve better accuracy and scalability in multi-tenant cloud environments. The models solve the weaknesses of the single approaches by combining the merits of precision, ability to detect anomalies and adaptability. The combination of RL and hybrid models enables cloud IDS to have the ability of context-aware, proactive security intelligence.

There is growing interest in hybrid models, integrating several learning paradigms, e.g., supervised, unsupervised, and reinforcement learning, due to their strength and ability to be applied broadly in cloud security settings [19]. The benefits of each type of learning are combined in these models: Unsupervised methods expose irregularities, supervised learning accurately identifies known dangers, and reinforcement learning makes it possible to adapt to new attack methods.

Hybrid model's Specific hybrid models are especially important in multi-tenant cloud systems where workloads and access patterns can differ dramatically. On the whole, reinforcement learning and hybrid techniques are the future of intelligent IDS in clouds, capable of providing proactive, scale-out, and context-aware defense mechanism.

3.3 Comparative Analysis of AI/ML Models for IDS

Modern detection systems for intrusions must be implemented in order to protect vital information infrastructure in the modern digital environment due to the proliferation and sophistication of cybersecurity threats.

Addressing the shortcomings of conventional methods has advanced significantly with the incorporation of artificial intelligence into IDS [20]. IDS can more accurately respond to new and changing threats because to AI approaches, especially ML and DL, which provide sophisticated capabilities for pattern identification and anomaly detection [21]. Deep learning, a type of machine learning that analyzes complex data using multi-layered neural networks, enhances IDS's capabilities with high dimensions.

AI's ability to solve a number of significant issues that traditional systems confront makes it a compelling addition to IDS. Real-time data allows AI-powered IDS to continually update their models in response to emerging threats, increasing detection accuracy and decreasing false positives.

4 IDS DEPLOYMENT IN CLOUD ENVIRONMENTS

Deploying IDS presents particular difficulties in cloud systems because of multi-tenancy, elasticity, and virtualization. Effective IDS integration requires compatibility with virtual machines, containers, and orchestration tools, while maintaining full network visibility and regulatory compliance. AI and ML-powered IDS solutions address scalability and performance constraints through distributed architectures and real-time analytics. These intelligent systems adapt to dynamic traffic, enabling proactive detection of sophisticated dangers like zero-day attacks and lateral movements. With capabilities like auto-scaling, automation, and behavior-based learning, AI-enhanced IDS provide resilient, low-latency defenses crucial for maintaining security in rapidly evolving cloud infrastructures.

4.1 Integration of IDS in Cloud Infrastructure

The Intrusion Detection Systems (IDS) deployment in cloud infrastructure poses some peculiar problems and opportunities due to the dispersed, multi-tenant, and virtualized characteristics of the cloud [22]. In contrast to the classic on-premise solutions, cloud environments necessitate the smooth integration of IDS into virtual machines (VMs), containers, and orchestration planes, e.g., Kubernetes. It should be integrated with the minimum impact on cloud services and give complete visibility across the network traffic, VM-to-VM communications, and API calls, due to the emergence of Infrastructure-as-a-Service (IaaS) and Software-defined Networking (SDN) [23]. Appropriate integration of IDS enhances visibility of threats, minimizes the time needed to respond to an incident and provides compliance with data security regulations on dynamic cloud environments.

- **Dynamic Placement:** IDS can be deployed at various layers host-based, network-based, or application-level depending on cloud architecture.
- **Virtualization-Aware:** Integration must support hypervisors, VMs, containers, and service meshes commonly used in cloud-native environments.
- **Scalability:** IDS must scale horizontally with cloud workloads and remain effective under high traffic volumes.
- **Automation:** Integration with orchestration tools (e.g., Terraform, Kubernetes) enables auto-deployment and lifecycle management of IDS instances.
- **Visibility & Compliance:** IDS provides visibility into east-west and north-south traffic, aiding in monitoring, forensic analysis, and regulatory compliance.

4.2 Scalability and Performance Considerations

Performance and scalability play critical roles in the effective implementation of IDS in cloud structures. The cloud environments are known to be elastic, with high data flows and dynamically scaled workloads. An IDS to this effect should have the capacity to scale with the varying traffic loads without compromising the system performance or creating a latency in the detection. Conventional IDS products can fail in these circumstances because centralized processing can create a bottleneck and because they cannot scale horizontally [24]. The AI and machine learning-based IDS architectures can alleviate these problems using distributed processing, microservices, and parallelism to achieve real-time detection at a reduced computational load.

- **Elastic Scaling:** IDS should be able to support auto-scaling to accommodate real time changes in workloads.

- **Real-Time Detection:** It is important to have low-latency security threat responses without compromising on the accuracy.
- **Resource Efficiency:** Lightweight and optimized ML models can aid in reducing CPU, memory and storage overheads.
- **Distributed Deployment:** The fault tolerance and load balancing needs of IDS components should be addressable by deploying those components in several zones or regions.
- **Precision-Performance Balance:** Scalable intrusion detection systems ought to have low false alarm rates, short recognition latency as well as along with excellent precision for detection [25].

4.3 Real-Time Threat Detection and Response

Safety in the cloud relies heavily on immediate risk assessment and control to ensure service continuity and limit the damage caused by highly organized cyberattacks. Analysis of distributed, huge traffic in the cloud can be a problem with traditional IDS systems since they can be slow and inefficient [26]. AI and machine learning technologies, however, permit actual time data processing and analysis by IDS learning behavioral patterns and discovering anomalies on the fly. This cloud workload proactive detection mechanism enables quick identification of zero-day attacks, insider threats, and lateral movement in cloud workloads [27]. Models that use machine learning, specifically recurrent neural network (RNNs), online learning algorithms and ensemble methods, are particularly well adapted to real-time analysis because they are flexible and continually learn.

- **Continuous Monitoring:** AI-based IDS performs anomaly detection in live traffic in real time.
- **Faster Response Times:** ML-based actions are automated to reduce manual operations.
- **Zero-Day Attack Identification:** The unknown or adaptive threats can be detected by behavioral learning.
- **Integration with Orchestration Tools:** Enables automated, smooth defensive response throughout the cloud elements.
- **Lower Operational Impact:** Reduces unplanned outages and degraded service with instantaneous response patterns.

5 APPLICATIONS AND CHALLENGES WITH ADVANCES OF CLOUD-BASED IDS AND THREAT DETECTION

IDS have emerged as essential components in the modern cyber-security landscape, particularly due to the dynamic, distributed, and scalable nature of cloud environments. The integration of AI, ML, and deep learning with cloud-based IDS has significantly improved the accuracy, adaptability, and real-time capabilities of threat detection [28]. This section discusses major applications and the pressing challenges associated with the development and deployment of advanced cloud-based IDS.

- Real-Time Threat Detection Cloud-based IDS solutions enable continuous monitoring of massive, high-velocity data streams generated by virtual machines, containers, and APIs. By leveraging real-time analytics, these systems can detect anomalies, zero-day attacks, and malware propagation with minimal latency.
- Multi-Tenant Security Monitoring Cloud IDS supports multi-tenant architectures by providing isolated, scalable detection capabilities across multiple clients. This allows CSPs to implement shared but secure IDS systems using role-based access and custom rules.
- Integration with DevSecOps Pipelines Modern IDS tools in the cloud can be embedded into DevSecOps workflows, allowing security policies to be enforced during development and deployment phases [29]. This supports continuous integration and continuous delivery (CI/CD) without compromising security.
- Data Privacy and Confidentiality IDS systems in the cloud process sensitive data, which can raise concerns regarding data privacy, regulatory compliance (e.g., GDPR, HIPAA), and confidentiality breaches. Ensuring that intrusion detection does not violate tenant data sovereignty remains a complex challenge.
- Encrypted Traffic Analysis The increasing use of encryption protocols (e.g., TLS 1.3, VPNs) limits the ability of cloud-based IDS to inspect packet content. Advanced techniques such as TLS fingerprinting and metadata analysis are being explored but remain immature.
- Adversarial Machine Learning ML-based IDS are vulnerable to adversarial attacks, where carefully crafted inputs can mislead models. Securing AI pipelines and improving model robustness against evasion and poisoning attacks is a growing concern.

6 LITERATURE OF REVIEW

The following section reviews the research on machine learning and artificial intelligence uses for secure cloud services, emphasizing model topologies, adversarial resistance, explainability, and intrusion detection techniques.

Bankó et al. (2025) explains how different datasets affect model performance and how they are used to train and assess ML models for identifying DDoS attacks in IoT networks. Additionally, the results indicate that filtered datasets and lightweight machine learning techniques are preferred because of equipment constraints. Present indicators suggest that more sophisticated ML models, like deep learning, are still going to get traction with bigger or particular to an industry datasets. With SDNs providing flexibility, edge computing being thoroughly investigated in cloud-based settings, and blockchain-integrated networks emerging as a potential strategy for boosting protection, this highlights the demand for reliable and flexible installation alternatives [30].

Abdel-Wahid (2024) examines how to improve the identification of threats, avoidance, and reaction capacities in wireless security solutions by integrating AI and ML approaches. The study explores the main factors that are driving the adoption of AI-powered cloud security, such as the requirement for real-time, adaptive security solutions, the exponential increase of cloud-based data and applications, and the rising incidence of sophisticated persistent threats. It looks at how massive volumes of security-related data may be analyzed using AI and ML algorithms to find abnormalities and identify new risks more quickly and accurately than with conventional security methods [31].

Kikissagbe and Adda (2024) examine several ML techniques, including supervised, unsupervised, deep learning, and hybrid models, for identifying breaches in Internet of Things platforms. Conventional systems for intrusion detection (IDSs) frequently don't perform well with the diverse and constantly shifting networks that make up the Internet of Things. A possible answer to these problems is ML, which provides the level of intelligence and adaptability required to combat intricate and dynamic dangers. It evaluates their usefulness, drawbacks, and real-world uses, emphasizing how machine learning might improve IoT system security. The report also looks at present patterns and concerns in the market, emphasizing the need of continuing research to stay up with the ever-changing IoT security environment [32].

Hernandez-Ramos et al. (2023) provide a thorough, up-to-date taxonomy for FL-enabled IDS techniques that is based on a thorough review of the literature from 2018 to 2022. The discussion includes an examination of the primary ML models, datasets, aggregation functions, and application collections that are used by the suggested FL-enabled IDS techniques. By using machine learning techniques to identify more complex cybersecurity assaults concealed in large data, intrusion detection systems (IDSs) have seen significant development in recent years. These methods, however, have historically relied on consolidated education structures, where data centers receive end-node data for processing [33].

Zhang et al. (2022) provide a thorough analysis of the most recent research on XAI techniques for cybersecurity systems. Artificial intelligence, including ML and DL, has been widely used in the domains of cybersecurity, such as identifying breaches, virus identification, and spam filtering, as a result of the quick growth of devices with Internet access. Yet most machine learning-based as well as DL-based methods are carried out in a black-box fashion, even though AI-based methods for detecting and defending against internet attacks and risks are more sophisticated and effective than traditional based on signatures and based on rules cybersecurity strategies [34].

Alatwi and Morisset (2021) examine the studies that use various facets of competitive ML in the field of discovering network breaches to offer guidance for possible fixes. The assessed research is first grouped according to how well they contribute to the creation of hostile instances, assess how resilient machine learning NIDs are to instances of adversary, and then protect these models from such attacks. In addition, they emphasize the features discovered in the studied study. Because of this flaw, hackers can target NIDSs by subtly altering illicit traffic in order to avoid identification and interfere with the system's essential operations. The subject of deep adversarial training has been widely researched in the computer vision arena; nevertheless, it is still an area of open study in network security applications [35].

Table 1 summarizes key studies on AI and machine learning techniques for intrusion detection in cloud environments, highlighting focus areas, methodological approaches, core findings, limitations, and potential directions for future research.

Table 1: Comparative Analysis of Recent Studies on AI and ML Techniques for Intrusion Detection in Cloud Environments

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Bankó et al. (2025)	Datasets and ML model performance for DDoS detection in IoT	Lightweight ML models, Preprocessed datasets, SDNs, Edge computing	Preprocessed lightweight models perform better in constrained environments; industry-specific datasets improve detection	Hardware limitations in IoT; lack of standard datasets	Blockchain-integrated networks and scalable IDS deployment strategies
Abdel-Wahid (2024)	AI/ML integration in cloud-based security	AI/ML for threat detection and response	AI/ML enhances real-time detection, precision, and adaptability to advanced threats	Managing real-time analysis of massive cloud data	Adoption of adaptive and self-learning cloud IDS frameworks
Kikissagbe and Adda (2024)	ML approaches for IDS in IoT systems	Supervised, Unsupervised, Deep Learning, Hybrid models	ML improves detection accuracy and flexibility over traditional IDS	Lack of robustness in dynamic, heterogeneous environments	Developing intelligent hybrid IDS tailored for IoT-cloud ecosystems
Hernandez-Ramos et al. (2023)	Federated Learning (FL) for IDS	Federated ML models and decentralized IDS architectures	FL avoids data sharing, enhances privacy, and enables collaborative threat detection	Integration complexity, limited model transparency	Refining aggregation strategies and expanding FL adoption in cloud IDS
Zhang et al. (2022)	Explainable AI in cybersecurity	XAI for IDS, DL-based methods	AI offers advanced detection capabilities but lacks explain ability	Black-box nature of DL/ML models reduces trust and interpretability	Enhancing transparency with interpretable ML models in IDS
Alatwi and Morisset (2021)	Adversarial ML in Network IDS	Evaluation and defense against adversarial attacks	ML-based IDS are vulnerable to adversarial inputs that can bypass detection	High susceptibility to minor perturbations; lack of robust defenses	Designing resilient ML models resistant to adversarial manipulation

7 CONCLUSION AND FUTURE WORK

In conclusion, smart safety measures are becoming ever more essential in current digital landscapes to protect critical cloud-based systems. The incorporation of machine learning and artificial intelligence into wireless malware Identification systems has increased due to the rising need for protection from threats that is adaptable, extensible, and instantaneously. In addition to improving detection accuracy, intelligent models are turning cloud security from a reactive to a proactive approach. This analysis highlighted the need for sophisticated, AI-driven detection techniques by examining the changing environment of cloud security threats and the limitations of conventional IDS. In addition to mixed and deep learning algorithms designed for identifying anomalies, risk reaction, and adaptability in decentralized contexts, it investigated a broad variety of machine learning approaches, which includes supervised, unsupervised, and reinforcement learning. Additionally, for practical use, the significance of installation methodologies, optimized performance, and immediate identification was emphasized. The creation of strong, smart IDS for the cloud will be further influenced by future developments in artificial intelligence, supervised learning, and adversarial robustness.

Future research should focus on building security experts' trust by improving the clarity of AI-driven IDS using comprehensible models and presentation approaches. Federated learning developments can provide cooperative IDS training across cloud settings while protecting data privacy. Furthermore, developing more resilient, adaptable, and smart cloud security frameworks will require tackling adversarial machine learning risks and enhancing real-time adaptation in changing threat environments.

REFERENCES

[1] D. Gangwani, H. A. Sanghvi, V. Parmar, R. H. Patel, and A. S. Pandya, "A Comprehensive Review on Cloud Security Using Machine Learning Techniques," *Intell. Syst. Ref. Libr.*, vol. 240, no. January 2024, pp. 1–24, 2023, doi: 10.1007/978-3-031-28581-3_1.

[2] T. Sowmya and E. A. M. Anita, "A comprehensive review of AI based intrusion detection system," *Meas. Sensors*, 2023, doi: 10.1016/j.measen.2023.100827.

[3] Q. O. Ahmed, "Machine Learning for Intrusion Detection in Cloud Environments: A Comparative Study," *J. Artif. Intell. Gen. Sci. ISSN3006-4023*, vol. 6, pp. 550–563, 2024, doi: 10.60087/jaigs.v6i1.287.

[4] S. Neupane *et al.*, "Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities," *IEEE Access*, vol. 10, pp. 112392–112415, 2022, doi: 10.1109/ACCESS.2022.3216617.

[5] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3220622.

[6] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[7] J. Thomas, K. V. Vedi, and S. Gupta, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[8] A. Goyal, "Optimising Cloud-Based CI/CD Pipelines: Techniques for Rapid Software Deployment," *Tech. Int. J. Eng. Res.*, vol. 11, no. 11, pp. 896–904, 2024.

[9] 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.

[10] S. S. Nasim, P. Pranav, and S. Dutta, "A systematic literature review on intrusion detection techniques in cloud computing," *Discov. Comput.*, vol. 28, no. 1, p. 107, 2025, doi: 10.1007/s10791-025-09641-y.

[11] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions," pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

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

[13] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," *Computers*, vol. 14, no. 3, 2025, doi: 10.3390/computers14030087.

[14] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," *Glob. J. Eng. Technol. Adv.*, vol. 14, no. 2, pp. 155–158, Feb. 2023, doi: 10.30574/gjeta.2023.14.2.0031.

[15] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," *ESP J. Eng. Technol. Adv.*, vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

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

[17] S. P. Bheri and G. Modalavalasa, "Advancements in Cloud Computing for Scalable Web Development: Security Challenges and Performance Optimization," *JCT Publ.*, vol. 13, no. 12, pp. 01–07, 2024.

[18] H.-S. Yoon, "Review on Reinforcement Learning-Based Energy Management Strategies for Hybrid Electric Vehicles," *Evol. Mech. Eng.*, vol. 4, 2022, doi: 10.31031/EME.2022.04.000579.

[19] S. Kabade and A. Sharma, "Intelligent Automation in Pension Service Purchases with AI and Cloud Integration for Operational Excellence," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 725–735, Dec. 2024, doi: 10.48175/IJARSCT-

14100J.

[20] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[21] 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*, 2023, doi: 10.1109/ACCESS.2023.3296444.

[22] 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.

[23] B. C. Preethi, R. Vasanthi, G. Sugitha, and S. A. Lakshmi, "Intrusion detection and secure data storage in the cloud were recommend by a multiscale deep bidirectional gated recurrent neural network," *Expert Syst. Appl.*, vol. 255, Dec. 2024, doi: 10.1016/j.eswa.2024.124428.

[24] V. S. Thokala and S. Pillai, "Optimising Web Application Development Using Ruby on Rails, Python, and Cloud-Based Architectures," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, pp. 630–639, 2024, doi: 10.5281/zenodo.14576620.

[25] A. Bondi, "Characteristics of Scalability and Their Impact on Performance," in *Proceedings Second International Workshop on Software and Performance WOSP 2000*, 2000, pp. 195–203. doi: 10.1145/350391.350432.

[26] V. Jain and A. Mitra, "Real-Time Threat Detection in Cybersecurity: Leveraging Machine Learning Algorithms for Enhanced Anomaly Detection," 2024, pp. 315–344. doi: 10.4018/979-8-3693-7540-2.ch014.

[27] P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[28] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. P. Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.

[29] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," *J. Adv. Dev. Res.*, vol. 11, no. 1, 2020.

[30] M. B. Bankó *et al.*, "Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges," *Algorithms*, vol. 18, no. 4, 2025, doi: 10.3390/a18040209.

[31] T. Abdel-Wahid, "AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention," *Int. J. Inf. Technol. Electr. Eng.*, vol. 13, no. 3, pp. 11–19, 2024.

[32] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," *Electronics*, vol. 13, no. 18, p. 3601, Sep. 2024, doi: 10.3390/electronics13183601.

[33] J. L. Hernandez-Ramos *et al.*, "Intrusion Detection based on Federated Learning: a systematic review," 2023, doi: 10.48550/arXiv.2308.09522.

[34] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[35] H. A. Alatwi and C. Morisset, "Adversarial Machine Learning In Network Intrusion Detection Domain: A Systematic Review," pp. 1–21, 2021.