IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

AI-Based Intrusion Detection and Prevention in Cloud Security: A Comprehensive Review

Dr. Jvalantkumar Kanaiyalal Patel
Assistant Professor, Department of Computer of Application
Shri Manilalkadakia College of Commerce, Management, Science and Computer Studies, Ankleshwar
Jvalant007@gmail.com

Abstract: *CloudComputing has proven to be an essential technology for today's organizations due to its scalability, flexibility and cost-effectiveness. However, with the cloud services trend comes the increased threat of high-level attacks like DoS, insider threats, malware and unauthorized access. Typically, signature-based Traditional Intrusion Detection and Prevention Systems (IDPS) are not effective in detecting zero-day attacks and attacks that have evolved over time in dynamic cloud environments. This in-depth analysis delves into how AI can improve intrusion detection and prevention systems in cloud security. The study explores different AI methods such as ML, DL, supervised, unsupervised, semi-supervised, and hybrid models, and their contributions to anomaly detection, threat prediction, and adaptive security. The review also addresses different types of IDS, attacks during the cloud era, real-time threat detection and adaptive learning. The topics of current issues such as data privacy, scalability, explainability and compliance, are also addressed. The results show that AI-powered IDPS can enhance the accuracy of detections, minimize false alarms, and bolster proactive cloud security measures against new threats..*

Keywords: Artificial Intelligence (AI), Cloud Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Machine Learning, Deep Learning

I. INTRODUCTION

With the growing ubiquity of cloud computing, the storage, processing, and managing of data have shifted in the business and private sectors [1]. Cloud environments provide for scalability, cost-effectiveness and flexibility, which are fundamental elements of modern IT infrastructure[2][3][4]. It has also transformed the digital world by enabling people to access computing power, storage, networking, databases and software applications on demand, via the internet. Cloud platforms can facilitate the deployment of services quickly, lower infrastructure expenses, and enhance operational efficiency for businesses. The increasing adoption of technologies like the IoT, Big Data Analytics, AI, and edge computing has contributed to the need for cloud-based infrastructures[5][6][7]. The continuing growth of cloud services makes it vital to industries like finance, healthcare, education, e-commerce, and enterprise management, where access must be continuous to data and services[8][9].

Although there are benefits to cloud computing environments, they also have significant cybersecurity issues from a distributed and shared architecture. Cloud systems are made up of several users, virtual machines, and interdependent services, making them appealing targets for cybercriminals. Denial-of-service (DoS) attacks, insider threats, phishing, malware infections, unauthorized access, hypervisor attacks, and data breaches are common threats [10][11]. Cloud technologies are dynamic and multi-tenant, adding to the complexity of security management, which makes traditional security mechanisms inadequate to effectively tackle new cyber threats. Further, there are growing complexities in cyber threats, such as zero-day attacks and APTs, which have revealed the weaknesses of traditional rule-based and signature-driven security approaches.

IDPS are now important tools for detecting malicious activity and for monitoring network activity and protecting cloud infrastructures from cyber attacks[12][13]. Traditional IDPS are primarily based on signature-based techniques and a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

set of rules. As useful as they may be against known threats, they are not very effective at detecting new attacks, generate too many false positives, and are hard to scale in a cloud environment. Thus, a need has arisen to develop intelligent, adaptive security frameworks that can react to dynamically changing threats in real-time.

Cloud security has been revolutionized by the use of AI, especially with the machine learning and DL skills, which allow for intelligent intrusion detection and automated responses[14]. AI-powered systems produce vast amounts of information in the cloud that can be processed to detect variations, predict threats and continuously adjust to new attack strategies. This paper explores the concept of AI IDPSs in cloud security, their techniques, advantages, difficulties, current uses, and potential future research.

A. Structure of the paper

This paper is organized into following sections. In Section II, IDPS in Cloud Computing are discussed in terms of attacks, intrusion detection system types, and limitations of traditional IDS approaches. Section III provides the details of the techniques used by AI in ID, including machine learning and deep learning models. Section IV offers challenges, benefits and applications. The existing literature is reviewed in Section V, and future research directions are concluded in Section VI.

II. INTRUSION DETECTION AND PREVENTION SYSTEMS IN CLOUD COMPUTING

Cloud Computing security is essential to protecting against cyber threats and Unauthorized Access, and IDPS are a crucial part of this. The systems track network traffic, user activities, and system events for security and reliability, and to detect anomalies, prevent attacks, or increase overall cloud security and reliability.

A. Attacks on Cloud Computing

Security concerns for data kept on cloud servers are major obstacles to cloud computing. Security is of utmost importance in cloud computing [15][16]. The following is a brief overview of the different forms of assaults that might target cloud computing:

- **Denial of Service (DoS) Attack:** The great bulk of the available bandwidth is used by these fake packets, which prevents new connections from being made. As a result, authorized users cannot access the service.
- **User-to-Root Attack:** A malicious actor attempts to get access to a legitimate user's account by eavesdropping on their password. An attacker may get root access and change all critical data using this method.
- **Insider Attack:** This kind of attack occurs when a legitimate user tries to leak information by abusing their access rights.
- **Port Scanning:** While targeting a specific computer, an attacker might look for open ports. With the use of a port scanner, they compile a database of all the ports, open, closed, and filtered and then use this information to launch attacks against legitimate services [17].
- **Hypervisor Attacks / Virtual Machine Attacks:** An intruder can take over the installed virtual machine (VM) by taking advantage of security holes in the hypervisor. By targeting installed hypervisors, these attacks enable attackers to seize control of hosts and systems.
- **Backdoor Channel Attacks:** If a computer has a backdoor, hackers can utilize it to access the system remotely. Installing malware and stealing data from systems or networks are both possible through backdoors.

A wide variety of threats can infiltrate cloud computing because of its decentralized and open design. Consequently, systems to identify and thwart such assaults must be put in place. In order to safeguard a computer system from these types of dangers, an intrusion detection system is required.

B. Types of IDS (Network-based, Host-based, Hybrid)

The decentralized nature of the cloud makes it an easy target for cybercriminals. Therefore, Intrusion Detection Systems are a solution to security issues, such as numerous attacks in the cloud. Intrusion detection systems (IDS) keep

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

tabs on human actions and network traffic to identify potentially harmful ones [18]. Security systems sound an alarm if they detect malicious behavior [19]. Intruder detection systems rely on a variety of methods, such as attack signatures or anomalies, to identify attacks; the effectiveness of these methods is crucial to the success of IDSs. IDS can be categorized into two main types based on their network deployment.

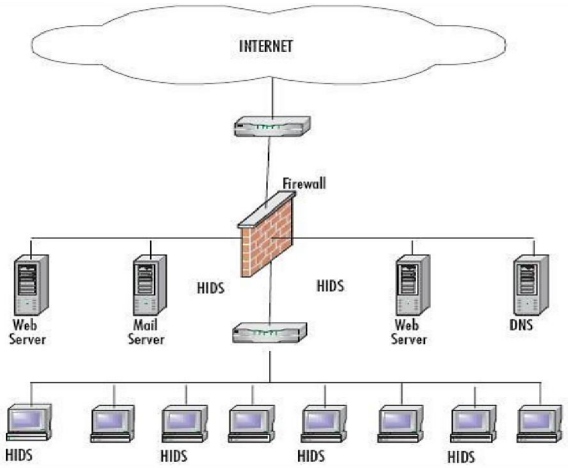

Fig. 1. Host-Based IDS

Host-Based IDS

HIDS are programs that, once installed on a host system, keep tabs on all of the data sent and received by that machine. HIDS monitors the dynamic behavior and internal condition of a system. It examines network packets that are distinctive to a given host. HIDS may detect and discover which software accesses which resource on the host, as shown in Fig. 1. HIDS examines the host's stored information in the file system and log files to ensure that the contents of these appear as intended.

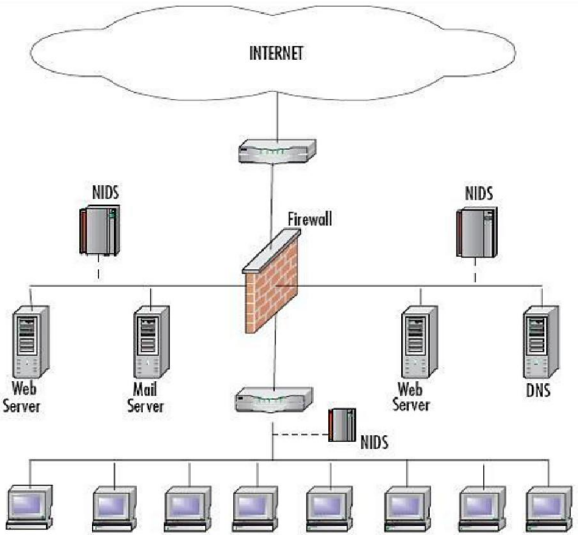

Fig. 2. Network-Based IDS

Network-based IDS

Distributed NIDS are installed at strategic nodes in a network, such as routers and switches. The traffic is routed through the NIDS. It checks all packets sent and received across the network for harmful content. A disadvantage of NIDS is that it cannot detect encrypted communication between hosts. However, NIDS outshines HIDS due to the fact

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

that NIDS can safeguard all hosts linked to a network, while HIDS can only safeguard a single machine. As seen in Fig. 2, the NIDS is located.

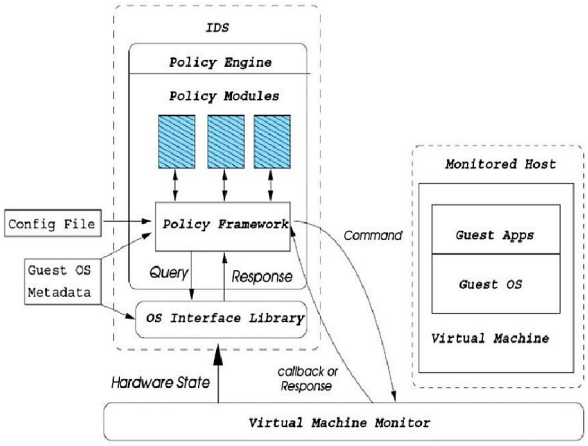

Fig. 3. VM-based IDS

VM-based IDS

A **VM-based IDS** is a security system that runs in a virtualized environment to detect malicious activities in virtual machines (As shown in Fig. 3). It monitors system behavior, network traffic, and logs either inside the VM, at the host level, or at the hypervisor layer. It improves security through isolation, making it harder for attackers to hide or disable the system. Common approaches include host-based IDS (inside VMs), network-based IDS (monitoring virtual network traffic), and hypervisor-based IDS (monitoring all VMs from the virtualization layer). VM-based IDS is widely used in cloud and data center environments because it is scalable and efficient, but it may introduce performance overhead and can face challenges from advanced evasion techniques.

C. Limitations of traditional IDPS

However, there are several limitations that make traditional IDPS less effective in meeting the challenges of new cyber threats in cloud computing environments. The main drawbacks are briefly outlined below:

- **Dependency on Signature-Based Detection:** Traditional IDPS heavily rely on predetermined attack signatures and known malicious patterns. They are helpful in combating known attacks, but not against zero-day attacks, APTs, and new variants of malware.
- **High False Positives and False Negatives:** There are many cases where conventional systems can be misled in marking legitimate activity as malicious, leading to a high FP rate. In the meantime, the complex attacks may not be detected (false negative) which increases security risks.
- **Scalability Challenges:** The cloud-based environments create a lot of data in a wide range of sources such as systems, virtual machines, network traffic, etc. This vast amount of dynamic data is hard to process with traditional IDPS, and it has performance problems and lags.
- **Lack of Adaptability to Evolving Threats:** Legacy systems are based on rules which need to be updated regularly so as to keep up with new attack patterns. This hinders their capacity to react swiftly to the quickly changing threat in cyberspace.
- **Difficulty in Encrypted Traffic Inspection:** Cloud communications typically rely on encrypted traffic, making it difficult for the traditional network-based IDPS to discern encrypted traffic, and therefore malicious activity within encrypted traffic.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

- **Limited Visibility in Virtualized Environments:** Conventional IDPS are mostly for traditional infrastructure, may not be suitable for inter-VM communications monitoring, hypervisor activities, or multi-tenant cloud monitoring.
- **High Operational and Maintenance Costs:** The traditional IDPS is known for being costly and complex, as it requires frequent updates and manual provisioning and expert knowledge with a high number of Cyber Security experts.

The restrictions highlight the increasing significance of AI-powered IDPS. These systems deliver Adaptive Learning, Real-time Threat Detection, AutomatedResponse and accuracy gains in the cloud security environment.

III. AI TECHNIQUES FOR INTRUSION DETECTION AND PREVENTION

AI-powered technologies have made significant contributions to IDPS in the cloud by providing sophisticated threat detection, anomaly identification, and automated reactions[20]. The advantage of ML and DL is that they enhance the accuracy of detection, adaptability, and real-time identification of new cyber threats.

A. Machine Learning approaches

An important part of anomaly-based IDS is ML [21]. This is because both types of systems work by first learning typical patterns of data and then warning of any changes that deviate from these patterns, which could be signals of hostile activity.

Supervised Learning

Supervised Learning uses labelled Training Data to generate the output-label mapping (e.g., normal or malicious); as a result, the model learns to anticipate the desired objectives through training on labelled instances. Supervised learning methods include SVM, NB, DT, KNN and RF. Supervised models are efficient at identifying known attack classes based on previously seen examples. [22]. The issue with this is that it is practically hard to collect tagged data in the real world due to a combination of the intrinsic complexity of the labelling procedure and the emergence of new and undiscovered attack types.

Unsupervised Learning

When labelled data is unavailable for model training, unsupervised learning is employed. Without any background information, these models aim to find structures, trends, or anomalies in the data. A number of methods have been employed, including PCA, K-means Clustering, and autoencoder. Similarly, situations requiring zero-day attack detection and novel patterns growing frequently are well-suited to unsupervised approaches.

Semi-supervised and Hybrid Models

To find the best examples from the unsupervised methods' generated lists, semi-supervised learning employs a limited number of instances that have been tagged by an expert and a large number of unlabeled samples. Because this technique lessens the reliance on labels, semi-supervised ML is ideal for ID tasks where instance labeling is impractical or too expensive. By making better use of the instances that are available, semi-supervised models are able to infer labels of unlabeled examples. This is achieved through processes like label propagation and self-training. To improve the detection rate of intrusions and decrease the occurrence of FP and FN alerts, Hybrid Models integrate many learning tactics and approaches, including supervised and unsupervised learning, signature-based methods, and machine learning (ML). The enhanced scalability, adaptability, and fault tolerance of hybrid and semi-supervised models make them ideal for usage in real-time systems.

B. Deep Learning Models

Deep learning techniques eliminate the need for human feature engineers by automatically learning complicated representations from raw data and identifying sophisticated patterns [23].Some characteristics of deep learning models include the following: the necessity for a large database for training, the high computational resources required, and the difficulty in interpreting the results [24]. In intrusion detection systems, CNNs, RNNs, and GANs are common forms of

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

deep learning algorithms.

Table I provides a summary of the machine learning approaches utilized by intrusion detection systems. System detection and response to threats has been transformed by the incorporation of machine learning techniques into intrusion detection systems (IDS). While supervised techniques are great at using known patterns to attain high accuracy, unsupervised methods are great at detecting new dangers. A combination of deep learning and hybrid methods allowed for scalability and flexibility. The availability of data and computational resources, as well as the security measures implemented in the environment where the technology will be implemented, are crucial factors to consider when selecting a technology.

Table I summarizes the major ML algorithms used in intrusion detection systems, highlighting their learning types, key features, and suitability for detecting attacks, anomalies, and complex malicious activities in cloud environments

TABLE 1: SUMMARY OF MACHINE LEARNING ALGORITHMS IN IDS

IDS Learning Type	Algorithm	Key Features	Suitability
Supervised	Support Vector Machine (SVM)	Effective in high-dimensional spaces	Attack detection, malware classification
	Random Forest	Robust, ensemble-based approach	Large-scale intrusion detection
	Decision Tree	Interpretable rules, prone to overfitting	Small to mid-size data, basic classification
	K-Nearest Neighbor (KNN)	No training phase, lazy learning	Lightweight IDS with low data volume
	Naïve Bayes	Probabilistic, fast computation	Phishing detection, spam detection
Unsupervised	Principal Component Analysis (PCA)	Visualization, linear transformation, feature reduction	Outlier detection, feature reduction
	K-Means	Distance-based clustering	Anomaly detection
	Autoencoders	Neural representation learning	Unknown pattern recognition
Semi-supervised	Self-Training	Bootstrapping unlabeled data	Label-scarce environments
Hybrid	Machine Learning + Signature-Based Detection	Combines behavior and pattern matching	Real-time intrusion detection systems
Deep Learning	GAN, RNN, CNN	Deep, non-linear pattern discovery	Complex network behavior modelling

C. Real-time threat detection and adaptive learning

The capacity to identify threats in real time is a basic aspect of cloud-based IDPS that is powered by AI. Instead of using static rules and defined signatures, these systems constantly analyze Network Traffic, User Activity and System Logs to detect malicious activity in real-time. These systems can use ML and DL to rapidly identify threats like malware, unauthorized access, insider threats, and DDoS attacks. In cloud settings, real-time analysis is especially crucial because stalling the detection process can lead to data breaches, service interruptions, or monetary damages.

By the use of ML and DL models, the systems can learn the normal behavior and help detect anomalies in real time to a great extent. Supervised learning algorithms – learn how to classify activities as normal or malicious from labelled datasets; Unsupervised learning algorithms – learn how to detect activities that are unusual without any prior knowledge of attacks. The DL techniques like RNN and LSTM models are effective in analyzing complex and sequential cloud traffic patterns, thereby enabling the detection of evolving cyber threats more accurately.

AI-driven cloud security is further bolstered by adaptive learning, which allows the systems to continuously learn and enhance themselves based on new data and evolving attack patterns. An adaptive system can automatically adjust detection models and prevention mechanisms to counter new threats and zero-day attacks; traditional IDPS systems

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

need manual updating. These systems also feature automated functions such as blocking malicious traffic, isolating an infected VM and real-time updates to the security policies to limit false alarms and enhance cloud security system effectiveness.

IV. CHALLENGES, APPLICATIONS, AND BENEFITS

Al has the potential to make a significant contribution to the security of clouds, but has some challenges that hinder its use and influence. To fully leverage the power of Al in securing the cloud, these concerns and challenges need to be addressed.

- **Data Privacy and Compliance:** When using Al in the context of Cloud Security, a large amount of data is accessed, including sensitive data, which might present risks to data privacy and compliance. It raises a big security and privacy issue, particularly in the context of regulatory obligations such as those under the CCPA and GDPR. Emphasize Data encryption and anonymization measures, with the aim that everybody will be mindful of the dangers to their privacy if they use Al services in the cloud.
- **Data Security and Privacy:** One of the key challenges in a shared environment is data security.
- **Regulatory Compliance:** Cloud computing has introduced a layer of complexity to ensuring compliance with legal and industry-specific requirements, including GDPR and HIPAA standards.
- **Vendor Lock-In:** The use of proprietary tools and platforms may lead to a lack of flexibility and dependence on a select few vendors.
- **Performance Concerns:** Cloud-based applications, such as real-time analytics and gaming, may be impacted by latency.

A. Benefits of Al-Powered Cloud Security

The use of generative AI, a novel formative technology, can significantly improve cloud security by automating threat detection, incident handling in real-time, and vulnerability management [25]. The many advantages provided by cloud computing make it superior to traditional computing. Cloud computing offers numerous advantages, including flexible security, accessible data from any location, cost savings, mobility, scalability, agility, and efficiency.

Improved Threat Detection Accuracy and Reduced False Positives

- Solutions for security that use AI and ML can sift through mountains of data in search of intricate patterns.
- Recognize threats more accurately than conventional rule-based techniques.
- The reliability and efficacy of the security system are enhanced as the number of FP alarms is reduced.

Faster Response Times to Security Incidents

- It takes less time to identify, analyze, and mitigate occurrences when you use automated solutions powered by AI.
- It becomes feasible to proactively and successfully protect against cyber-attacks.

Scalability to Handle Large Volumes of Security Data

- Security-related big data, such as logs, Network Traffic, and user behaviors, may be handled by Al and ML algorithms.
- The complexity of the cloud is only going to increase over time, yet cloud security solutions are adaptable and scalable.

Continuous Learning and Adaptation to Evolving Threats

- AI-powered systems are always becoming better as they gather more data.
- Revise models to include emerging risks.
- Ensures that safety measures function as intended in the long run.

Reduced Workload for Security Teams and Improved Efficiency

- Automates routine security tasks.
- Provides data-driven insights.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

- Frees security teams to focus on strategic, high-impact initiatives.

The use of cloud computing is similar to that of a utility, and it is more cost-effective than hardware-based computing. Cloud computing also has the attractive characteristic of moving application processing to the cloud rather than on-premises servers.

B. Applications in Cloud Environments

The use of AI-driven IDPs has become more widespread in the cloud to enhance cybersecurity, safeguard critical data, and maintain business continuity. They are intelligent threat detection and automatic response solutions that help ensure secure cloud operations across various sectors:

Finance Sector

Cloud computing is utilized in the finance industry for various digital banking, online transactions, and financial data management applications. But with cloud-based systems comes the possibility of cyber-attacks like phishing, ransomware, fraud and DDoS attacks. An AI-driven IDPS enhances security by eliminating financial risks through threat response at real-time speeds and detecting suspicious activity by transaction pattern analysis.

Healthcare Sector

The healthcare sector has seen cloud computing being used for electronic health records (EHRs), telemedicine, and patient monitoring applications. Healthcare systems are susceptible to cyber-attacks because of the sensitivity of medical data. AI-powered IDSs bolster security by tracking unusual activity, identifying malware and breaches, and maintaining patient privacy and compliance with regulations.

Internet of Things (IoT) Environments

In fact, cloud-integrated IoT systems are found in many smart homes, health and industrial automation applications. But when devices are interconnected, they are more vulnerable to attacks like botnets, spoofing and unauthorized access. With AI, IDSs can monitor the communication behavior of devices, identify anomalies and automate threat remediation, safeguarding IoT ecosystems.

Enterprise Systems

Cloud infrastructures are now the foundation of enterprises, allowing them to execute a business, work remotely and manage data. The AI-powered IDPS constantly monitors, analyzes behavior, and automatically detects threats, boosting enterprise security. These systems monitor for suspicious activity, prevent unauthorized access and aid in the management of cloud security.

V. LITERATURE REVIEW

The studies highlight the urgent need for real-time cloud intrusion detection, anomaly detection, explainable cloud security, adaptive defenses and other tools, and their limitations in preventing attacks, scalability, transparency, and real-time deployment.

Patel et al. (2026) review studies conducted by both academics and businesses on the topic of AI in cloud security and operations during the past three years (2022–2055), lays out a taxonomy of AIOps functions such as detection, compliance, response, and governance, and talks about problems that still need fixing, such as transparency, adversarial resilience, and multi-cloud coordination. Part three delves into potential future courses of action, including explainable and neuro-symbolic AIOps, federated analytics for decentralized settings, and autonomous self-healing systems. With this study, they want to provide academics and practitioners with a single point of reference for creating AI-powered cloud operations that are reliable, scalable, and secure [26].

Jain (2025) gives an overview of AI-based solutions for enhancing cloud security, emphasizing the next generation of IDPS, such as WIDS, host- and network-based IDPS and IoT-related IPS. Additionally, it discusses cloud security standards, tactics for mitigation, and problems with hybrid and multi-tenant clouds. Some of the main gaps that are explored include data privacy, FP, adversarial attacks, and integration complexity. Lastly, the article provides a look at

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

how AI can be integrated with other new technologies, such as blockchain, edge computing and the Internet of Things, to build flexible, adaptable and strong cloud security solutions [27].

Upadhyay, (2025) in-depth analysis of how the use of ML and AI techniques can improve the capabilities of IDS in cloud security. The analysis of Unsupervised Learning models for recognition and unidentified acts of violence, as well as adaptation to the fluctuation of violence and an increase in the detection accuracy, is included in the study of Supervised Learning models and Reinforcement Learning models. Further, hybrid approaches that combine several learning techniques to create scalable and context-aware defenses are analyzed. Moreover they address problems with cloud deployment, such as virtualization, real-time monitoring and communication with orchestration tools. There is an emphasis on AI-based intrusion detection system designs that are elastic, have behavior-based threat detection, and offer automated response mechanisms [28].

Abdel-Wahid (2024) discusses the use of AI and ML methods to improve the effectiveness of threat detection, prevention, and response in cloud-based security systems. Key reasons for the rise of Al-powered cloud security are discussed, such as the fact that cloud-based data and apps are exploding in number, advanced persistent threats (APTs) are becoming more common, and the necessity of real-time, adaptive security. It delves into how Al and ML can help reduce the burden on security teams and provide them with more insights into the large volumes of security data, identify anomalies and patterns, and detect new threats earlier and more effectively than existing security solutions. Furthermore, the study discusses the spectrum of Al algorithms and technologies that can be used to provide various types of security services on the cloud, such as predictive analytics, self-healing systems, and automatic incident responses [29].

Viharika and Balaji (2024) compare the capabilities of AI-based IDS in cloud-based infrastructure to the traditional security models and present modern AI techniques. The paper summarizes the pros and cons of various ML and DL techniques, and recommends adopting hybrid techniques that combine traditional security methods with AI-based ones. It tackles the major issues of privacy compliance, scalability and reduction of false positives and provides workable solutions to these issues [30].

Upadhyay et al. (2023) discuss the multifaceted world of IDSs in cloud computing, including the different types of IDSs and their challenges and limitations. The study also delves into the concept of Explainable AI (XAI) and the implications it carries, examining the concept and its potential to offer insights into the inner workings of complex AI models. Considering the constantly evolving cybersecurity field, the paper discusses the synergic potential of combining XAI with IDS and how it can improve the transparency and interpretability of the decision-making process of an AI-based IDS. This investigation of the promises of XAI also includes its ability to alleviate current problems of conventional IDS such as false positives and false negatives [31].

Table II summarizes the approaches, findings, limitations, and recommendations proposed by authors, highlighting the gaps in the field of intrusion detection and prevention in cloud security using artificial intelligence

Table 2: Summary of Recent Studies on Research Gaps in AI-Based Intrusion Detection and Prevention for Cloud Security

Authors	Approaches	Findings	Limitations	Recommendations
Patel et al. (2026)	Reviewed AI-driven cloud security and AIOps (2022–2025).	Highlighted AI roles in detection, compliance, and self-healing systems.	Limited focus on AI-based intrusion prevention and real-time cloud implementation.	Develop scalable and explainable AI-driven IDS/IPS for multi-cloud security.
Jain (2025)	Surveyed AI-driven IDS/IPS models in cloud and IoT security.	Showed AI improves threat detection and cloud resilience.	Lacks comparative analysis of AI models and hybrid prevention systems.	Evaluate ML/DL models and integrated IDS-IPS frameworks.
Upadhyay (2025)	Examined supervised,	AI improves detection accuracy	Limited discussion on intrusion prevention and	Integrate prevention mechanisms and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

	unsupervised, RL, and hybrid AI models for IDS.	and adaptive defense.	real-world deployment.	explainable AI in cloud IDS.
Abdel-Wahid (2024)	Studied AI/ML for cloud threat detection and response.	Found AI enhances anomaly detection and predictive security.	Broad cloud security focus; lacks dedicated IDS/IPS evaluation.	Develop specialized AI-based IDS/IPS for dynamic cloud environments.
Viharika and Balaji (2024)	Compared AI-based IDS with traditional security approaches.	AI improves detection but faces privacy and scalability issues.	Minimal focus on automated prevention and adaptive response.	Explore hybrid AI-driven IDS/IPS with reduced false alarms.
Upadhyay et al. (2023)	Investigated XAI integration in cloud IDS.	XAI improves transparency and reduces false positives.	Limited focus on prevention systems and real-world validation.	Develop XAI-enabled IDS/IPS with adaptive prevention.

VI. CONCLUSION AND FUTURE WORK

AI-powered intrusion detection and prevention systems (IDS/IPS) have proven to be a valuable tool in tackling the cybersecurity challenges that arise in cloud computing environments. Traditional IDSs are signature or rule-based, and can cause problems with new and advanced attacks. AI-powered solutions, including ML and DL models, can, however, enable intelligent threat detection, anomaly identification, Adaptive Learning, and automated responses. These solutions provide significant improvements in detection capability, reduce false alarms, and enable scalable and secure solutions that can be adapted to changing cloud environments. The review also highlights the importance of hybrid and semi-supervised models, which are expected to enhance the accuracy of detection as well as address cloud-specific challenges such as virtualization, encrypted traffic, and multi-tenant designs. Although there have been numerous advances, data privacy, model explanation, computational complexity, adversarial attacks and regulatory compliance are still very much concerns. Future research should focus on developing interpretable and reliable AI systems, efficient and low-power algorithms, federated learning to ensure privacy while maintaining the ability to detect and prevent adversarial attacks in real-time, with adaptive strategies that evolve as the attack surface changes. Furthermore, AI-driven IDPS, when combined with the edge computing concept, zero-trust models, can provide a more holistic level of security for cloud with a resilient and transparent cloud security approach to defend novel and emerging threats in a more complex cloud environment.

REFERENCES

[1] B. P. Singh, "Convergence of AI and Zero Trust : Enabling Continuous Verification Across Hybrid Cloud Environments," *Int. J. Intell. Syst. Appl. Eng.*, vol. 14, pp. 339–359, 2026.

[2] A. Parupalli and H. Kali, "An In-Depth Review of Cost Optimization Tactics in Multi-Cloud Frameworks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 5, pp. 1043–1052, Jun. 2023, doi: 10.48175/IJARSCT-11937Q.

[3] K. Jangiti, "Design and Validation of a Machine Identity Governance Framework for AI Agents in Multi-Cloud Environments," in *SoutheastCon 2026*, 2026, pp. 1–6. doi: 10.1109/SoutheastCon63549.2026.11476363.

[4] D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

[5] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

[6] A. K. Padhy, C. Medicherla, B. Vulugundam, C. Kulkarni, T. P. Patel, and S. Shivam, "Latency-Optimized Microservices Orchestration for Real-Time E-Commerce in Multi-Cloud Environments," in *2025 International Conference on Computer and Applications (ICCA)*, IEEE, Dec. 2025, pp. 1–6. doi: 10.1109/ICCA66035.2025.11430930.

[7] V. K. Sharma, "Cloud Computing & IoT: 5G Focused IoT with Cloud Solutions," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 6, no. 3, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I3P103.

[8] B. Mohan, V. R. Surasani, and R. Kumar, "Autonomous Data Stewardship: Multi-Agent AI for Real-Time Master Data Management in Financial Services," in *2026 IEEE 16th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2026, pp. 0689–0698. doi: 10.1109/CCWC67433.2026.11393832.

[9] M. R. C. Mukkolakkal, "InfraLLM: A Generic Large Language Model Framework for Production-Grade Microservice Auto-Scaling in Cloud Infrastructure," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 11, pp. 113–123, 2025, doi: 10.38124/ijsrmt.v4i11.1023.

[10] S. Tatavarthi, S. Tarakampet, and R. R. Koilakonda, "Leveraging Generative AI for Adaptive Compliance Workflows in Enterprise Platforms," *Int. J. Res. Appl. Sci. \& Eng. Technol.*, vol. 14, no. 1, 2026, doi: 10.22214/ijraset.2026.77213.

[11] V. Sanikal, "AI-Enhanced Network Security Framework for Cloud-Edge Integrated Environments," in *2026 Innovations in Machine, Engineering, and Digital Conference (IMED)*, IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/IMED68921.2026.11484417.

[12] R. Lingam, S. Nagi, M. Chigurupati, and B. T. Myneni, "Resilient DevSecOps: Self-Healing Cloud-Native Systems via SRE-Driven AI Threat Detection and Response," in *2026 International Conference on Smart Futuristic Technology*, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/ICSFT66733.2026.11508049.

[13] M. Parikh, A. A. Soni, S. M. Shah, and A. R. Jha, "Big Data Workload Profiling for Energy-Aware Cloud Resource Management." 2026. doi: 10.48550/arXiv.2601.11935.

[14] S. K. Anumula, "AI-Powered Cybersecurity Framework for Cloud- Based Applications : Enhancing malware detection and threat response using deep learning," *Int. J. Syst. Des. Inf. Process.*, vol. 13, no. 4, pp. 109–116, 2025, doi: 10.64971/j.cph.ijsdip.v13.14.16.2025.

[15] S. M. Othman, A. Y. Al-mutawkkil, and A. M. Alnashi, "Survey of Intrusion Detection Techniques in Cloud Computing," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 2, no. 4, pp. 363–374, Aug. 2024, doi: 10.59628/jast.v2i4.970.

[16] P. C. Jakku, P. Sundaramoorthy, S. C. Kondaparthy, T. Desai, R. Jarubula, and A. Nerella, "Enhancing Cloud Security Via Quantum Computing," in *Proceedings of Data Analytics and Management*, A. Swaroop, B. Virdee, S. Correia, and Z. Polkowski, Eds., Cham: Springer Nature Switzerland, 2026, pp. 377–386. doi: 10.1007/978-3-032-03558-5_31.

[17] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

[18] P. Parida and N. Senguttuvan, "Responsible Utilization of Cloud in Retail Banking Ecosystem," *Int. J. Comput. Appl.*, vol. 187, no. 49, pp. 34–39, Oct. 2025, doi: 10.5120/ijca2025925835.

[19] U. Kumar and B. N. Gohil, "A Survey on Intrusion Detection Systems for Cloud Computing Environment," *Int. J. Comput. Appl.*, vol. 109, no. 1, pp. 0975–8887, 2015.

[20] V. Methuku, S. Kamatala, P. Naayini, and P. R. Vontela, "From Ethical Principles to Technical Safeguards: A Unified Framework for Safe and Human-Centered Artificial Intelligence," *Am. Int. J. Comput. Sci. Technol.*, vol. 4, no. 5, pp. 26–34, Sep. 2022, doi: 10.63282/3117-5481/AIJCST-V4I5P103.

[21] M. Ogunbadejo, O. Adedamola, A. Adewale, and O. Alade, "Machine Learning Methods for Intrusion Detection : A Comprehensive Survey," *Int. J. Sci. Res. Manag.*, vol. 13, no. 07, pp. 2446–2456, 2025, doi: 10.18535/ijsrm/v13i07.ec07.

[22] M. J. B. Mehta, "AI-Driven Test Engineering for Cloud-Native Systems," *Int. J. Data Sci. IoT Manag. Syst.*, vol.

5, no. 1, Jan. 2026, doi: 10.64751/ijdim.2026.v5i1.297.

[23] H. P. Cyril and S. Kumara, "Identification of Anomalies via Deep Learning Based Models for High Dimensional Telecom Traffic Data," *J. Adv. Artif. Intell.*, vol. 4, no. 1, pp. 24–37, 2026, doi: 10.18178/JAAI.2026.4.1.24-37.

[24] M. Kari, "Deep Learning-Based Fault Prediction Models for Enhanced Network Security Monitoring," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, p. 492, Jun. 2023, doi: 10.48175/IJARSCT-11600I.

[25] D. A. Jain, "AI-Powered Cloud Security: A Review of Intrusion Detection and Prevention Strategies," *Int. J. Adv. Res. Comput. Sci. Softw. Eng. J. Adv. Res. Comput. Sci.*, vol. 16, no. 6, pp. 114–120, Dec. 2025, doi: 10.26483/ijarcs.v16i6.7385.

[26] A. Patel *et al.*, "AI-Driven Cloud Security: AIOps for Threat Detection and Compliance," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 13, no. 1, 2026, doi: 10.53735/cisse.v13i1.219.

[27] A. Jain, "AI-Powered Cloud Security: A Review of Intrusion Detection and Prevention Strategies," *Int. J. Adv. Res. Comput. Sci.*, vol. 16, no. 6, p. 114, 2025, doi: 10.26483/ijarcs.v16i6.7385.

[28] N. Upadhyay, "AI and Machine Learning for Cloud Security: A Comprehensive Survey of IDS and Threat Detection Methods," *J. Glob. Res. Math. Arch.*, vol. 12, no. 6, pp. 34–41, 2025.

[29] 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.

[30] S. Viharika and Na. Balaji, "AI-Driven Intrusion Detection Systems in Cloud Infrastructures: A Comprehensive Review of Hybrid Security Models and Future Directions," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, IEEE, Dec. 2024, pp. 1201–1207. doi: 10.1109/ICUIS64676.2024.10866856.

[31] U. Upadhyay, A. Kumar, S. Roy, U. Rawat, and S. Chaurasia, "Defending the Cloud: Understanding the Role of Explainable AI in Intrusion Detection Systems," in *2023 16th International Conference on Security of Information and Networks (SIN)*, 2023, pp. 1–9. doi: 10.1109/SIN60469.2023.10475080.