DOI: http://dx.doi.org/10.26483/ijarcs.v16i6.7385

ISSN No. 0976-5697

Volume 16, No. 6, November-December 2025

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

AI-POWERED CLOUD SECURITY: A REVIEW OF INTRUSION DETECTION AND PREVENTION STRATEGIES

Dr. Amit Jain
Professor
Department of Computer Science and Engineering
OP Jindal University
Raigarh (C.G)

***Abstract*—**Cloud computing has been able to revolutionize current organizations through the usefulness of scaling, flexibility, and affordability of data storage and access. However, a number of serious security problems have been brought about by the widespread use of cloud services, including data breaches, malware insertion, denial-of-service (DoS), and unauthorized access. Although they can offer much-needed protection, traditional techniques like firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and log inspection are ineffective in addressing the new dangers of today. Cloud security systems are increasingly being implemented using Artificial Intelligence (AI) and Machine Learning (ML) to help with anomaly detection, predictive threat modelling, and automated incident response in order to get around these limitations. The paper provides a survey of AI-driven solutions that can be used to improve cloud security, paying attention to the next-generation intrusion detection and prevention models that include Web Intrusion Detection Systems (WIDS), host-based and network-based IDPS, and IoT-related IPS. It also examines standards of cloud security, mitigation methods and problems of multi-tenant and hybrid environments. The major gaps, such as data privacy issues, false positives, adversarial attacks, and the complexity of integration, are examined. Lastly, the paper examines how AI can be integrated with new technologies like blockchain, edge computing, and IoT to construct flexible, adaptable, and resilient cloud security environments.

***Keywords*—**Cloud Security, Artificial Intelligence, Intrusion Detection, Intrusion Prevention, Edge Computing, IoT, Machine Learning.

I. Introduction

Cloud computing is now a component of the contemporary digital infrastructure that builds on ideas of grid and distributed computing and offers scalable virtual resources and easy access to data and services through the Internet [1]. It is extensively used in industrial, as well as academic, fields today. However, the necessity for a high level of security has become a pressing concern due to the quick expansion of cloud computing use, given the fact that users make the cloud their depository of sensitive data, any compromise of confidentiality, integrity, or availability can greatly topple the trust of users and prevent further adoption.

Network-Based Intrusion Prevention Systems (NBIPS) and IDS are critical in protecting cloud and IoT environments against changing cyber threats [2]. Whereas IDS identifies abnormalities and malicious operations, NBIPS is proactive and verifies traffic streams across the network and prevents cases of misuse on the spot [3]. NBIPS is placed behind firewalls, which offer an extra defense layer, enhancing the security of the cloud and IoT. As the IoT equipment continues to be a focus of attacks by industrial machinery, smart grids, and building automation systems, integration of IDS and IPS is even more essential in the protection of ecosystems of interconnections.

Cloud security technologies now incorporate AI to address these issues [4]. In particular, algorithms for DL and ML have shown promise in identifying, deterring, and mitigating a variety of security risks [5]. By enabling any adaptive learning, real-time monitoring, and independent decision-making, AI-based solutions provide proactive protection mechanisms against cyberattacks, unwanted access, and data breaches [6]. Such smart solutions are the core of Artificial Intelligence-Based Architectures (AIBA) that would strengthen the cloud security infrastructure by reacting to attacks in a continuous manner and being able to react to them automatically. The other new dimension is AI-as-a-Service (AIaaS), in which ML models are deployed on the cloud by vendors and used by end-users [7][8]. This paradigm creates additional privacy and security threats, where even ML and DL models can be attacked or used. The solution to these issues lies in strong taxonomies and formal risk evaluation to categorize the vulnerabilities, compare defenses and create a resilient AI solution that does not compromise privacy. These taxonomies not only enhance the security in AI-enhanced cloud services but also assist in the modelling of responsibilities performed by the providers and consumers in the process of risk reduction.

The contribution of AI to the improvement of threat detection and cybersecurity, with references to the latest developments and current issues in the dynamic sphere. Identifying and mitigating cybersecurity-related threats, such as network attacks, adversarial attacks, and zero-day attacks, have been greatly enhanced by the incorporation of AI and in particular ML and DL algorithms [9][10]. The review stresses the importance of the explainability and resilience of the AI models to achieve trustworthiness and reliability in AI-based security solutions. Analyzed studies demonstrate AI's versatility in addressing distinct security challenges across several domains, including autonomous vehicles, the IoT, 5G networks, and Industry 5.0. Innovative methods are enhancing the creation of stronger and real-time threat detection systems. These include federated learning, blockchain integration, and transformer-based models.

A. Structure of the Paper

This paper is structured to provide an AI-Powered Cloud Security, Section II Next-Generation Cloud Security, Section III Advanced Approaches to Intrusion Detection and Prevention, Section IV Challenges, benefits and Emerging Technologies. A review of the literature is given in Section V, and important conclusions and recommendations for the future are given in Section VI.

II. Next-Generation Cloud Security

The information technology sector has developed from mainframes to client PCs, cloud computing, and Internet virtualization. The term "cloud computing" refers to an information technology service that is mostly used by service providers and consumers. It describes a distributed and versatile service that offers configurable IT resources (such as computation, networking, applications, storage, and information) on demand through a networked system [11] [12]. The service requires little maintenance effort and is centered around service-level agreements between providers and customers. Tools and programs hosted on the internet also fall into this category; users access and use them through a web interface just like they would any other desktop application. Cloud computing provides on-demand access to apps, infrastructure, or technological tools in the form of platform-as-a-service, software as a service, or infrastructure as a service, as opposed to buying licensed software or hardware.

A. Cloud Security Issues

The organization uses a number of cloud services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), and deployment patterns such as public, private, and hybrid clouds. There are multiple cloud security concerns with these models and services. There are problems with every service model [13]. The main issues with cloud computing are data breaches, data loss, account theft, unsecured APIs, denial-of-service attacks, abusive service, hostile insiders, inadequate due diligence, shared technology, and inadequate security. These dangers and how to protect from them are detailed below. "Multi-tenancy" refers to a cloud architecture that allows numerous users to safely and effectively share the same resources.

- **Elasticity -** Cloud computing's scalability refers to its capacity to increase or decrease available resources in response to different levels of demand.
- **Insider attacks -** Security threats caused by malicious or negligent actions of authorized users within the organization.
- **Outsider attacks -** Cyber threats from unauthorized external attackers trying to gain access or disrupt systems.
- **Loss of control -** A problem where businesses have little visibility into and control over the data and infrastructure stored in the cloud [14].
- **Data Loss -** Permanent or temporary loss of sensitive information due to accidental deletion, corruption, or malicious activities.
- **Network security -** Techniques used to safeguard resources and data while they are being transmitted over cloud networks.
- **Malware Injection Attack Problem -** Attackers inject malicious code or applications into cloud services to steal or manipulate data.

B. Techniques to Secure Data in Cloud

Data protection is the top priority in the field of information security and cloud computing. To address this issue, countless solutions have been developed. To ascertain whether these solutions are suitable and can meet the requirements, it is required to examine, classify, and assess the substantial body of previous work on the subject because it is evident that the current solutions do not undergo rigorous investigation [15]. There are a plethora of models that have been researched and created for various objectives related to data security in the cloud [16]. This article focuses on getting effective protection by stopping leaks and identifying the hostile entity causing them, as seen in Fig. 1. Leaker detection and leak prevention are typically used to protect data. While cryptography, access control mechanisms, and differential privacy with ML algorithms form the foundation of most strategies to ensure data remains secure, watermarking and probabilistic approaches are the cornerstones for leaker discovery.

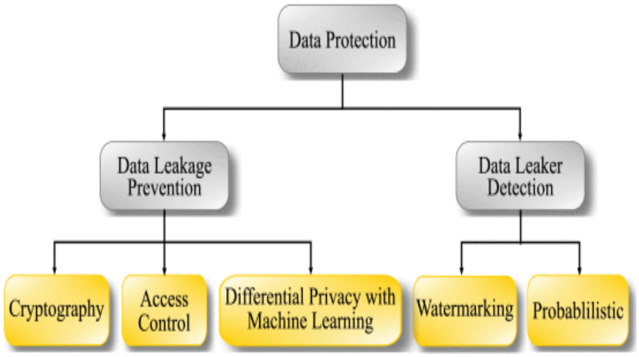

Fig. 1. Major classification of data protection techniques.

1) Data Leakage Prevention (DLP)

Techniques that prevent sensitive information from being accidentally or maliciously exposed outside an organization.

- **Cryptography:** Secures the information by transforming it into inaccessible formats so that only the authorized individuals with the decryption keys can access the information [17].
- **Access Control:** Limits the access to data using user identity, roles or permissions, which reduces unauthorized access.
- **Differential Privacy with Machine Learning:** Guarantees privacy in data by controlled noising, which enables ML models to be trained without any data record being shown.

2) Data Leaker Detection

Techniques used to detect the origin or the party that is leaking sensitive information.

- **Watermarking:** Appends distinctive encryptions on data to track and identify illegal sharing.
- **Probabilistic Methods:** Apply statistical analysis and probability-based to deduce and identify suspicious data leaks or anomalies.

III. Advanced Approaches to Intrusion Detection and Prevention

The use of AI and ML to detect and prevent intrusion cases in real-time is an advanced intrusion detection and prevention method. These systems are automatic in their response to attacks, they adapt to the changing threats, and they are more accurately detected with a smaller number of false positives than traditional systems.

A. Prevention

Prevention is defined as the collection of measures, instruments and mechanisms that prevent security breaches, data breaches or unauthorized entry before they can happen.

Prevention is done in the context of data protection that involves actively detecting and exploiting vulnerabilities and applying controls to protect sensitive information, which include encryption, access control, and monitoring [18]. It makes sure that information is not spilled, abused, or altered by unauthorized users. The preventive strategies involve such techniques as cryptography to safeguard confidentiality, access control to limit permissions, and privacy-guaranteeing measures to safeguard datasets involved in analytics. Prevention can be used to ensure trust, regulatory compliance and overall integrity of digital systems by concentrating on risk reduction before it occurs.

B. Intrusion Detection System

The IDS is essential in contemporary cybersecurity systems [19]. These are designed to keep an eye on system activity and network traffic in order to spot potential security lapses or malicious activity that might compromise a system's availability, confidentiality, or integrity. IDS has become a vital part of the organizational defense strategy that ensures the early detection and prompt response to security breaches.

C. Categories of IDPS

There are several different types of IDPS technologies. Depending on the type of event they track and how they are put into practice, they can be divided into the following four categories in order to address this chapter: Network-based IDPS, host-based IDPS, network behavior analysis (NBA) system, and wireless IDPS [20]. Each of these four groups is discussed in this section in greater detail. In the case of each group, it provides an overview of the group and then talks of the security capabilities and limitations of the IDPS in Detail.

1) Network-based Intrusion Detection and Prevention System (NIDPS)

Network traffic can be monitored and scanned by a network-based intrusion detection and prevention system to find intrusions that could compromise the network's infrastructure. This is very useful to identify threats over a large network when it is used in the examination of traffic flow patterns [21]. This system scans over data packets and, no, can detect suspicious activity in the perimeter level. In network security, NIDPS is frequently built into firewalls and other associated software, and it provides comprehensive protection. Network Behavior Analysis (NBA) System is interested in finding the common patterns or behaviors of traffic in a network, which can indicate intrusions or malicious activities. It places great emphasis on anomaly detection using the deviations from the normal behavior of the network.

2) Wireless Intrusion Detection and Prevention System (WIDPS)

WIDPS systems are used to ensure that there are no attempts at unauthorized access or threats that are specific to wireless communications. This system is thus very important in regard to security in Wi-Fi networks since it identifies rogue access points and suspicious wireless usage like threats specific in wireless protocol, eavesdropping and spoofing threats. The enforcement of security regulations for mobile and remote access points is another area where WIDPS might be helpful.

3) Host-based Intrusion Detection and Prevention System (HIDPS)

HIDS identify host-local threats, such as illegal file access or alteration, by operating at the host or device level. By keeping tabs on system-level operations, this system can prevent both internal and external threats to individual devices.

D. IoT-based Network-Organization Handling IPS

The number of hosts and terminals in a computer network is growing exponentially in today's information and communication age. The number of security flaws and instances of illegal access to computer networks is also on the rise dramatically [22]. Among the most widely used strategies to support internet security measures are firewalls, access restrictions, antivirus software, malware, applications, behavioral analytics, data loss prevention, distributed denial of service (DDoS), and network segmentation. These techniques can filter content, block data outflow, alert about and prevent malicious activities, and so on. Typically, firewalls and spam filters employ basic rule-based algorithms to authorize or disallow protocols, ports, or IP addresses.

However, these firewalls and filters do have a few limitations, such as the fact that they can't always distinguish between "good traffic" and "bad traffic" and that they can't always handle complex DDoS attacks [23]. When combined with antivirus software, an intrusion detection system (IDS) greatly improves computer network security measures, making the case for safeguarding networks against unauthorized access more compelling. When looking at computers and networks through the lens of information systems, an intrusion is defined as any attempt to violate their availability, confidentiality, integrity, or security mechanisms.

IV. Challenges, Benefits and Emerging Technologies

AI has the potential to significantly improve cloud security, but a number of barriers stand in the way of its widespread application and success. Full utilization of AI-driven solutions for cloud security requires resolving these concerns and hurdles.

- **Data Privacy and Compliance:** Concerns about Access to massive datasets, which frequently contain sensitive information, is necessary for the employment of AI to cloud security [24]. This raises significant privacy concerns, particularly in light of stringent laws like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Make sure everyone is aware of the potential risks to their privacy while using AI services hosted in the cloud by calling attention to the importance of strong data encryption and anonymization measures.
- **Data Security and Privacy:** Data security in shared environments is still a major issue.
- **Regulatory Compliance:** The necessity to comply with industry-specific and legal regulations like GDPR and HIPAA complicates cloud adoption [25].
- **Vendor Lock-In:** Dependence on a small number of providers and a lack of adaptability are two potential outcomes of using proprietary tools and platforms.
- **Performance Concerns:** Problems with latency could arise in cloud settings for applications like real-time analytics and games.

A. Benefits of AI-Powered Cloud Security

Cloud security can greatly benefit from the introduction of generative AI, a new formative technology, in automating threat detection, incident handling in real-time, and vulnerability management [26]. Cloud computing outperforms conventional computing in terms of the benefits offered by a variety of services. Flexible security, data access from anywhere at any time, cost savings, portability, scalability, agility, and efficiency are just a few of the many benefits of cloud computing.

1) Improved Threat Detection Accuracy and Reduced False Positives

- AI and ML-powered security solutions are able to search for complex patterns in vast amounts of data.
- Identify dangers with higher precision than standard rule-based methods.
- Improves the security system's effectiveness and dependability by decreasing the number of false positive alerts.

2) Faster Response Times to Security Incidents

- Time spent detecting, analyzing, and mitigating events is decreased via automated AI-driven solutions.
- The ability to proactively and effectively defend against cyber threats is made possible.

3) Scalability to Handle Large Volumes of Security Data

- Big data pertaining to security (logs, network traffic, user actions) can be processed by AI and ML algorithms [27].
- Security solutions for the cloud are scalable and flexible enough to handle ever-growing cloud complexity.

4) Continuous Learning and Adaptation to Evolving Threats

- Systems driven by AI are always improving as they acquire new data.
- Update models to account for new dangers.
- Makes sure safety precautions work as intended over the long term.

5) Reduced Workload for Security Teams and Improved Efficiency

- Automates routine security tasks.
- Provides data-driven insights.
- Frees security teams to focus on strategic, high-impact initiatives.

Cloud computing has several advantages over hardware-based computing, including being a cost-effective service and being able to be utilized like a utility. The relocation of application processing from on-premises computers to the cloud is another appealing feature of cloud computing.

B. Integration with Emerging Technologies

The efficacy of AI-powered cloud security can be increased by combining it with emerging technologies like edge computing, blockchain, and the IoTs. The immutability and auditability of data pertaining to security can be enhanced with blockchain technology, which adds an extra safeguard to cloud settings [28]. Cloud security solutions that integrate AI with blockchain can use the distributed ledger to ensure that security events are authentic and that AI-based decisions are trustworthy. The technologies are displayed in Fig. 2.

1) AI Technologies for Cloud Security

AI has become an essential part of modernizing cloud security frameworks, enhancing threat detection and mitigation capabilities. The AI tools have been found to be effective in cloud security by detecting patterns, forecasting threats and responding to the attack in real-time using AI technologies like ML, DL, and NNs [29]. These technologies and, more so, cloud security utilize the volume of data processing and analysis to continually learn about new trends and systems become better with time without human intervention.

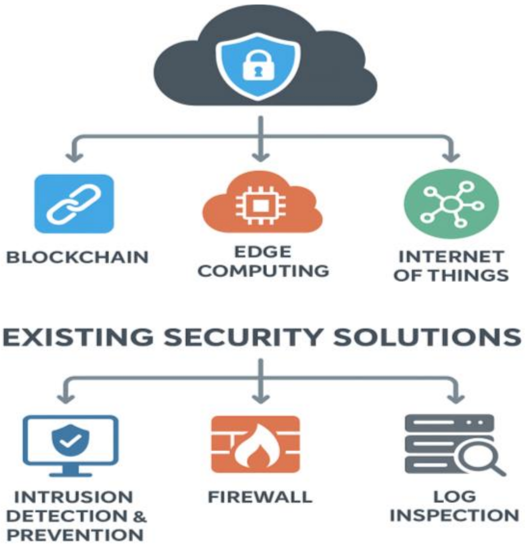

Fig. 2. Integration with Emerging Technologies.

2) Machine Learning (ML)

One of the most popular AI methods, which is known as ML, is the use of algorithms to identify patterns and make decisions using data [30]. ML models are used in cloud security in anomaly detection systems, which are able to signal abnormal behavior or unauthorized access.

3) Deep Learning (DL)

DL is also known as a part of ML, which entails neural networks in multiple layers, further advancing the recognition power with learning complexities and functions through large datasets. DL models are also very useful when identifying complex attacks like zero-day exploits or APTs, which are capable of bypassing traditional security systems.

4) Neural Networks (NNs)

The other important AI technology in the field of cloud security is the NNs that mimic how human brains process information [31]. They are especially good at categorizing complex data and making decisions on the basis of numerous input characteristics. In the cloud setup, NNs have the potential to be trained to detect more suspicious access patterns that signal a possible security threat, like a data breach or account takeover.

5) Intrusion Detection System (IDS)

Enterprise applications and operating systems are protected from vulnerabilities by Intrusion Prevention Systems (IPS) until patches or updates are released. This aids in thwarting attacks like zero-day attacks. Hardware, operating systems, and applications are frequently shared between cloud servers and virtual machines (VMs). Installing intrusion detection and prevention systems (IDS and IPS) on VMs provides a workaround for this.

6) Firewall

VMs in a regular cloud setting can have their attack surfaces diminished with the help of a firewall. Deploying a bidirectional firewall, also known as a two-way firewall, on individual virtual machines allows for the integrated administration of firewall policies. the firewall that includes a firewall and other filtering functions of the network appliance, for example, an inline intrusion prevention system and deep packet inspection [32].

7) Log Inspection

Administrators and service providers, whether they are located locally or remotely, have complete access to their organizations' resources and can therefore represent serious risks to data security. One of the most important things for a trustworthy environment is making sure system resources are secure. The purpose of audit logs in an information system is to track user actions and resource utilization, as well as to identify and fix IT problems.

V. Literature Review

This section reviews the research on machine learning-based intrusion detection in cloud security, as summarized in Table I.

Singh and Choudhry (2025) cloud computing, offering such as unparalleled flexibility, cost savings, and scalability, has changed the way companies manage their IT resources and IT ecosystem. Power of Generative AI (Gen AI) provides a much-needed and new approach for cloud infrastructure management. Gen AI offers a route towards self-optimizing, self-healing cloud settings by enabling systems to continuously learn from data and make autonomous decisions, in contrast to traditional rule-based automation [33].

Seth, Ratra and Sundareswaran (2025) Compliance automation ensures compatibility with regulations like PCI DSS for payment handling, while AI-powered security automation protects against evolving cyber threats. This paper also explores workflow facilitation, improving e-commerce operations, and integrating Gen AI into cloud coordination systems. As a result, operating costs are significantly reduced, service deployment is accelerated, and security breaches are reduced [34].

Sharma et al. (2025) AI-powered security products are intended to increase cloud infrastructure management scalability, reliability, and security posture. The overall aim is to identify the feasibility of AI, especially ML and DL methods, to complement the security aspects of cloud computing. These measures include intrusion detection systems (IDS), threat modeling, vulnerability management, real-time security monitoring, and anomaly detection. AI technologies offer a chance for these measures to be improved through adaptive response to ongoing threats, threat prediction of possible vulnerabilities, and automatic response on recommendations in real-time [35].

Al-Doori and Komotskiy (2024) explain sophisticated IDS and IPS techniques that use AI-based feature optimization and different ML techniques to improve network intrusion detection and prevention. The application of genetic algorithms and particle swarm optimization, two types of AI that seek to optimize characteristics in a way that maximizes both information gain and entropy, is a crucial part of this strategy. This is combined with boosting techniques, which are further improved by Random Forest (RF), to decrease class overlaps. Random Forest is paired with Grey Wolves Optimization (GWO) [36].

Innab et al. (2024) present a description of the different security attacks associated with the cloud environment, in addition to the other classifications and types of IDS. The difficulties intrusion detection systems face in cloud environments are also covered in the essay. Building a solid cybersecurity posture, safeguarding sensitive data, and guaranteeing the availability, confidentiality, and integrity of cloud-based services and infrastructure all depend on this conversation [37].

Qi et al. (2023) provide an investigation and analysis of the current state of IDS techniques in cloud computing. It encompasses the classification of existing techniques and an examination of the security requirements specific to cloud computing. Take a hard look at how AI may improve intrusion detection and methodically outline the new ways that cloud computing has approached intrusion detection. Examining the strengths and weaknesses of existing datasets allows us to assess these methods [38].

G et al. (2022) offer solutions to protect cloud systems by utilizing highly effective intrusion detection technologies. The efficiency of the detection methods and the rate of detection have been the principal areas of concentration within IDS. ML and parallelization, propose, can help us overcome these challenges. ML-based approaches learn from data automatically, making human experts less important [39].

TABLE I. Review Analysis of AI and ML Approaches for Cloud Security and Intrusion Detection

Author(s) & Year	Study Focus	Key Findings	Challenges	Limitations	Future Work
Singh & Choudhry (2025)	Generative AI in cloud infrastructure management	Gen AI enables self-optimizing, self-healing cloud environments by learning from data instead of rule-based automation	Complexity in integrating Gen AI into existing IT ecosystems	Early-stage adoption, lack of standardized frameworks	Develop robust frameworks for autonomous cloud management and scalability
Seth, Ratra & Sundareswaran (2025)	AI-powered security and compliance automation in cloud	Improves security, ensures compliance (e.g., PCI DSS), reduces operational costs, accelerates service rollout, and lowers breaches	Rapidly evolving cyber threats and regulatory landscapes	Dependence on AI system accuracy, potential false positives	Broader adoption of AI in compliance and workflow automation with enhanced trust
Sharma et al. (2025)	AI-powered security tools for cloud infrastructure	ML/DL improves IDS, threat modeling, vulnerability management, real-time monitoring, and anomaly detection	Handling dynamic threats and large-scale cloud infrastructure	Scalability of AI models, resource-intensive training	More adaptive and lightweight AI-based real-time response systems
Al-Doori & Komotskiy (2024)	AI-based IDS/IPS with feature optimization	Used PSO, GA, RF, Boosting, and GWO to improve IDS performance and reduce class overlap	High-dimensional data and overlapping classes	Computational cost of hybrid optimization approaches	Develop efficient, low-cost hybrid AI optimization for IDS/IPS
Innab et al. (2024)	Security attacks and IDS challenges in cloud	Classified IDS attacks and discussed challenges in cloud intrusion detection	Complexity of evolving attack vectors in cloud	Lack of unified taxonomy for IDS attacks	Create comprehensive IDS frameworks tailored for multi-cloud and hybrid environments

Qi et al. (2023)	Comparative analysis of IDS techniques in cloud	Classified IDS methods, summarized AI-enhanced intrusion detection, analyzed datasets	Dataset imbalance and lack of standardization	Limited benchmarking across real-world datasets	Build standardized IDS datasets and benchmarks for fair evaluation
G et al. (2022)	Machine learning + parallelization for IDS	ML improves detection effectiveness and speed when combined with parallelization	High resource demand for ML models	Reliance on data quality and lack of generalization	Optimize ML-based IDS for real-time cloud-scale deployment

VI. Conclusions and Future Scope

Cloud computing has brought new security risks, including data breaches, denial of service assaults, and unauthorized access, but it has also made modern enterprises more agile, cost-effective, and scalable. The increasing complexity of cyber-attacks has rendered traditional methods such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) ineffective. The use of AI and ML in cloud security has revolutionized the field, opening the door to adaptive defense mechanisms, automated incident response, predictive threat detection, anomaly analysis, and more. AI-powered approaches, including Web Intrusion Detection Systems (WIDS), host- and network-based IDPS, and IoT-integrated IPS, offer higher detection accuracy with reduced false positives, scalability for massive data processing, and continuous learning to counter emerging threats. Data privacy issues, false alarms, integration complexity, and adversarial assaults are still major obstacles that need to be resolved for long-term security, despite recent developments.

Future research should concentrate on establishing standardized frameworks for AI-driven cloud security and on developing hybrid solutions that combine blockchain, edge computing, and IoT to improve transparency, traceability, and real-time threat mitigation. Additionally, collaboration between industry, academia, and regulatory bodies will be essential to establish best practices, reduce false positives, and improve interoperability across multi-cloud and hybrid environments. By combining automation with human expertise, cloud security can evolve into a proactive, intelligent, and self-healing system capable of addressing the rapidly growing scale and sophistication of cyberattacks.

References

[1] G. Gupta, P. R. Laxmi, and S. Sharma, "A Survey on Cloud Security Issues and Techniques," Int. J. Comput. Sci. Appl., vol. 4, no. 1, pp. 125–132, Feb. 2014, doi: 10.5121/ijcsa.2014.4112.

[2] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion detection and prevention system for an IoT environment," Digit. Commun. Networks, vol. 8, no. 4, pp. 540–551, Aug. 2022, doi: 10.1016/j.dcan.2022.05.027.

[3] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[4] 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.

[5] S. R. Mamidi, "Enhancing Cloud Computing Security Through Artificial Intelligence-Based Architecture," J. Artif. Intell. Gen. Sci., vol. 5, no. 1, pp. 63–72, Jun. 2024, doi: 10.60087/jaigs.v5i1.166.

[6] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," Int. Res. J. Innov. Eng. Technol., vol. 9, no. 3, 2025, doi: 10.47001/IRJIET/2025.903027.

[7] A. Luqman, R. Mahesh, and A. Chattopadhyay, "Privacy and Security Implications of Cloud-Based AI Services : A Survey," vol. 1, no. 1, pp. 1–25, 2024.

[8] 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.

[9] D. Kavitha and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," IEEE Access, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3493957.

[10] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," ESP J. Eng. Technol. Adv., vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[11] B. S. Bhati and C. S. Rai, "A Survey on Intrusion Detection Tools," in 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 806–810.

[12] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," Int. J. Sci. Res. Mod. Technol., vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[13] S. K. A, A. Rajlingam, and B. Gokila, "Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies," Sci. Comput. Eng. Res., vol. 6, no. 8, pp. 6–11, 2023, doi: 10.46379/jscer.2023.0608002.

[14] 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.

[15] I. Gupta, A. K. Singh, C. N. Lee, and R. Buyya, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," 2022. doi: 10.1109/ACCESS.2022.3188110.

[16] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," Int. J. Artif. Intell. Data Sci. Mach. Learn., vol. 4, no. 3, pp. 18–30, Oct. 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[17] V. Shah, "Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 877–885, 2023.

[18] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," TIJER – Int. Res. J., vol. 11, no.

12, pp. 922–928, 2024.

[19] S. K. Wanjau, G. M. Wambugu, and A. M. Oirere, “Network Intrusion Detection Systems: A Systematic Literature Review of Hybrid Deep Learning Approaches,” Int. J. Emerg. Sci. Eng., vol. 10, no. 7, pp. 1–16, Jun. 2022, doi: 10.35940/ijese.F2530.0610722.

[20] A. Mahendiran, R. Appusamy, and K. S, “Intrusion Detection and Prevention System: Tchnologies and Challenges,” Int. J. Appl. Eng. Res., vol. 10, no. 87, pp. 1–12, 2015.

[21] S. Narang and V. G. Kolla, “Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing,” Int. J. Res. Anal. Rev., vol. 12, no. 3, pp. 1–7, 2025, doi: 10.56975/ijrar.v12i3.319048.

[22] S. Kumar, S. Gupta, and S. Arora, “Research Trends in Network-Based Intrusion Detection Systems: A Review,” IEEE Access, vol. 9, pp. 157761–157779, 2021, doi: 10.1109/ACCESS.2021.3129775.

[23] A. R. Bilipelli, “AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis: A Comparative Study,” Tech. Int. J. Eng. Res., vol. 11, no. 12, pp. a922–a928, 2024.

[24] S. Alzide, “Cloud Computing: Evolution, Challenges, and Future Prospects,” J. Inf. Technol. Cybersecurity, Artif. Intell., vol. 1, no. 1, pp. 52–63, Dec. 2024, doi: 10.70715/jitcai.2024.v1.i1.007.

[25] R. Patel, “Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence,” Int. J. Curr. Eng. Technol., vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[26] A. Patel, P. Pandey, H. Ragothaman, R. Molleti, and D. R. Peddinti, “Generative AI for Automated Security Operations in Cloud Computing,” in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), IEEE, Feb. 2025, pp. 1–7. doi: 10.1109/ICAIC63015.2025.10849302.

[27] R. Q. Majumder, “Machine Learning for Predictive Analytics: Trends and Future Directions,” Int. J. Innov. Sci. Res. Technol., vol. 10, no. 4, pp. 3557–3564, May 2025, doi: 10.38124/ijisrt/25apr1899.

[28] S. C. G. Varma, “AI-Enhanced Cloud Security: Proactive Threat Detection and Response Mechanisms,” Int. J. Multidiscip. Res., vol. 6, no. 6, pp. 1–11, Dec. 2024, doi: 10.36948/ijfmr.2024.v06i06.31587.

[29] V. Varma, “Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization,” ESP J. Eng. Technol. Adv., vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[30] S. Srinivasan, R. Sundaram, K. Narukulla, S. Thangavel, and S. B. Venkata Naga, “Cloud-Native Microservices Architectures: Performance, Security, and Cost Optimization Strategies,” Int. J. Emerg. Trends Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 16–24, 2023, doi: 10.63282/3050-9246.ijetcsit-v4i1p103.

[31] V. M. L. G. Nerella, K. K. Sharma, S. Mahavratayajula, and H. Janardhan, “A Machine Learning Framework for Cyber Risk Assessment in Cloud-Hosted Critical Data Infrastructure,” J. Inf. Syst. Eng. Manag., vol. 10, no. 4, pp. 2409–2421, 2025.

[32] H. Sharma, “Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud,” Eng. Technol. Adv., vol. 1, no. 1, pp. 98–111, 2021, doi: 10.56472/25832646/JETA-V1I1P112.

[33] K. A. Singh and A. Choudhry, “AI-Powered Strategies for Cloud Infrastructure Management,” in 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, IEEE, Apr. 2025, pp. 1–5. doi: 10.1109/OTCON65728.2025.11070393.

[34] D. K. Seth, K. K. Ratra, and A. P. Sundareswaran, “AI and Generative AI-Driven Automation for Multi-Cloud and Hybrid Cloud Architectures: Enhancing Security, Performance, and Operational Efficiency,” in 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Jan. 2025, pp. 00784–00793. doi: 10.1109/CCWC62904.2025.10903928.

[35] L. Sharma, A. Dokania, A. Verma, D. P. Shah, P. M. Parekh, and S. S. Shinde, “AI-Augmented Security Protocols for Scalable Cloud Infrastructure Management,” in 2025 International Conference on Engineering, Technology &amp; Management (ICETM), IEEE, May 2025, pp. 1–6. doi: 10.1109/ICETM63734.2025.11051957.

[36] M. B. Al-Doori and E. I. Komotskiy, “Intrusion Detection and Prevention System AI Based Features with Random Forest,” in 2024 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), May 2024, pp. 326–328. doi: 10.1109/USBEREIT61901.2024.10584056.

[37] N. Innab et al., “Intrusion Detection System Mechanisms in Cloud Computing: Techniques and Opportunities,” in 2024 2nd International Conference on Cyber Resilience (ICCR), IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICCR61006.2024.10532903.

[38] W. Qi, W. Wu, H. Wang, L. Ou, N. Hu, and Z. Tian, “Intrusion Detection Techniques Analysis in Cloud Computing,” in 2023 IEEE 12th International Conference on Cloud Networking (CloudNet), IEEE, Nov. 2023, pp. 360–363. doi: 10.1109/CloudNet59005.2023.10490069.

[39] G. R. G, R. Santhoshkumar, D. Venkatesan, K. S, and P. S. K. Patra, “Intrusion Detection in Cloud Architecture Using Machine Learning,” in 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), IEEE, Dec. 2022, pp. 483–487. doi: 10.1109/ICAC3N56670.2022.10074376.