Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Leveraging Artificial Intelligence for Enhanced Data Protection: A Comprehensive Review of Cloud Security amid Emerging threats

Deepthi Kamidi [1], Dr PVRD Prasada Rao [2]

[1] *Scholar, Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, A.P.-522302. India. Email: deepthikamidi83@gmail.com*

[2] *Professor, Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, A.P. – 522302. India, Email: pvrdprasad@kluniversity.in*

ARTICLE INFO

Received: 24 Dec 2024

Revised: 14 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

Cloud computing offers scalable, adaptable, and affordable solutions that spur innovation across multiple industries, it has fundamentally changed how industries function. However, with this widespread adoption comes the growing challenge of protecting sensitive data, especially as more sophisticated cyberattacks become common. Advanced Persistent challenges (APTs), insider assaults, data breaches, and Distributed Denial of Service (DDoS) attacks are just a few of the challenges that modern cloud environments must contend with. These threats highlight flaws in conventional security paradigmsThe integration of cutting-edge technologies like artificial intelligence (AI) and machine learning (ML) into cloud security is becoming more and more important in response to these issues. These technologies are proving to be effective instruments for increasing prediction accuracy, automating threat detection, and enabling real-time encryption protocol modifications. We can improve cloud security by utilising AI and ML to detect anomalies, find zero-day vulnerabilities, and employ predictive models that assist in addressing problems before they become more serious. A thorough analysis of the present uses of AI and ML in cloud security is provided in this work including how these tools are being used to enhance traditional methods like encryption and access control. It also evaluates the latest research in AI-driven threat detection, behavioral analysis, and adaptive encryption. Additionally, we highlight critical gaps in current AI/ML security frameworks, particularly in terms of scalability, false positive rates, and the challenges of real-time implementation. The primary goals of this review are threefold: first, to systematically analyze the emerging threats to cloud data security; second, to propose the development of more adaptive and robust algorithms that use AI and ML to enhance cloud protection; and third, to present a framework for integrating these algorithms into existing cloud security infrastructures. Ultimately, we hope this review contributes valuable insights that can shape the future of AI/ML-driven cloud security, helping to tackle the evolving challenges that come with modern cloud computing.

Keywords: Cloud security, Artificial Intelligence, Machine Learning, Data protection, Emerging threats, Predictive security, Adaptive encryption, Threat detection.

INTRODUCTION

With its scalable and adaptable services, cloud computing has completely changed data management, but it also brings with it difficult security issues. Traditional security methods are increasingly inadequate against sophisticated threats like Advanced Persistent Threats (APTs) [1] and insider attacks, particularly in multi-tenant cloud environments. Artificial Intelligence (AI) and Machine Learning (ML) are emerging as powerful solutions to these security challenges, offering adaptive, real-time threat detection and response capabilities. AI-based systems can analyze massive amounts of data, recognize anomalies, and detect previously unknown threats that conventional rule-based systems might miss. Two deep learning techniques that have shown significant promise in reducing false positives and improving threat identification are convolutional neural networks [2] and long short-term memory networks.

The research aims to develop adaptive security frameworks that can dynamically counter evolving cyber threats, integrate AI algorithms [3] into existing security systems, and provide robust protection for cloud infrastructure while maintaining compliance with ethical and regulatory guidelines. In Figure 1: it can be observed that how in the cloud architecture various attacks can be done at different levels.

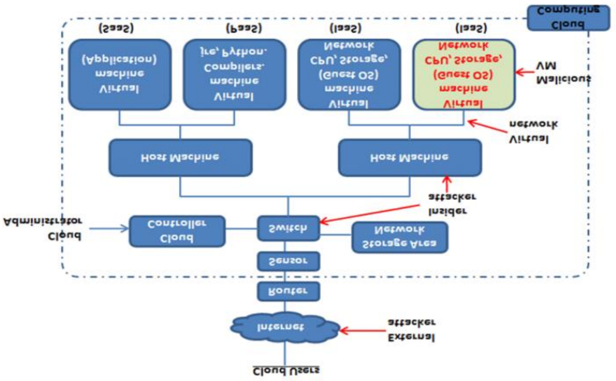

Figure 1. The various stages of attack as in the cloud architecture.

CLOUD SECURITY: A BRIEF OVERVIEW

Traditional Security Approaches

When it comes to securing data in the cloud, the standard approach has traditionally involved tried-and-tested techniques like encryption, authentication, and access control. These methods ensure that sensitive data stays protected while it's stored and transmitted. For example, data is frequently jumbled using encryption techniques like RSA and AES (Advanced Encryption Standard), rendering it unintelligible to anyone lacking the necessary keys. However, access control systems like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) limit who has access to certain data based on their responsibilities or specified policies [4].

In addition to these techniques, the first line of defence in cloud settings is comprised of firewalls and Intrusion Detection Systems (IDS)[5]. Firewalls are responsible for monitoring and filtering traffic based on predetermined ruples, while IDS are designed to flag suspicious activities by analyzing traffic patterns [6]. However, most IDS rely on signature-based techniques, where they match known attack signatures to identify potential threats. In Figure 2 the architecture of an intrusion detection is observed.

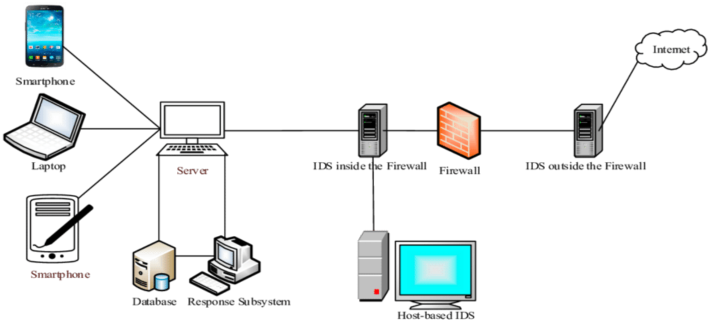

Figure 2. Intrusion Detection System Architecture

While these traditional methods are certainly valuable, they come with limitations. Encryption and access control, for instance, are static measures that require regular manual updates to stay effective. They can't adapt to rapidly changing threats on their own, and they fall short when it comes to protecting against insider threats—those situations where authorized users misuse their access [7]. Furthermore, static encryption doesn't provide enough defense against more advanced and subtle attacks, like malware injections or stealthy Advanced Persistent Threats (APTs)[8], where attackers gain access and remain unnoticed for long periods.

IDS systems also face hurdles, primarily because they are signature-based and only identify known threats. This makes cloud environments vulnerable to zero-day attacks—those that exploit previously unknown vulnerabilities—since such attacks don't match any known signatures [9]. As hackers become more sophisticated, it's clear that traditional security measures need to evolve to offer real-time, adaptive protection.

Challenges in Traditional Methods

Cloud environments present unique security challenges due to their distributed, multi-tenant nature, which creates multiple potential vulnerabilities for cybercriminals [10]. These infrastructures are particularly susceptible to Advanced Persistent Threats (APTs) [11], where hackers can infiltrate systems and remain undetected for extended periods by exploiting legitimate credentials. Insider threats further compound the risk, as employees with authorized access can intentionally or accidentally compromise data security. Traditional security measures are increasingly inadequate in detecting nuanced, sophisticated attacks within these complex, dynamic cloud networks, underscoring the urgent need for more intelligent, adaptive security solutions that can monitor and respond to evolving threats in real time. Below Figure 3 shows the analytics of various attacks on the cloud.

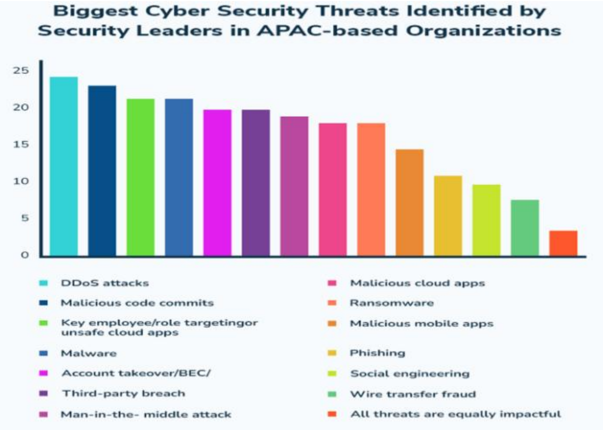

Figure 3. The analytics of various attacks on the cloud.

Need for Advanced Solutions

By offering sophisticated, adaptable defence against changing cyberthreats, AI and machine learning are revolutionising cloud security [12]. By examining enormous volumes of data, spotting irregularities, and spotting trends that conventional security systems might overlook, these technologies are excellent at real-time threat detection. Neural network-based predictive threat forecasting, dynamic adaptive encryption, and automated incident response capabilities are some of the main benefits. Businesses may proactively identify and stop any breaches before they do serious harm by utilising AI's capacity to learn from past data and quickly adjust to shifting security environments. As cyber threats become increasingly sophisticated, AI and ML technologies [13] offer a crucial evolutionary step in cloud security strategies, enabling more intelligent, responsive, and efficient protection of digital infrastructure.

Dynamic AI-Driven Encryption Techniques

As cyberattacks become more advanced, static encryption techniques are no longer enough to protect sensitive data in the cloud. AI-driven encryption offers a more dynamic approach by allowing encryption protocols to be adjusted in real-time based on threat assessments. These AI-powered systems evaluate the current threat landscape and automatically adapt the encryption methods, ensuring that data remains secure even in high-risk environments [14].

One of the most effective techniques in this space is reinforcement learning, which allows systems to continuously learn and optimize their encryption strategies based on their interactions with the environment. Reinforcement learning algorithms assess the current security context—whether it's a detected threat or a vulnerability—and adjust encryption protocols accordingly [15]. For example, if a system detects a heightened security risk, it might apply a more complex encryption method like homomorphic encryption, which allows data to be processed without decryption, ensuring confidentiality even when the data is in use [16].

AI-driven encryption also strikes a balance between security and performance by dynamically adjusting encryption levels based on the severity of the threat. When the threat level is low, the system can use lighter encryption to reduce computational overhead and improve performance. Conversely, when the risk is high, the system can automatically switch to stronger encryption protocols to maximize security [17]. This flexibility makes AI-driven encryption an excellent fit for cloud environments, where both security and performance are critical.

SURVEY OF EXISTING LITERATURE

Studies on AI and ML in Cloud Security

AI and ML have been generating a lot of interest in the field of cloud security due to their impressive ability to detect threats in real-time, adapt to new challenges, and generally make cloud environments more resilient. There have been numerous studies highlighting just how effective these technologies can be in spotting and dealing with a wide range of security threats[18].

One comprehensive survey conducted by Sharma et al. reviewed various AI and ML techniques used in cloud security, focusing on their applications in cybersecurity. The study highlighted AI-driven anomaly detection, automated incident response, and dynamic encryption as areas with the most potential for further exploration. According to the authors, AI-based systems can continuously monitor cloud traffic, flag irregularities that might indicate an attack, and respond on their own—capabilities that are especially valuable in large-scale, multi-tenant cloud environments.

The expanding significance of AI in combating insider risks, Advanced Persistent risks (APTs), and Distributed Denial of Service (DDoS)[19] attacks in the cloud was highlighted in another thorough assessment by Ghafir et al. Their findings showed that ML models, especially unsupervised learning techniques and deep learning models, outperformed traditional methods that rely on signatures for detecting these complex and evolving threats. For instance, unsupervised clustering algorithms were able to spot deviations in typical cloud behavior, signaling potential insider misuse or a malicious attack. Deep learning models like LSTM networks were also highly effective, particularly in identifying and mitigating APTs by analyzing long-term patterns in cloud system logs.

In another study, Pham and Nguyen demonstrated that ML-based models significantly enhanced intrusion detection capabilities in cloud environments. Models like Random Forest and SVM provided robust classification of cloud traffic, while unsupervised techniques like K-Means clustering helped identify zero-day vulnerabilities by flagging outliers in network behavior. This shows the increasing trend of integrating AI and ML into security frameworks to effectively detect and prevent sophisticated attacks.

Comparison of Cloud Security Frameworks

Several AI-enhanced cloud security frameworks have been proposed in recent years to address specific challenges unique to cloud environments. These frameworks develop more intelligent, flexible methods for threat detection, encryption, and incident response by utilising a variety of AI and ML methodologies. Convolutional Neural Networks (CNNs)[20] are used in Zhang and Wang's deep learning-based cloud security architecture, for instance, to identify anomalous network traffic patterns. Their model achieved impressive accuracy in identifying anomalies that could indicate DDoS attacks or unauthorized access attempts. They found that CNNs could handle vast amounts of network data and extract key features, which significantly improved the detection of malicious activities.

On the other hand, Hussain and Hussain introduced an AI-based incident response system that autonomously adjusts security policies based on real-time threat levels. Their framework leverages reinforcement learning to dynamically change access controls, encryption levels, and firewall settings depending on the severity of detected threats. The primary advantage of this system is that it can respond to threats without manual intervention, which helps reduce response time and minimize the risk of prolonged exposure to attacks.

Another study, conducted by Liu et al., compared traditional rule-based security frameworks with AI-enhanced systems. The results clearly favored AI-enhanced approaches, which showed better performance in terms of threat detection and response efficiency. The AI-based framework was able to reduce false positives by using ML algorithms to analyze historical attack data, which improved the accuracy of anomaly detection

Lastly, we need to think about the moral and legal issues surrounding the use of AI in cloud security. Concerns over responsibility and adherence to data protection laws such as the General Data Protection Regulation (GDPR) are raised by AI systems' ability to make decisions on their own regarding data access, encryption, and incident response. Further research is needed to determine how AI-based security frameworks can operate legally while preserving accountability and transparency in automated decision-making processes. The AI and ML-based cloud security frameworks are contrasted in Table 1 below.

Table 1: Comparative Table of AI and ML-based Cloud Security Frameworks

Technique	**Application**	**Advantages**	**Limitations**
AI-driven anomaly detection.	Continuous monitoring and autonomous response to cloud traffic irregularities.	Real-time detection and response, crucial for large-scale environments.	Potential for false positives in dynamic environments.
Unsupervised learning, LSTMs	Tackling insider threats, APTs, and DDoS attacks in the cloud.	Better detection of complex, evolving threats compared to traditional methods.	High computational requirements for deep learning models.
Random Forest, SVM, K-Means	Enhancing intrusion detection and identifying zero-day vulnerabilities.	Robust classification of cloud traffic and identification of outliers.	Difficulty with handling large-scale, real-time analysis due to computational limitations.
Deep Learning (CNNs)	Detecting abnormal traffic patterns indicative of DDoS or unauthorized access.	High accuracy with automated feature extraction from large datasets.	Requires significant computational resources and labeled data.
Reinforcement Learning [11]	Autonomous adjustment of security policies based on real-time threat assessments.	Minimizes response time, reducing exposure to attacks.	Complex to implement in multi-tenant, large-scale environments.
AI-enhanced security framework	Comparing rule-based vs. AI-based frameworks for threat detection and response efficiency.	Reduced false positives and faster adaptation to new threats.	Integration challenges with existing cloud infrastructure.
Layered Security Protocols & Shared Responsibility Model	Implementing multiple layers of security, including encryption and user authentication & Both IoT users and cloud service providers must collaborate to ensure security,	can help protect against cyber threats & emphasizing a shared responsibility for safeguarding data	As the number of layers increases, managing and maintaining the security infrastructure becomes more complex.
SEPCVN Protocol	designed to enhance data transmission efficiency while addressing security flaws	utilizing specialized authentication methods	Some of the limitations are bandwidth restrictions, Rigid message structure.
O-HMACSHA3	combines Particle Swarm Optimization (PSO) with a secure hash algorithm, achieving a turnaround time (TAT) of 316	outperforming traditional methods	Potential length extension vulnerabilities also needs to focus on complex key

Technique	Application	Advantages	Limitations
	milliseconds and energy consumption of 47.7 joules for 20 tasks,		management requirements.

Core Finding:

1. **AI-driven Anomaly Detection**: Most frameworks focus on anomaly detection, which is effective but prone to false positives, especially in dynamic environments. Hybrid AI models are increasingly used to mitigate this issue.
2. **Deep Learning Models**: CNNs are effective in extracting features from network data for threat detection but require extensive labeled data and computational resources.
3. **AI-based Incident Response**: Autonomous systems that adjust security policies in real-time offer a significant reduction in response times but are challenging to implement on a large scale.
4. **Dynamic Encryption**: AI-driven dynamic encryption systems adapt to real-time threats but can introduce computational overhead, especially in large, multi-tenant cloud environments.
5. **Research Gaps**: Several frameworks lack integration across the entire security lifecycle, and there are concerns about the ethical implications of autonomous AI systems in cloud security.

PROPOSED METHODS FOR FUTURE RESEARCH

The sophistication and frequency of cyber attacks are increasing along with cloud computing. Even while AI and ML have already shown a great deal of promise in improving cloud security, some crucial areas still need more study and advancement. These advancements are crucial for making data protection more effective and for mitigating new types of threats. Below, we outline the proposed objectives for future research on AI/ML-driven cloud security.

Identification and Analysis of Emerging Threats

With new attack types including malware insertion, cloud jacking, insider attacks, and side-channel attacks becoming increasingly prevalent in cloud systems, the landscape of cyber threats is continuously shifting. To keep up, it's critical that we improve our ability to identify and analyze these emerging threats. One of the technique is Multi-dimensional computation trust, it is computed using multi-dimensional quality of service (QoS) evidence and user feedback, which helps in identifying malicious behaviors such as collusion and Sybil attacks. AI and ML, with their strength in processing massive datasets and detecting complex patterns, are well-suited for this task. However, existing models still struggle when it comes to zero-day threats and unknown vulnerabilities, making this an important area for future research. Below Figure 4 shows the various security risks in the cloud computing.

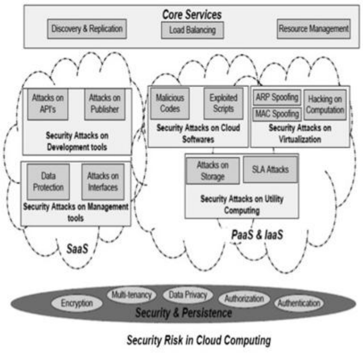

Figure 4. Security Risks in Cloud Computing

Research should focus on developing advanced AI and ML models capable of continuously monitoring cloud traffic and user behavior to spot these emerging threats. Promising methods such as unsupervised learning, reinforcement learning, and deep learning (such as CNN and LSTM models) may be able to identify abnormalities that point to novel attack types. By analyzing real-time data from cloud infrastructure, these models can identify deviations from normal patterns, signaling the possibility of an attack. For example, reinforcement learning could be used to observe user activity, allowing the system to learn and adapt security measures dynamically whenever abnormal behavior is detected, preventing threats before they escalate.

Additionally, Blockchain technology provides a distributed ledger that enhances the security of key management processes, mitigating risks associated with centralized systems .AI models must be equipped to recognize more complex, multi-vector attacks like APTs and insider threats. These types of attacks often consist of a series of seemingly harmless actions that, when looked at together, reveal a malicious pattern. In order to prevent overburdening cloud managers with pointless alerts—a major difficulty in today's hectic cloud environments—future models should concentrate on lowering false positives while preserving high detection accuracy. The different attacks occurring at different stages in the cloud are depicted in figure 5 below.

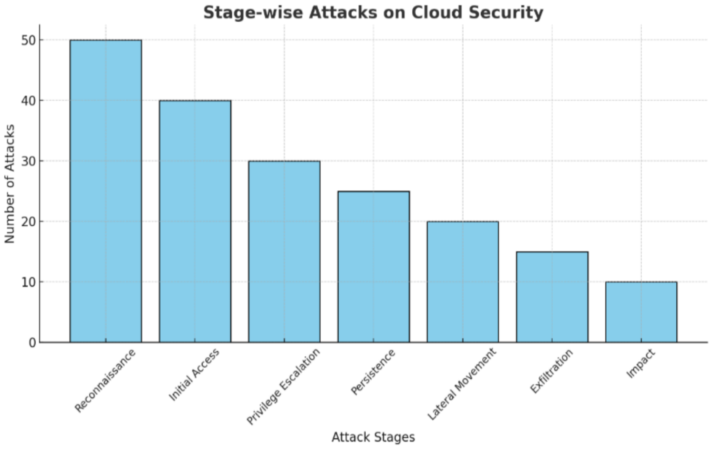

Figure 5. Attacks at various stages in Cloud.

Development of Robust Data Protection Algorithms

As cyber threats become more sophisticated, traditional measures like static encryption and basic access control aren't enough to protect data in the cloud. Future research should prioritize developing adaptive algorithms that can adjust dynamically to the security needs of cloud systems in real time. These algorithms should integrate AI-driven encryption, ML-based anomaly detection, and predictive security models to form a comprehensive security framework.

One promising direction is the development of AI-driven adaptive encryption algorithms that can modify encryption protocols based on the current level of threat. For instance, reinforcement learning could be used to determine the best encryption method based on the sensitivity of the data and the present risk assessment [21]. During periods of heightened risk, such as during an ongoing attack, stronger encryption could be applied, while lighter encryption could be used during regular operations to optimize system performance. Another exciting area is homomorphic encryption, which allows data to be processed without decryption, thus providing enhanced security for sensitive data in the cloud without sacrificing functionality.

Another area of focus should be the creation of predictive security models capable of forecasting potential threats before they occur. By analyzing historical data, these models could identify patterns that often precede a security incident, allowing cloud providers to take preventive action. Models like LSTMs are particularly effective here, given their ability to process and analyze sequences of data to predict threats based on past events. This proactive approach gives cloud administrators the ability to adjust security settings or take preventive measures in advance.

Scalability should also be a priority for future algorithms. These adaptive security measures must be able to work efficiently in multi-tenant cloud environments without consuming too many resources. This includes creating real-time, lightweight AI models that don't require a lot of processing power, which is crucial for massive cloud infrastructures.

Implementation of Proposed Algorithms

Successfully implementing AI and ML-based security algorithms in real-world cloud environments presents several practical challenges. These include ensuring seamless integration with existing cloud architectures, minimizing false positives, maintaining computational efficiency, and scaling effectively.

Research should explore how to integrate AI-driven security algorithms into existing cloud infrastructure without disrupting operations. This includes embedding AI models within Security Information and Event Management (SIEM) systems for real-time threat detection and automated responses. Integrating with SIEM systems allows for continuous monitoring and provides a full view of potential security incidents. With AI algorithms in place, organizations can dynamically adjust security measures as threats evolve, without requiring constant human intervention.

Another challenge is the computational overhead that AI-driven security systems often introduce. Many AI models, particularly those that use deep learning, require significant processing power, which makes them difficult to use in real-time cloud operations. Future research should focus on developing more computationally efficient algorithms, potentially by using edge computing, where AI models are distributed closer to where the data is generated. This approach reduces latency and resource consumption on the central cloud server [22]. Edge AI could also help with scalability by moving some of the computational load away from the central cloud infrastructure, allowing security systems to operate more efficiently.

Furthermore, federated learning—in which AI models are taught across several dispersed devices without sending raw data to a central server—should be taken into account in future studies. By dividing the computational load among several nodes, this method not only increases privacy by preserving sensitive data locally, but it also increases the scalability of AI-driven security solutions. This could be particularly useful in multi-tenant cloud environments, where data from various clients needs to be processed securely and simultaneously.

Ethical and Legal Considerations in AI-Driven Security

A critical but often overlooked aspect of implementing AI-driven security algorithms in the cloud is the ethical and legal considerations. As AI systems take on greater responsibility for critical security decisions, concerns about transparency, accountability, and adherence to laws such as the General Data Protection Regulation (GDPR) surface. Future research must address how to make AI-based systems more transparent so that the decisions they make can be explained and audited. Additionally, researchers must consider how to develop AI-driven security solutions that comply with existing legal frameworks while still maintaining the privacy and security of sensitive data. Below Table 2 shows the comparison of various AI/ML driven security methods adapted in cloud and their benefits and challenges faced.

Table 2: Comparative Table of Future Research Objectives in AI/ML-Driven Cloud Security

Method	Proposed Method	Potential Benefits	Challenges
Identification and Analysis of Emerging Threats	Advanced AI/ML models (unsupervised learning, reinforcement learning, deep learning)	Continuous monitoring for previously unknown threats (e.g., zero-day attacks, APTs).	High computational requirements and potential for false positives in dynamic environments.
Development of Robust Data Protection Algorithms	AI-driven adaptive encryption, predictive security models (LSTMs, RL-based models)	Dynamically adjust encryption and access control policies based on real-time threats.	High resource consumption for continuous adaptation; balancing security and performance.

Method	Proposed Method	Potential Benefits	Challenges
Implementation of Proposed Algorithms	Integration into existing SIEM systems, edge AI for scalability, federated learning	Real-time threat detection, improved scalability, reduced response times.	Integration complexity, computational overhead, and scalability across multi-tenant environments.
Ethical and Legal Considerations	Ensuring transparency and accountability in AI-driven decisions, GDPR compliance	Legal compliance, transparent decision-making, increased trust in AI security systems.	Balancing automation with accountability, potential conflicts with privacy regulations.

Notable Trends from Our Findings:

Emerging Threat Detection: AI/ML models (e.g., reinforcement learning, unsupervised learning) are essential for identifying novel threats, but require advanced computational capabilities to operate effectively in real-time cloud environments.

Adaptive Data Protection: AI-driven encryption and predictive security models offer dynamic responses to threats, but these algorithms must balance performance and security to ensure efficient use of cloud resources.

Algorithm Implementation: Integration of AI models into cloud systems, especially through edge AI and federated learning, can improve scalability and efficiency but introduces challenges in seamless integration and computational resource management.

Ethical and Legal Considerations: As AI systems autonomously make security decisions, ensuring transparency, accountability, and compliance with data regulations like GDPR will be crucial.

Global Developments and Future Directions in AI-driven Cloud Security

Globally, cloud security is advancing rapidly as AI and ML become integral to protecting data in dynamic, multi-tenant cloud environments. Developments include anomaly detection systems that leverage deep learning models, like CNNs and LSTMs, to identify irregular patterns in real-time; adaptive encryption methods using reinforcement learning to strengthen security based on threat levels; and predictive threat modeling that forecasts potential risks by analyzing historical data. AI is also increasingly used in automated incident response systems embedded in Security Information and Event Management (SIEM) platforms, providing swift and autonomous reactions to detected threats.

To further improve the efficiency of these systems, my idea focuses on two key areas:

Resource-efficient AI Models: Developing lightweight, adaptive AI models optimized for real-time analysis and lower resource consumption would improve performance in large-scale cloud environments. Edge AI, where processing is distributed closer to the data source, can reduce latency and offload computational demands from central servers. This approach allows for more scalable, responsive security systems that function efficiently even in high-demand situations.

Federated Learning for Privacy-preserving Security: Federated learning enables AI models to be trained across multiple cloud nodes without centralizing data, which not only improves privacy but also reduces data transfer overheads. By integrating federated learning with AI-based threat detection, cloud providers can enhance security without compromising user privacy or increasing data processing costs, ensuring efficient and secure operations across distributed cloud systems.

CONCLUSION

Cloud security is being revolutionised by artificial intelligence (AI) and machine learning (ML), which offer sophisticated, dynamic defence against ever-more-complex cyberthreats. By using advanced anomaly detection, predictive analytics, and adaptive encryption techniques, these technologies allow for real-time threat detection. These techniques are more effective than static ones at identifying and addressing possible security threats. Artificial intelligence (AI)-driven security systems are able to foresee possible breaches, analyse previous data, and dynamically modify protection measures by utilising methods such as neural networks and reinforcement learning. Despite significant promise, these approaches face challenges including high false positive rates, computational complexity, and the need for transparent, ethical decision-making. Ongoing research focuses on refining detection algorithms, improving system integration, and developing more precise, scalable security frameworks that can protect cloud infrastructures while maintaining performance and adhering to legal standards, representing a critical evolution in cybersecurity strategy. Developing advanced AI and ML models for continuous monitoring. Focusing on unsupervised learning techniques for threat detection. Enhancing algorithms for adaptive and robust cloud protection.

REFERENCES

[1] E. Bertino, "Data protection in cloud computing," IEEE Computer, vol. 47, no. 2, pp. 76-79, Feb. 2014.

[2] Cloud Security Alliance (CSA), "Top Threats to Cloud Computing: The Egregious Eleven," Report, 2019.

[3] P. Gupta, et al., "Artificial intelligence applications in security mechanisms of cloud computing: A review," International Journal of Computer Science and Information Security, vol. 14, no. 6, pp. 1-7, 2016.

[4] K. A. Dey, et al., "Real-time detection and prevention of security threats in cloud using machine learning algorithms," International Journal of Information Management, vol. 40, pp. 138-149, 2018.

[5] A. Shone, et al., "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018.

[6] K. Zhang and X. Liao, "AI-driven encryption and data privacy in cloud computing environments," IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, pp. 2625-2637, Oct. 2019.

[7] Y. Xiao and S. Xiao, "Emerging threats in cloud security: A survey," IEEE Cloud Computing, vol. 6, no. 1, pp. 40-47, Jan./Feb. 2019.

[8] S. Zhang and Q. Wang, "A survey of intrusion detection techniques in cloud computing environments," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2752-2770, 2015.

[9] R. Zhang, J. He, and Z. Han, "Security-aware resource allocation for mobile social big data: A deep reinforcement learning approach," IEEE Transactions on Network Science and Engineering, vol. 6, no. 3, pp. 576-588, Jul.-Sept. 2019.

[10] G. P. Wampler, M. J. Steindorf, and A. S. Wadhwani, "Detecting zero-day attacks using machine learning in cloud computing environments," Proceedings of the IEEE International Conference on Cloud Computing, 2019, pp. 543-550.

[11] M. Shehab, et al., "Security-as-a-service for cloud environments: Towards continuous security," Proceedings of the 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), pp. 424-431.

[12] Y. Liang and J. Du, "A recurrent neural network approach to model predictive control in cloud environments," IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 7, pp. 2033-2045, Jul. 2019.

[13] Y. Xiao and S. Xiao, "Emerging threats in cloud security: A survey," IEEE Cloud Computing, vol. 6, no. 1, pp. 40-47, Jan./Feb. 2019.

[14] S. Gupta, "Unsupervised learning approaches to anomaly detection in cloud computing environments," Proceedings of the 2020 IEEE International Conference on Cloud Engineering (IC2E), pp. 156-163.

[15] B. Taher, et al., "Hybrid supervised and unsupervised models for improved anomaly detection in cloud environments," IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 555-567, Apr.-Jun. 202.

[16] X. Wang, et al., "Advanced persistent threat detection using LSTM networks," IEEE Access, vol. 8, pp. 108512-108524, 2020.

[17] L. Sun and K. Zhang, "Reducing false positives in anomaly detection using hybrid AI models," Proceedings of the 2020 IEEE International Conference on Cloud Engineering (IC2E), pp. 124-132.

[18] J. Singh, T. Pasquier, and D. Eyers, "Hybrid cloud security: Adaptive methods for reducing false positives," IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 80-91, Jan.-Mar. 2021.

[19] R. Dutta and A. Banerjee, "AI-driven dynamic encryption in cloud computing: Current approaches and future trends," Journal of Cloud Computing, vol. 9, no. 30, pp. 1-18, 2021.

[20] S. Kang, et al., "Towards an integrated AI-based security framework for cloud computing," Proceedings of the 2021 IEEE International Conference on Cloud Computing (CLOUD), pp. 345-353.

[21] M. Chen and Y. He, "Adaptive encryption for cloud computing: A deep reinforcement learning approach," Proceedings of the 2021 IEEE International Conference on Cloud Computing (CLOUD), pp. 310-319.

[22] S. Garg and A. Kaur, "Edge AI for cloud security: A distributed approach for threat detection," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7585-7597, Aug. 2020.