Enhancing Cloud Security with AI Techniques

Soonja Yeom
School of Information and Communication Technology, University of Tasmania, Hobart, 7001, Australia
soonja.yeom@utas.edu.au

Geonmin Kim
Dept. of Software Engineering
Chonnam National University
Gwangju, Korea
204869@jnu.ac.kr

Kyungbaek Kim*
Dept. of Artificial Intelligence Convergence, Chonnam National University, South Korea'
kyungbaekkim@jnu.ac.kr

*Corresponding Author: Kyungbaek Kim (kyungbaekkim@jnu.ac.kr)

ABSTRACT

As cloud infrastructures expand across public, private, and hybrid models, ensuring robust cybersecurity has become a critical challenge. Traditional, static security mechanisms struggle to defend against sophisticated threats such as misconfigurations, insider attacks, and multi-cloud vulnerabilities. This paper reviews six recent studies that explore artificial intelligence (AI)-based approaches to strengthen cloud security. The surveyed methods include machine learning models for intrusion detection, reinforcement learning for adaptive threat response, blockchain-powered frameworks for decentralized identity and access management, and generative AI for intelligent orchestration and automation. These technologies address key challenges in dynamic threat detection, resource allocation, compliance enforcement, and operational resilience. The reviewed works demonstrate how AI and distributed technologies can significantly improve scalability, accuracy, and privacy in cloud systems. Furthermore, the integration of smart contracts, fuzzy logic, and optimization algorithms enables real-time decision-making and policy automation across heterogeneous environments. This review highlights the transition from static defense to proactive, intelligent, and decentralized security architectures in modern cloud computing. Future directions emphasize the need for explainable AI, quantum-resilient encryption, and interdisciplinary research combining AI, cryptography, and policy.

KEYWORDS

Cloud Security, Artificial Intelligence, Threat Detection

1. INTRODUCTION

As cloud computing becomes the cornerstone of digital transformation, enterprises increasingly depend on public, private, and hybrid cloud platforms to ensure scalability, flexibility, and cost efficiency. However, this shift brings an expanded attack surface, exposing cloud infrastructures to advanced persistent threats (APTs), misconfigurations, insider attacks, and regulatory non-compliance risks. Traditional static security models, which rely on perimeter-based defenses, are no longer sufficient to address the dynamic and distributed nature of modern cloud environments.

In response, artificial intelligence (AI) and related technologies such as machine learning (ML), reinforcement learning (RL), blockchain, and generative AI have emerged as transformative tools in building adaptive, intelligent, and automated cloud security frameworks. This paper reviews six recent studies that exemplify this shift toward AI-powered cloud security. The contributions range from ML-based threat detection and blockchain-based identity management to hybrid cloud orchestration and generative AI-driven automation. Together, these approaches highlight the evolution of cloud security from static rule-based models to self-learning, context-aware systems.

2. AI-BASED THREAT DETECTION AND INTRUSION PREVENTION

One of the primary applications of AI in cloud security is real-time intrusion detection. Dhinakaran et al. [1] propose a multi-model architecture using Random Forest (RF), Deep Neural Networks (DNN), and Q-learning to detect and respond to security threats. The DNN model achieved the highest accuracy at 97%, outperforming RF (95%) and Q-learning (88%). Each method provides different benefits: RF offers fast classification, DNN excels at recognizing complex patterns, and Q-learning

enables dynamic policy adjustment based on evolving threat landscapes.

Notably, Q-learning introduces adaptability into intrusion prevention systems by learning optimal security actions from real-time feedback. While Q-learning lags in precision due to a higher false positive rate (5%), it lays the foundation for building autonomous threat response agents. The study concludes that model selection must align with application-specific constraints such as latency, data sensitivity, and interpretability [1].

3. MULTI-CLOUD SECURITY AND AI OPTIMIZATION

Hybrid and multi-cloud architectures are widely adopted to balance agility, redundancy, and compliance. However, securing such complex environments is difficult due to inconsistent policy enforcement and heterogeneous configurations. Srimathi et al. [2] introduce an AI-enhanced security management framework for hybrid clouds using mixed-integer linear programming (MILP), convolutional neural networks (CNNs), and RL agents.

The system intelligently distributes cloud workloads across providers like AWS, Azure, and GCP by analyzing threats, asset sensitivity, and compliance requirements. CNNs detect anomalies in user behavior, and RL dynamically reallocates resources under threat conditions. Experimental results show improved threat response, SLA compliance, and resource utilization in hybrid deployments. The model's AI-driven optimization reduces false positives and supports cross-platform orchestration [2].

4. ENCRYPTION, SIEM, AND FUZZY LOGIC

Gaur et al. [3] explore layered security frameworks using hybrid encryption, Security Information and Event Management (SIEM) systems, and fuzzy logic-based decision engines. The authors propose combining RSA and Elliptic Curve Cryptography (ECC) with SSL to secure data flows in hybrid cloud infrastructures. ECC, with shorter key lengths, demonstrates better computational performance than RSA.

The SIEM systems discussed correlate log data across virtual machines using a centralized Data Identifier Manager (DIM), enabling anomaly detection and dynamic policy enforcement. Meanwhile, fuzzy logic enhances decision-making in SLA-based access control. For instance, IF-THEN rules evaluate service conditions and user roles to grant or deny access. This rule-based intelligence supports real-time response to SLA violations or suspicious activity.

The study highlights that no single mechanism can guarantee comprehensive cloud security. Instead, a combination of encryption, analytics, and intelligent access control offers a more resilient solution [3].

5. Securing Infrastructure as a Service (IaaS)

Charu et al. [4] examine security challenges specific to Infrastructure as a Service (IaaS), including misconfigurations, insider threats, and shared resource vulnerabilities. Using data from industry reports, they observe that over 70% of cloud breaches stem from misconfiguration errors, emphasizing the need for automated compliance and access controls.

The authors propose an IaaS optimization framework integrating IAM systems, encrypted APIs, and anomaly detection using deep learning and hybrid metaheuristic algorithms such as Particle Swarm Optimization–Genetic Algorithm (PSO-GA). The system supports dynamic threat modeling, enabling real-time policy enforcement as workloads change. Moreover, blockchain is used to verify data integrity across virtual machines.

The paper emphasizes layered defense mechanisms and continuous monitoring to adapt to evolving risks. By bridging theoretical architectures with real-world IaaS configurations, the study illustrates how AI can transform reactive security strategies into proactive and scalable defense systems [4].

6. BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY

Centralized security mechanisms often create single points of failure. Rajasekar et al. [5] propose using blockchain-based DLT to decentralize access control and audit logging. Their framework assigns cryptographic keys to users and logs all interactions

on an immutable ledger, ensuring transparency and tamper-proof activity tracking.

The integration of smart contracts automates identity and access management (IAM). For example, conditional access can be granted to third parties during peak workloads and automatically revoked thereafter. Additionally, the system supports encrypted data sharing and federated access across multiple cloud providers.

The framework addresses insider threats, credential theft, and data manipulation by leveraging blockchain's decentralized trust model. Although challenges such as integration complexity and consensus latency remain, the authors suggest that hybrid DLT-cloud models could deliver scalable, secure architectures in sectors like finance, healthcare, and government [5].

7. GENERATIVE AI FOR CLOUD AUTOMATION AND SECURITY

Seth et al. [6] explore the emerging role of generative AI in automating and securing multi-cloud environments. Their framework uses generative models to design optimal infrastructure configurations based on historical data and predictive analytics. These configurations are automatically deployed to respond to changing workloads, traffic patterns, and threat signals.

Generative AI is also employed to evolve firewall policies, API schemas, and encryption settings in real time. For instance, if a spike in traffic is detected from a suspicious IP range, the system can generate new access control policies and reallocate workloads to safer regions or providers.

Case studies from e-commerce platforms showed increased availability, reduced operational costs, and stronger compliance with standards such as GDPR and PCI-DSS. The study highlights the potential of generative AI not just for automation but for predictive and adaptive security in complex cloud ecosystems [6].

8. SYNTHESIS AND DISCUSSION

The reviewed studies illustrate a collective trend toward intelligent, decentralized, and automated cloud security. AI enables enhanced detection accuracy, dynamic threat modeling, and proactive response mechanisms. DNNs, RL agents, and generative models offer context-aware defenses that adapt over time—a significant shift from rule-based systems.

Furthermore, the integration of blockchain and DLT redefines identity and trust models. Smart contracts and immutable logs support secure collaboration across federated cloud environments. Encryption schemes and fuzzy logic engines ensure that access control remains both secure and context-sensitive.

Despite these advances, challenges remain. Issues like explainability of AI decisions, model drift, computational overhead, and cross-provider interoperability must be addressed for widespread adoption. Additionally, combining multiple AI techniques introduces system complexity, requiring robust orchestration frameworks and human oversight.

Future research should focus on privacy-preserving AI, quantum-resistant encryption, and explainable decision-making to ensure ethical, scalable, and compliant security systems.

9. CONCLUSION

As cloud environments become more complex and distributed, traditional security strategies fall short of meeting the demands of real-time threat detection, compliance, and resilience. The reviewed research demonstrates that AI, in its various forms, is central to redefining cloud security architectures.

From machine learning models for anomaly detection [1] to optimization-driven hybrid cloud orchestration [2], fuzzy decision engines [3], and blockchain-based identity frameworks [5], AI-driven approaches offer measurable improvements in speed, accuracy, and adaptability. Generative AI further expands the frontier by enabling predictive and autonomous cloud security configurations [6].

Moving forward, integrating these intelligent techniques into cohesive, explainable, and scalable architectures will be key. By doing so, we can transition from reactive defenses to proactive, intelligent, and trust-enhancing cloud security systems capable of evolving with the threat landscape.

REFERENCES

[1] M. Dhinakaran, M. Sundhari, S. Ambika, V. Balaji and R. T. Rajasekaran, "Advanced Machine Learning Techniques for Enhancing Data Security in Cloud Computing Systems," 2024 IEEE Int. Conf. on Computing, Power and Communication Technologies (IC2PCT), pp. 1598–1602, 2024.

[2] S. J., K. Kanagasabapathi, K. Mahajan, S. Ahamad, E. Soumya, and S. Barthwal, "AI-Enhanced Multi-Cloud Security Management: Ensuring Robust Cybersecurity in Hybrid Cloud Environments," 2023 Int. Conf. on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1–6, 2023.

[3] K. Gaur, M. Diwakar, P. Singh, and N. K. Pandey, "Prevention of Security Attacks in Cloud Computing," 2023 6th Int. Conf. on Information Systems and Computer Networks (ISCON), pp. 1–5, 2023.

[4] Charu, S. Mathur and A. S. Sengar, "Evaluating Current Cloud Security Challenges and IaaS Optimization," 2024 7th Int. Conf. on Contemporary Computing and Informatics (IC3I), pp. 951–956, 2024.

[5] P. Rajasekar, K. Kalaiselvi, R. Shanmugam, S. Tamilselvan and A. P. Pandian, "Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management," 2024 Second Int. Conf. on Advances in Information Technology (ICAIT), pp. 1–6, 2024.

[6] D. K. Seth, K. K. Ratra and A. P. Sundareswaran, "AI and Generative AI-Driven Automation for Multi-Cloud and Hybrid Cloud Architectures," 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), pp. 784–793, 2025.