AI-Driven Automated Threat Hunting for Secure and Scalable Private Clouds - A Review

Dr. Denis R[1, 2], Dr. Basant Kumar[3], Dr.T. Manivannan[4]

[1] Post Doctoral Researcher, Lincoln University College, Selangor, Malaysia

[2]Mount Carmel College, Autonomous, Bengaluru;

[3] Modern College of Business and Science, Muscat, Oman;

[4] St. Joseph's University, Bengaluru, India

pdf.denis@lincoln.edu.my; basant@mcbs.edu.om; manivannan.t@sju.edu.in

Abstract:

The rapid adoption of private cloud environments by enterprises leads to enhanced flexibility, increased regulatory compliance, and increased control of infrastructure. This movement in the security space presents considerable problems for security operation center teams, including a lack of understanding of the meaning of threats, difficulty on the part of operations teams in detecting anomalies in real-time, and challenges in incident handling. The existing manual and rule-based methods employed by security teams are insufficient to address the modern, complex, and rapidly evolving threats initiated by hackers. This paper reviews the literature on AI-configured automated threat hunting frameworks oriented to the specific private cloud environment. Furthermore, it discusses the application of machine learning, deep learning, and reinforcement learning algorithms in constructing adaptive, real-time threat detection and prediction systems embedded in cybersecurity defense techniques. The use of integrating AI algorithms in cloud monitoring systems, Security Information and Event Management (SIEM), and other threat intelligence solutions is discussed to justify the conclusion that scalable architectures and self-healing systems are possible through these architectures. Given the discussion of the many reasons why AI-integrated systems are favored over traditional approaches, although the problems of model explainability, real-time adaptability, and generalizability across different tenant environments will still be present, the implementation of AI capabilities would considerably enhance detection accuracy and the timeliness of response.

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), Automated Threat Hunting, Private Cloud Security, SIEM, Federated Learning, Zero-Trust Architecture.

1. Introduction

The need for secure, compliant, and personalized computing environments is the main driver for companies to embrace the digital transformation of the private cloud. The technology infrastructure provides added control over data and resources, while also creating new types of problems, including access management, anomaly detection, and incident response. Traditional rule-based systems are insufficient for managing cloud operations and mitigating advanced cyber threats, including persistent threats (APTs), polymorphic malware, and insider attacks. Artificial Intelligence (AI) and its sub-elements, including Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL), have proven to be promising technologies for automating and augmenting the detection and response to threats.

The AI automated threat hunting runs on predictive models and pattern recognition to find possible intrusions before they grow into full-fledged attacks. This paper presents a comprehensive literature review of current AI-driven threat hunting techniques in private cloud security, their integration with SIEM and cloud-native tools, and future directions for intelligent, self-learning defense systems.

2. Literature review

A. Traditional Security Approaches

Conventionally, intrusion detection and prevention systems depend on predefined signatures and rule-based mechanisms. While fitting against known attacks, quality system detection of zero-day exploits and novel threat vectors suffers. Mukkamala et al. [1] emphasized that manual rule updates and reactive responses are significant limitations in evolving cloud infrastructures. Furthermore, human-driven systems are prone to fatigue and slow decision-making in high-volume alert environments.

B. Machine Learning in Cloud Security

Machine Learning (ML) has been widely applied to anomaly detection, intrusion prevention, and log analytics. Salo et al. [2] demonstrated that ML models such as Support Vector Machines (SVM) and Random Forests (RF) outperform static security systems in anomaly detection. Buczak and Guven [3] examined ML techniques in cyber defense and found that hybrid approaches improved accuracy over single techniques. Sharma and Gupta [10] implemented hybrid ML techniques for predictive cloud security management that employ adaptive learning and achieve 96% detection accuracy on multi-cloud datasets.

C. Deep Learning-Based Detection Models

Deep learning frameworks, including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders, have shown better feature extraction and classification capabilities. Kim et al. [4] applied CNN models for intrusion detection in private cloud networks. Alrawais et al. [5] implemented an LSTM-based log analysis system capable of real-time anomaly detection. In Kumar et al. [11] conducted a survey noting the dominance of DL-based architectures for detecting insider threats and advanced attacks in cloud systems.

D. Reinforcement Learning and Adaptive Defense

Reinforcement Learning (RL) enables a fluid approach to understanding security responses, with AI agents learning to adapt and respond most effectively, as measured by the rewards they receive. Xu et al. [6] employed RL in addressing resource allocation and attack mitigation problems in dynamic cloud computing environments. Fang et al. [7] studied RL to develop an automated UI-based incident response framework, resulting in shorter times from detection to recovery. These adaptive systems demonstrate that positive outcomes can be achieved through the use of RL in contexts involving continuous learning and decision-making, particularly in light of the ongoing evolution of model cyberattack patterns.

E. Integration with SIEM and Threat Intelligence

Infusing artificial intelligence analytics with Security Information and Event Management (SIEM) offers greater visibility and context for security events. Patel [8] noted that detection rates improved when artificial intelligence modules were integrated into the SIEM pipelines. Thomas and Denis [9] demonstrated that incorporating threat intelligence feeds with machine learning-based anomaly detection reduced the false positive rate. In 2025, Zhang et al. [12] employed a federated integrated AI-SIEM architecture that enables cross-domain learning without sharing sensitive information, thereby enhancing privacy and adaptability.

F. Federated and Edge AI for Cloud Security

Federated learning (FL) and edge AI have become increasingly relevant for decentralized and privacy-preserving model training. Lin et al. [13] introduced a federated intrusion detection framework, which

reduced training latency by 35% and enhanced privacy compliance. Zhao et al. [14] also addressed the problem of secure interaction with cloud tenants on enabled (through blockchain) federated learning. These studies provide insight into the growing trend of distributing intelligence closer to the data source, aiming to minimize risk and latency.

3. Research Gaps and Challenges

AI-driven threat hunting in private cloud environments faces several critical challenges that hinder its effectiveness and widespread adoption. One primary concern is the explainability of AI models. Deep neural networks and other complex learning algorithms often operate as "black boxes", making it difficult for security analysts and stakeholders to interpret their decisions. This lack of transparency not only affects trust in automated systems but also complicates regulatory compliance and accountability. Another significant issue is data privacy and label scarcity. Access to high-quality, labeled cybersecurity datasets is often limited because organizations are reluctant to share sensitive information due to concerns about privacy and proprietary restrictions. This scarcity makes training robust and reliable AI models challenging.

Model generalization also presents a notable problem; AI models trained on one dataset or environment may fail to maintain high performance when deployed across heterogeneous or multi-tenant private cloud infrastructures, where workloads and threat patterns vary significantly. In addition, while many existing frameworks focus primarily on threat detection, they frequently lack real-time responsiveness and autonomous mitigation capabilities, limiting their practical utility in dynamic cloud environments. Finally, resource constraints pose a significant barrier, as AI-based threat detection and mitigation algorithms can be computationally intensive, making their deployment challenging in smaller or resource-limited private clouds. Addressing these challenges is essential for developing secure, scalable, and practical AI-driven threat hunting solutions in modern private cloud infrastructures.

4. Future Research Directions

To address the research gaps discussed above, future research directions on AI synergized threat hunting in private clouds should focus on the following aspects. Federated learning will enhance the collaborative training of models between organizations without requiring the sharing of sensitive, underlying raw data, including personal data, thereby addressing privacy concerns. Deploying edge AI will enable low-latency decisions if lightweight models are allowed to run at the data location (i.e., low detection times with minimal network overhead). Utilizing explainable AI (XAI) techniques, such as SHAP and LIME, will enhance the ability to interpret decisions when using deep learning, thereby increasing trust in the system and facilitating regulatory compliance. AI models that implement techniques from zero-trust security architectures can contribute to continuous identity validation and behavioral control, thereby ensuring adequate protection levels in dynamic cloud environments. Autonomous security orchestration, integrating reinforcement learning and policy-driven management, can also lead to self-defending private cloud infrastructures. Threat intelligence sharing enabled through blockchain can provide a verifiable, decentralized solution for sharing threat intelligence information across private cloud setups, facilitating a collaborative defense solution that does not compromise privacy or security. These techniques can form essential avenues for developing secure, scalable, and intelligent threat detection methods in modern private cloud environments.

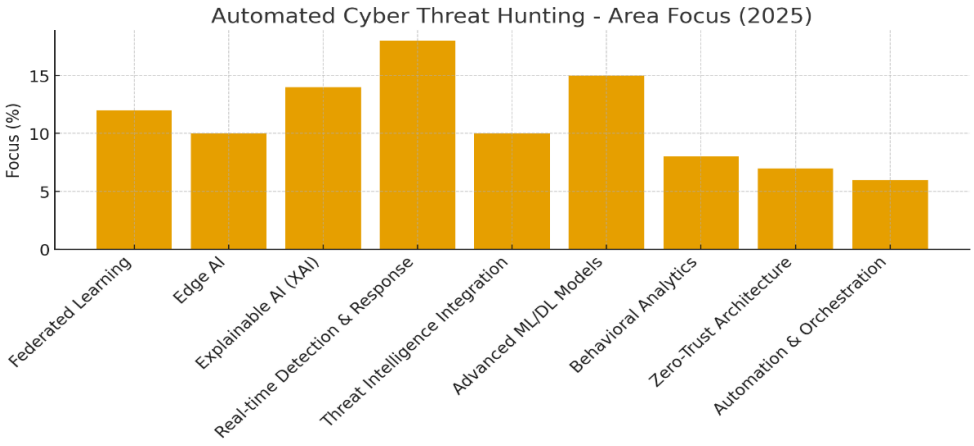

Fig. 1. Automated Threat Hunting- Area of Focus

Figure 1 highlights the projected research priorities, with the most significant emphasis on real-time detection and response (18%), followed by advanced ML/DL models (15%) and explainable AI (14%). Increasing attention is also directed toward federated learning (12%), edge AI (10%), and threat intelligence integration (10%) to enhance privacy, scalability, and contextual awareness. Other emerging areas include behavioral analytics (8%), zero-trust architecture (7%), and automation and orchestration (6%), reflecting a shift toward adaptive and autonomous cloud security frameworks.

5. Conclusion

The rise of AI-assisted autonomous threat hunting heralds a fundamental shift in enhanced preventive and intelligent cloud security. In this way, the detection becomes more accurate, adaptable, and has a greater capacity for real-time responses by the joint use of ML, DL, and RL. Some deficiencies to address include identifiability, data availability, and the versatility of domains, which are fundamental to further development. Emerging technologies, such as federated learning, edge AI, and zero-trust architecture, are pathways to greater innovation and the creation of new products. This communication across diversified domains, with in-depth interdisciplinary work, makes it possible to construct robust, extensible, and trustworthy private clouds.

References

1. S. Mukkamala, G. Janoski, and A. Sung, “Intrusion detection using neural networks and support vector machines,” Proc. IEEE Int. Joint Conf. Neural Networks, vol. 2, pp. 1702–1707, 2002.
2. F. Salo, M. Nassif, and D. Essex, “Anomaly detection in cloud computing using machine learning,” IEEE Access, vol. 7, pp. 110–128, 2019.
3. A. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2016.
4. Y. Kim, J. Kim, and H. Kim, "CNN-based intrusion detection for private cloud systems," Computers & Security, vol. 102, pp. 102–118, 2021.
5. A. Alrawais, A. Alhothaily, and X. Cheng, “Leveraging LSTM networks for real-time anomaly detection in cloud logs,” IEEE Trans. Cloud Comput., 2022.
6. J. Xu, L. Liu, and J. Jiang, “Reinforcement learning for automated security defense in cloud environments,” IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 1123–1136, 2022.
7. W. Fang, X. Li, and Y. Zhao, “Adaptive incident response using reinforcement learning,” Future Generation Computer Systems, vol. 128, pp. 190–202, 2022.

8. D. Patel, “AI-driven SIEM for enhanced cloud threat detection,” Proc. IEEE Int. Conf. Cloud Eng., pp. 88–95, 2023.
9. S. Thomas and R. Denis, “Integrating threat intelligence and ML for proactive private cloud security,” Int. J. Comput. Netw. Secur., vol. 12, no. 4, pp. 57–65, 2024.
10. R. Sharma and M. Gupta, “Hybrid machine learning models for predictive cloud security management,” J. Cloud Comput., vol. 13, no. 2, pp. 220–232, 2024.
11. V. Kumar, L. Singh, and R. Patel, “Deep learning trends in cloud intrusion detection: A comprehensive survey,” Applied Intelligence, vol. 54, pp. 4550–4572, 2024.
12. Z. Zhang, H. Lee, and P. Cho, “Federated AI-SIEM architecture for privacy-preserving multi-domain threat detection,” IEEE Access, vol. 13, pp. 22590–22604, 2025.
13. X. Lin, Y. Wang, and L. Zhao, “Federated learning-based intrusion detection for privacy-preserving clouds,” Appl. Sci., vol. 15, no. 12, p. 6878, 2025.
14. Q. Zhao, J. Ren, and M. Han, “Blockchain-enabled group federated learning for cloud-edge security,” J. Cloud Comput., vol. 13, no. 3, pp. 55–70, 2024.
15. A. Singh and S. Bhatia, “Beyond encryption: Multidimensional data protection using AI and ML in cloud computing,” Int. J. Comput. Appl., vol. 185, no. 28, pp. 41–48, 2023.