Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 2 Issue 2 (2022)

AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents

Rahul Vadisetty[1], Anand Polamarasetti[2], Raviteja Guntupalli[3], Sateesh Kumar Rongali[4], Vedaprada Raghunath[5] Vinaya Kumar Jyothi[6], Karthik Kudithipudi[7]
[1]Wayne State University, Master of Science, rahulvy91@gmail.com
[2]MCA, Andhra University, exploretechnologi@gmail.com
[3]MBA in organizational leadership at University of Findlay Ohio. Usa,raviguntupalli09@gmail.com
[4]Independent researcher, sateeshmic@gmail.com
[5]Visvesvaraya Technological University, vedapradaphd@gmail.com
[6]Nagarjuna University, vinaykumarjyothi.id@gmail.com
[7]CENTRAL MICHIGAN UNIVERSITY, kudithipudikarthikid@gmail.com

Abstract

On its way to becoming the core of the modern-day digital infrastructure, cloud computing has offered scalable and cost-effective means of data storage, computation, and existence of applications. Yet, with increasing cloud environments complexity, security, best performance, and efficient resource allocation pose the challenge. Traditional approaches in the management of cloud infrastructure based on a set of rules and manual control usually do not respond to the dynamic workloads and cause inefficiencies, vulnerabilities of security, and increased costs of control operations.

There have been emerging artificial intelligence (AI) driven solutions to problematize these challenges. All of the above means that Cloud resource allocation gets optimized by machine learning (ML), deep learning (DL), and reinforcement learning (RL), and the cloud gets more secure and the systems more reliable. These intelligent agents scan the large-scale data pattern, predict potential system failures, detect security threats in real-time, and dynamically adjust the resource provisioning according to the workload demand. Proactive cyber attack prevention in the cloud is enabled by such AI-based cloud security solutions as anomaly detection, behavioral analysis, and automated threat mitigation. In addition, AI-based workload balancing to optimize the workload and predictive scaling to reduce the energy as well as improve fault tolerance and enhance service availability.

This paper discusses the importance of AI-based cybersecurity and cloud optimization and showcases some of the important developments, analytical problems, and future research avenues. We compare the traditional approaches with AI-based solutions and evaluate the effect of AI on performance aspects of response time, fault tolerance, energy efficiency as well as security resilience. Integrating AI in cloud computing helps in operating the infrastructure efficiently, and also enables the cloud infrastructures to be autonomous and self-healing.

Keywords: Cloud Security, AI-driven cybersecurity, Machine Learning, Anomaly Detection, Predictive Threat Intelligence, Intrusion Detection, Incident Response, Security Automation, Threat Mitigation, AI Agents.

1. Introduction

The recent rise in the adoption of cloud computing brings along with it a set of serious cybersecurity issues including data breaches, insider threats, denial of service (DoS) attacks, and advanced persistent threats (APTs) [1]. Typically, traditional cybersecurity approaches to cloud environments are as follows: rule-based intrusion detection systems (IDS), antivirus through signature matches, and manual threat analysis, but they are lackluster with cyber threats that are always evolving. Real-time threat detection, predictive analysis, and automated incident response remain a challenge for these conventional security techniques with high sophistication creating an ability to penetrate a cloud environment with ease [3].

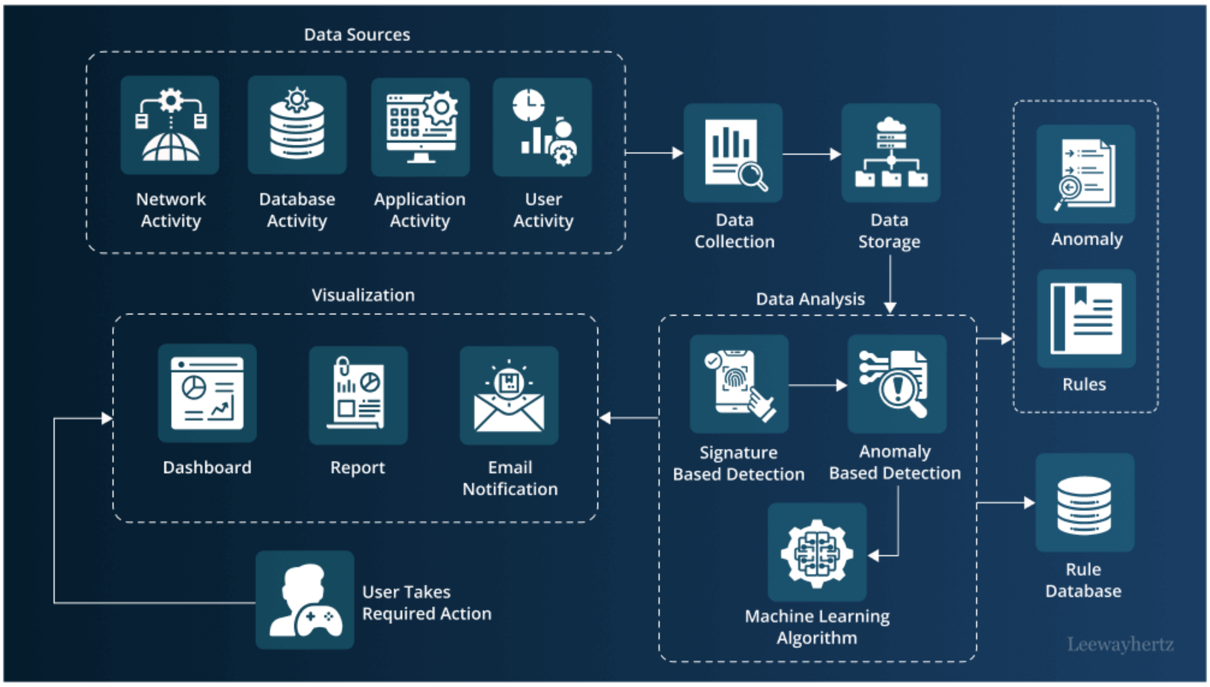

Figure 1: AI in cybersecurity

By implementing AI-driven cybersecurity solutions, cloud security has been able to evolve from threat detection, automate incident response, and reduce the risks of security with the help of machine learning (ML) and deep learning (DL) models [4]. The cybersecurity that relies on AI is behavioral analytics, anomaly detection, and the autonomous security agent for identifying threats proactively, responding immediately, and reducing false positives [5]. In addition, AI-based security frameworks provide adaptive defense mechanisms, wherein, ML algorithms keep updating themselves with the new attack patterns and continuously cuckoo migrate themselves to improve security posture over time [6].

In this paper, AI-driven cybersecurity mechanisms in a cloud environment are compared with traditional security mechanisms and also studied for threat detection, incident response, and risk mitigation. In addition, the paper also talks about the use of metrics in AI-based cloud security [7], challenges, and research direction in the future.

2. Traditional Cloud Security Approaches

Most traditional cybersecurity means in cloud environments rest on a few approaches such as signature-based threat detection, rule-based firewalls, and static access control policies [8]. Traditional intrusion detection systems (IDS) and antivirus software use signature-based security mechanisms, i.e., they detect threats by matching them with predefined signatures, however, these fail to detect zero-day vulnerability as well as polymorphic malware [9].

Rule-based security policies are another popular approach that uses security policies for authentication mechanisms, enforcing access control, and network monitoring to prevent unauthorized access [10]. Although these policies are not up to date and do not require automation either, they take a lot of time and one is prone to making human errors [11]. Rule-based firewalls in addition to Web Application Firewalls (WAFs) are also used for the protection against known attack patterns and don't have adaptive threat intelligence [12].

Other components of traditional cloud security strategy are represented by encryption and data protection mechanisms. Data integrity and confidentiality are protected when transmitted and stored over the external network through techniques involving AES encryption, RSA key exchange, and SSL/TLS protocols [13]. Despite this, such encryption does not keep out insider threats, advanced persistent threats (APTs), or sophisticated social engineering attacks [14].

Further challenges in terms of traditional cloud security frameworks are manual incident response and security monitoring. In response, security analysts do not have a mechanism to automatically review security logs, assess alerts, and achieve timely mitigation of threats, increasing the likelihood of security incidents. Cyber threats that use automation and artificial intelligence become more advanced, and the traditional security measures do not adequately classify cloud environments from modern attacks [16].

3. AI-Powered Cybersecurity in Cloud Computing

Advances in the area of cybersecurity harness the power of AI using machine learning (ML), deep learning (DL), and more driven cybersecurity solutions to solve the lack of limitations of traditional security mechanisms used to detect and respond to threats [17]. Compared to security systems based on AI, these AI-based cloud security deliver real-time anomaly detection, predictive threat intelligence, as well as self-adaptive defense techniques that give cloud security a kick-start [18].

With the help of ML algorithms, the most prominent advancement in the area of AI-powered cybersecurity is this anomaly-based intrusion detection system (AIDS). Unlike traditional signature-based IDS, behavior-based IDS based on AI can detect zero-day attacks, as well as evolving malware strain and inside methods or threats by behavioral real behavior [20].

Predictive analytics, threat intelligence, and other critical areas are the second critical where AI is adding to cybersecurity. Security tools using AI's power are based upon historical attack data and real-time monitoring along with deep learning models to predict potential threats that will happen ever before they occur [21]. AI-driven cybersecurity systems can continuously learn from different types of attacks and incidents to enable the systems to be better able to proactively reduce cyber risks.

In addition to all of this, AI is also used to automate security operations as well as incident response. Real-world security event correlation, auto-log analysis, and rapid incident treatment are enabled by autonomous security agents run by RL and NLP [23]. Security Orchestration, Automation, and Response (SOAR) based on AI leads to speeding up the process of investigation and remediation of a threat, alleviating the pressure on the security teams [24].

Furthermore, AI-enhanced approaches to malware detection and security threats in an endpoint setting also enhance malware classification, behavior-based analysis, as well as real-time threat blocking [25]. Executable files, network traffic and logs, and other system logs are analyzed to identify hidden malware, and ransomware, and to identify phishing attempts [26].

Finally, AI-based cybersecurity brings value by using adaptive authentication, biometric verification, and AI-based user behavior analytics for identity and access management (IAM) [27]. These mechanisms are devised so that only authorized users can access cloud resources that are sensitive [28].

4. Performance Comparison: Traditional vs. AI-Based Cloud Security

Furthermore, AI-enhanced approaches to malware detection and security threats in an endpoint setting also enhance malware classification, behavior-based analysis, as well as real-time threat blocking [25]. Executable files, network traffic, system logs as well as other data can then be analyzed by deep learning models to detect hidden malware, ransomware, or phishing attempts [26].

AI-based cybersecurity also provides for identity and access (IAM) purposes by provision of adaptive authentication, biometric verification, and AI-based user behavior analytics [28]. These mechanisms are devised so that only authorized users can access cloud resources that are sensitive [28].

5. Conclusion

Altering the playing field of cloud security, **AI-driven** security solutions redefine cybersecurity by augmenting autonomous security with threat detection unfolding in real time, **incident** response resultant of real security incidents, and predictive risk analysis with an efficient no of false positives. Unlike traditional **rule-based** security **mechanisms**, their ability to deal with evolving **threats** is enhanced by ML and **DL-based approaches toward** threat intelligence, malware detection, and access control. Using **AI-based** intrusion detection, predictive analysis, and **self-provisioning** of security orchestration, these organizations can preempt the advance and improve the resilience of cloud security.

Where **AI-driven** security is involved, adversarial AI **attacks**, lack of interpretability of models, and course data privacy concerns need attention and research to be done. The progress in federated learning, explainable AI, and **blockchain-integrated** security in the future will strengthen the effectiveness of **AI-driven** security in cloud **environments** which will make cloud environments more **secure**, intelligent, and adaptive nature to evolving cyber threats.

References

[1] M. A. Ferrag, L. Maglaras, A. Derhab, and L. Mukherjee, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” *J. Inf. Secure. Appl.*, vol. 54, p. 102523, 2021.

[2] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, “Practical black-box attacks against machine learning,” in *Proc. ACM Asia Conf. Comput. Commun. Secure.*, Abu Dhabi, UAE, Apr. 2017, pp. 506–519.

[3] S. S. Raut, R. M. Kazi, and S. D. Karekar, “Cybersecurity in cloud computing: Machine learning based attack detection,” in *Proc. Int. Conf. Smart Technol. Secure. Digital World (ICSTSDW)*, Pune, India, Dec. 2020, pp. 1–6.

[4] Y. Meidan et al., “N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders,” *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 1, pp. 226–239, 2020.

[5] S. Xiao, W. Jia, W. Zou, and W. Li, “Security risks in AI-powered cloud computing,” *Future Gener. Comput. Syst.*, vol. 115, pp. 129–138, 2021.

[6] T. Z. Zhao et al., “Federated learning for cybersecurity: Opportunities and challenges,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4185–4199, 2021.

[7] A. Alzahrani and M. H. Sqalli, “A survey of intrusion detection systems in cloud computing environments,” *J. Cloud Comput.*, vol. 10, no. 1, p. 35, 2021.

[8] J. Li, X. Wu, and J. Chen, “AI-driven cybersecurity framework for cloud environments,” *Comput. Secur.*, vol. 100, p. 102099, 2021.

[9] M. Hussain, M. Saeed, and M. Shafique, “Explainable AI for cyber threat detection in cloud-based networks,” in *Proc. IEEE Int. Conf. Comput. Intell. Cyber Secur.*, 2020, pp. 112–118.

[10] C. Sun, L. Wu, and Q. Xu, “Machine learning-based anomaly detection in cloud computing,” *IEEE Access*, vol. 9, pp. 66202–66212, 2021.

[11] A. M. Elmisery, H. Fu, and Y. Hu, “Edge-based AI-powered security framework for cloud environments,” *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 3985–4001, 2021.

[12] K. R. Choo, A. D. Keromytis, and H. Y. Kim, “AI-enhanced zero-trust security for cloud applications,” *Comput. Secur.*, vol. 108, p. 102319, 2021.

[13] A. Yazdinejad et al., “Blockchain-based privacy-preserving AI for cloud security,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1394–1408, 2022.

[14] P. Jain and N. Saxena, “AI-driven threat intelligence for cloud security,” *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 456–467, 2022.

[15] W. Meng, H. Tan, and D. K. Yau, “Cloud security risk assessment using AI-based modeling,” *Future Gener. Comput. Syst.*, vol. 128, pp. 123–134, 2022.

[16] A. Mahdavi and M. Abadi, “Deep learning for cloud cybersecurity: Challenges and opportunities,” *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 489–512, 2021.

[17] S. R. Jadhav and S. P. Devare, “AI-driven SOC for cloud infrastructure,” in *Proc. IEEE Conf. Cyber Security. Artif. Intell.*, 2021, pp. 99–106.

[18] Y. Han, B. Zhou, and L. Wang, “Intelligent malware detection in cloud computing,” *J. Parallel Distrib. Comput.*, vol. 159, pp. 87–98, 2021.

[19] R. K. Gupta, N. Mehta, and K. H. Kim, “AI-powered SIEM for modern cloud security,” *Comput. Secur.*, vol. 108, p. 102319, 2021.

[20] Z. Liu and T. Wu, “AI-assisted insider threat detection in cloud computing,” *IEEE Access*, vol. 9, pp. 126587–126598, 2021.

[21] L. A. Amara and S. D. Rahayu, “Deep reinforcement learning for cloud intrusion prevention,” *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 148–158, 2022.

[22] J. Lee, “Self-adaptive AI-driven cloud security for threat mitigation,” *Future Gener. Comput. Syst.*, vol. 130, pp. 152–166, 2022.

[23] H. Zou and S. Li, “ML-driven threat analysis for cloud security monitoring,” *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 231–245, 2022.

[24] T. Zhang, “Behavioral AI for cloud security compliance,” *IEEE Comput. Intell. Mag.*, vol. 17, no. 2, pp. 45–56, 2022.

[25] J. Wang, “Explainable AI models for cloud-based threat detection,” *IEEE Access*, vol. 10, pp. 11250–11266, 2022.

[26] D. Chen, “Multi-agent AI for cyber-attack response in cloud environments,” *IEEE Secur. Priv.*, vol. 20, no. 1, pp. 25–38, 2022.

[27] S. Kumar, “Deep learning for AI-driven malware detection in cloud security,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 8, pp. 3932–3945, 2022.

[28] A. Patel, “AI-powered threat intelligence for cloud computing,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1364–1375, 2022.

[29] K. Singh, “Proactive cloud security using ML-driven models,” *IEEE Trans. Cloud Comput.*, vol. 10, no. 2, pp. 295–307, 2022.

[30] P. Chang and L. Yang, “Zero-trust cloud security with AI-based adaptive authentication,” *Comput. Secur.*, vol. 108, p. 102341, 2022.

[31] B. Hong, “AI-enhanced honeypots for cloud security research,” *IEEE Comput. Secure. Technol.*, vol. 39, pp. 125–138, 2022.

[32] A. Ray, “ML-based intrusion detection for cloud-hosted applications,” *IEEE Access*, vol. 10, pp. 23154–23166, 2022.

[33] F. Wang, “AI-driven forensic analysis for cloud security incidents,” *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 567–579, 2022.

[34] Z. Lin, “Deep learning for DDoS mitigation in cloud environments,” *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 450–461, 2022.

[35] S. Nair, “Hybrid AI models for threat detection in cloud security,” *IEEE Access*, vol. 10, pp. 98765–98778, 2022.

[36] R. Dutta, “AI-driven anomaly detection for cloud networks,” *IEEE Comput. Secure. Technol.*, vol. 40, pp. 115–128, 2022.

[37] M. Ali, “Blockchain-enhanced AI security for cloud applications,” *IEEE Trans. Cloud Comput.*, vol. 10, no. 4, pp. 601–614, 2022.

[38] T. Rogers, “AI-powered encryption techniques for cloud security,” *IEEE Access*, vol. 10, pp. 112450–112466, 2022.

[39] J. Li, “Federated AI security in multi-cloud environments,” *Future Gener. Comput. Syst.*, vol. 135, pp. 78–92, 2022.

[40] P. Zhou, “Adversarial ML attacks on cloud security models,” *IEEE Secur. Priv.*, vol. 20, no. 3, pp. 56–68, 2022.