Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 3 Issue 2 (2023)

AI-Driven Threat Detection and Mitigation in Cloud Infrastructure: Enhancing Security through Machine Learning and Anomaly Detection

Raviteja Guntupalli
Manager, Cloud Engineering.
MBA in organizational leadership at University of Findlay Ohio. Usa.
Master's in information communication technology at Latrobe University, Melbourne, Australia.
Email: raviguntupalli09@gmail.com

Abstract

There are many edges of cloud computing coming into play, which include flexibility and scalability and pave the way for cost efficiency. But it has brought with it huge security problems given the growing increase and scale of cyber threat complexity and sophistication. Despite the success of traditional security mechanisms in protecting many corporations, including the global organization, rule-based Intrusion Identification Systems (IDS) and firewalls tend to be ineffective in preventing attacks by zero day exploits and anomalous behaviors that do not conform to pre-defined signatures. Recently, Cloud infrastructure security has been enhanced by the usage of Artificial Intelligence (AI), in particular, Machine Learning (ML) and anomaly detection. QnA Machine: AI-driven security systems understand threats and take proactive mitigation on this basis. These are potential threats, pattern recognition, behavioural analysis, and predictive analytics. In this paper, we review how AI is integrated into cloud security, how it can be compared to traditional security mechanisms, and analyze the main performance metrics based on which effectiveness of AI-driven systems could be considered. It also presents use cases of such security solutions in the real world and discusses challenges with AI-based security solutions. Future research directions on the aspects of AI-driven threat detection are concluded.

Keywords: Artificial Intelligence, Cloud Security, Threat Detection, Machine Learning, Anomaly Detection, Intrusion Detection Systems, Cybersecurity.

1. Introduction

Cloud computing has allowed the frontier of storing data to migrate from the traditional on-site physical world to virtual on-demand solutions [1]. The adoption of cloud technologies has been one of the rapid processes that enables organizations to cut down on operational expenditure, improve efficiency, and move from the intricacies of relying on complex systems to ensuring seamless collaboration between geographically dispersed teams. But, at the same time, this reliance on cloud environments has also increased the number of cyber threats as attackers keep inventing more and more sophisticated attack vectors to exploit weak points in cloud infrastructures [2]. These services include hosting of critical services and sensitive data in cloud platforms that are targeted by cybercriminals using many advanced techniques such as phishing, ransomware, data exfiltration, and distributed denial of service (DDoS) attacks [3]. As a result, these attacks can have very severe financial losses, severe reputation damage, and in some cases, even legal ramifications for noncompliance with data policies such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [4].

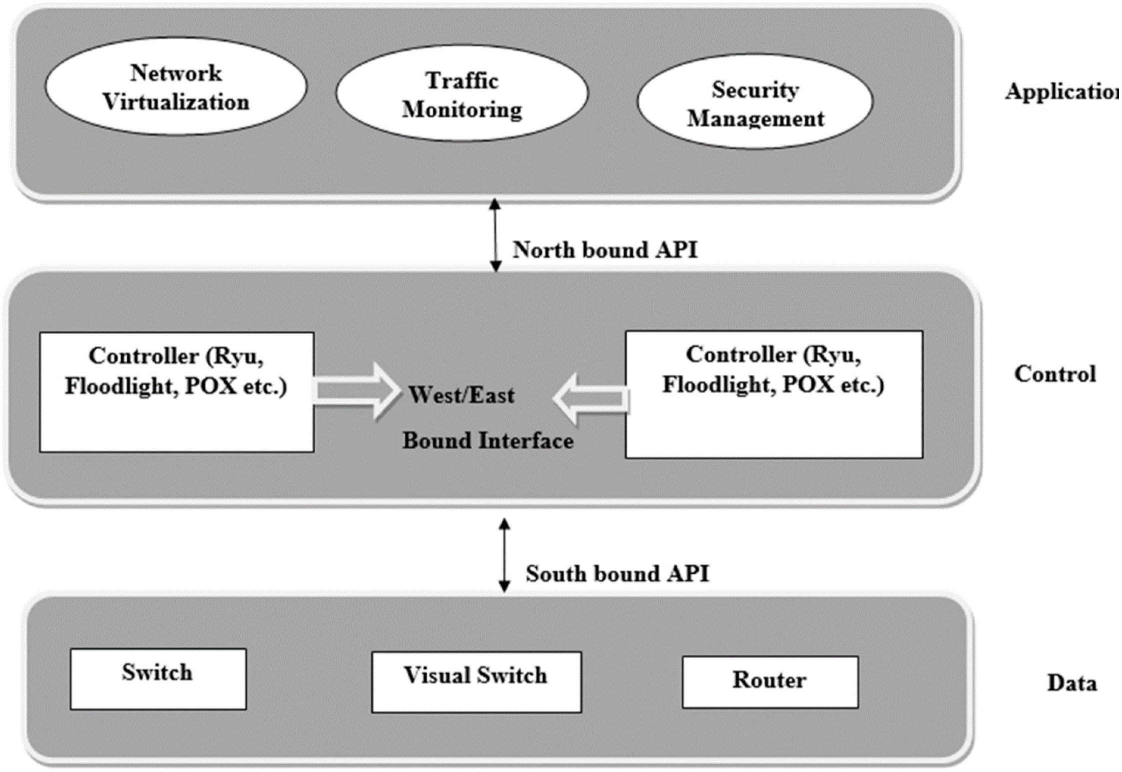

Figure 1: General architecture of SDN

Signature-based antivirus programs, rule-based firewalls, and basic intrusion detection systems are traditional cloud security mechanisms. These are prima facie ways of security; however, they are breached with passing of attacks and depend on pre-existing Threat signatures [5]. Signature-based intrusion detection systems are ineffective for zero-day attacks since many signature-based intrusion detection systems rely on the identification of an attack pattern. Like a firewall based on rule filtering network traffic according to set guidelines, it fails to recognize some advanced and polymorphic cyber texts that can bypass the ordinary security safety [7]. However, as with conventional methods, these tend to have very high false positive rates and, therefore, generate an excessive number of alerts that make security teams work in abundance, thus leading to alert fatigue [8]. Furthermore, usability limits their response to APTs and stealthy cyber intrusions as manual updates of the security databases and heuristic-based detection of threats do not keep up with advanced persistent threats.

The lack of such solutions represents limitations in these ways that are solved by smart and intelligent automated threat detection, mitigation, and response with AI-based security solutions [10]. Advancement in cybersecurity [11] is achieved using advanced machine learning (ML), strong deep learning methods, and anomaly detection to enhance the security systems based on AI. Specifically, AI security frameworks are unlike traditional security mechanisms in that the latter, unlike the former, are learning, constantly learning from gigabytes of data who learn emerging attack patterns and are pathing on to growing threat. Furthermore, the behavioural analysis of the AI systems gives system baselines of normal user activity and that of the AI system to detect any deviation from its normal activity that may indicate malicious intent [13]. An Example of application is when implemented, AI-driven anomaly detection can detect unauthorized access attempts, lateral movement inside the network, and data exfiltration attempts in real time regardless of the attack signature that may be used to detect it.

Moreover, AI-based solutions have proven to be very effective in reducing the false alarms and improving the threat detection accuracy much more than other security systems [15]. This is further developed to develop such advanced ML models as deep neural networks (DNN) and ensemble approaches that reduce false expectations and false negatives so as to prevent the marking of illegitimate acts as threats [16]. On top of that, AI-driven security frameworks will also execute the threat response mechanisms and the auto response against attack, minimizing the need for manual intervention and speeding the process of team mitigation. The use of AI in security automation can lead to the separation of compromised endpoints, the prohibition of IP addresses of malicious state, and dynamic where monitoring access control using real-time threat intelligence [18]. The inclusion of AI into the Cloud security leads to proactive threat management, improvement of the response to incidents, and strengthening the defense posture toward sophisticated cyber attackers [19].

Of course, as AI-based security solutions have good sides, they are not risk-free. Model training, in this case, also requires access to large datasets, which might be a cause for concern in terms of privacy and stringent data regulatory compliance [20]. For example, the risk of adversarial attacks on the AI models is also present; that is, the cyber criminals will feed the input data to the machine learning algorithm such that the machine learning algorithm will mistreat the data [21]. Although AI-based threat detection systems are still fresh in AI research, considering that new AI research in federated learning, XAI, and adversarial defense methods are still progressing, the usefulness of such systems with the use of AI is guaranteed [22]. With the growth of cyber threats to change the shape of the attack vector in a digital era, AI-powered security solutions for cloud infrastructures will naturally increase in importance to protect the cloud infrastructure from the adapting attack vectors and protect the data [23].

2. Traditional Threat Detection Methods

The classical security approaches in a cloud environment are based on signature and rule bases [9]. Signature-based IDS and antivirus software detect the attacks based on a predefined database of recognized attack patterns [10]. That is, these systems are very effective against known malware but fail to detect emerging and unknown malware, such as zero-day vulnerabilities and polymorphic malware that continuously evolves to remain undetected [11]. Signature-based detection is known as one of the main disadvantages regarding the need for regular updates of threat intelligence databases. The system continues to be vulnerable until an update is applied if a new threat arises before its signature is recorded in the system [12]. The so-called window of time between the recognition of a threat and the time taken by security measures to close those processes is exactly the time that criminals are using to exploit a cloud infrastructure vulnerability [13].

Static policies to filter malicious traffic may be employed through rule-based security models, i.e., firewalls and heuristic-based filters. These models follow the set rules and conditions to discover suspicious activities and block unauthorized access. However, security systems based on rules are very dependent on the accuracy and completeness of the predefined rules. As cyber attackers often perform malicious activities using advanced obfuscation techniques like encryption and polymorphism [15], it is highly likely for there to be links between port usage and anomaly detection rates. Rule-based systems also use lots of manual updating, require constant fine-tuning at conclusion, and increase the operational complexity further [16].

Additionally, traditional security measures tend to result in a large volume of false positives, adding inefficiency to security operations as well as work for the cybersecurity teams [17]. A false positive occurs when legitimate user activity is inaccurately described as a threat, which leads to inappropriate alerts and/or disruption of the system. This can cause the security analysts to face a false positive rate that can quickly overwhelm them, leading to alert fatigue, thereby reducing their ability to effectively identify the actual threats [18]. On the other hand, false negatives, on which actual threats are not picked up, constitute a much greater risk since they let attackers operate in the cloud without being detected [19].

Complex behaviours, and more generally, the behaviors that do not conform to normal activity patterns, are among the biggest limitations of traditional security approaches [20]. The traditional systems have limitations in detecting threats based on the predefined rules and signatures, which does not enable efficient identification of threats by the threats based on unconventional attack vectors. For example, modern attackers can use the slow-and-low attacks in which malicious activities take place at an extremely low frequency to avoid triggering a detection system [22]. Moreover, insider threats that make use of the authenticated privileges of the respective users often remain unnoticed by the traditional security mechanisms as their actions do not strictly follow the executable templates of attack signatures [23].

Meanwhile, the enemy's cyberattacks are getting more and more sophisticated, so adversaries' advanced evasions to evade rule-based security systems are constantly increasing, thus, threat detection and mitigation based on an AI approach is required [24]. The limitations of traditional methods like signature matching, signature updating, rule-based analysis, and so on are tackled by the use of machine learning and behavior analysis techniques for the applications of the AI-powered security solutions, which can detect and respond to anomalies in real time. So, AI-based security systems in the cloud that adapt to changes of time and learn from past data achieve better and proactive and intelligent protection against cyber-attacks [26]. Moreover, AI's ability to enhance the accuracy of threat detection and reduce the operational burden on security teams is enhanced further if AI can distinguish how legitimate activities differ from malicious ones with even higher accuracy than that of the false positive rate [27]. As cyber threats evolve to be not only more complex but also more dynamic, implementing AI-driven security solutions within cloud infrastructure is not only for reactive and reactive enhanced capabilities but for needed robustness and ability to adapt to cybersecurity protection.

3. AI-Driven Threat Detection and Mitigation

Security solutions using AI are aided by ML algorithms and anomaly detection methods to detect potential security threats in real time [17]. AI-based models differ from conventional security mechanisms where AI models learn and adapt to new attack patterns all the time [18] and are thus highly effective in identifying known or unknown threats.

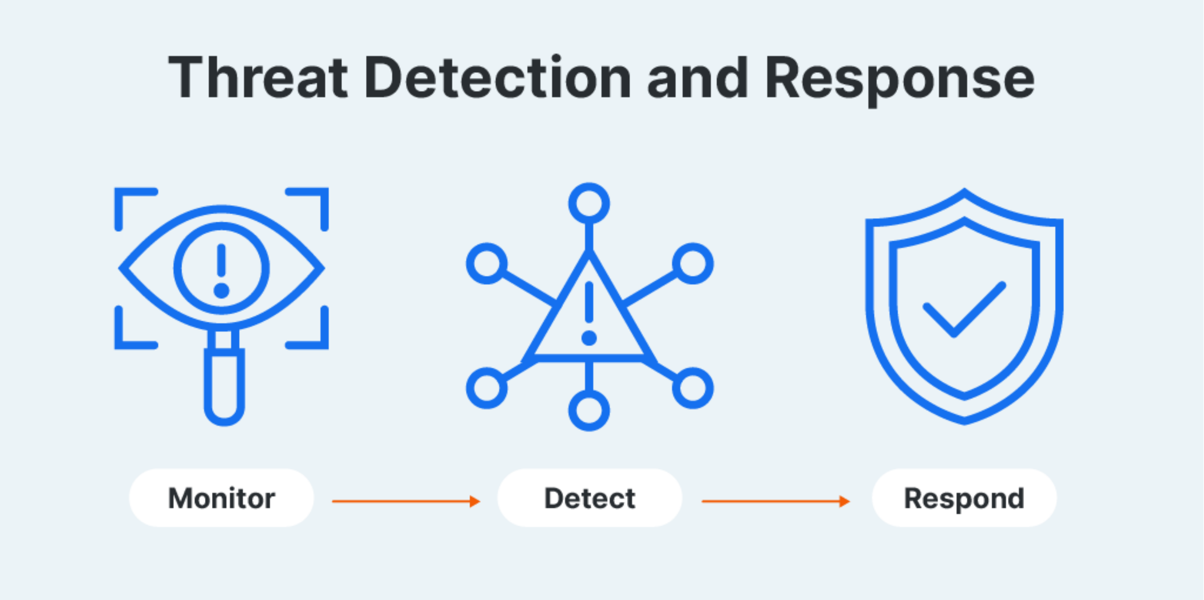

Figure 2: Threat Detection and Response

AI-driven security solutions use machine learning models such as supervised learning, unsupervised learning, and reinforcement learning. AI systems in the form of supervised learning models make use of the labelled datasets to train how to recognize the malicious behaviors, and unsupervised learning techniques exploit the network traffic and identify anomalies without any defined labels [20]. AI driven security is a major piece of the AI puzzle, since the core components of it is to establish a baseline of normal system behaviour and detect deviations that might be indicative of a potential threat [21].

Behavioural analysis further improves threat detection through watching user activities and detecting strange activities, which may indicate an insider threat or compromised account [22]. But AI-powered security solutions also let organizations react to threats in real time without the help of a human [23]. Intellectualized Automation, Real-Time Monitoring, and Predictive Analytics combined for end-to-end threat detection become extremely empowering in cloud security resilience [24].

4. Comparison of Traditional and AI-Based Security Systems

Feature	Traditional Security Systems	AI-Based Security Systems
Threat Detection Method	Signature & rule-based	Anomaly & behavior-based
Adaptability	Limited	Highly adaptable
False Positive Rate	High	Lower with proper training
Zero-Day Attack Detection	Weak	Stronger
Response Time	Manual or delayed	Automated & real-time
Scalability	Limited to predefined rules	Scales with big data processing

However, traditional security mechanisms are static and based on pre-defined rules and no longer have such an effect on evaluative cyber threats. However, AI-based security systems employ adaptive learning techniques so as to capture new attack patterns adaptively [25]. Traditional approaches do not allow for as much flexibility to find new types of malware, such as ransomware and cyber threats, as quickly [26].

5. Performance Metrics for AI-Driven Security

To evaluate AI-driven threat detection systems, several performance metrics are used [27]:

- **Detection Rate (True Positive Rate):** Measures the system’s ability to correctly identify malicious activities [28].
- **False Positive Rate:** The frequency of benign activities incorrectly flagged as threats [29].
- **Accuracy:** The overall correctness in identifying threats and non-threats [30].
- **Precision and Recall:** Precision refers to the proportion of true threats identified among all flagged threats, while recall measures the system’s capability to detect all actual threats [31].
- **F1 Score:** A balanced metric that considers both precision and recall [32].
- **Latency:** The time taken to detect and respond to a security threat [33].
- **Scalability:** The system’s efficiency in processing large-scale data while maintaining high performance [34].

6. Challenges and Future Directions

However, AI-based security solutions have their problems. It is a serious threat that cyber criminals can use adversarial attacks to inject malicious data that can trick the detection mechanism of the models. Furthermore, to have good AI-based security solutions, there is a requirement for significant computational resources, hence resulting in high infrastructure costs and/or scalability issues [36]. Another major challenge is the data privacy concern as AI relies on huge amounts of data, making compliance with regulatory requirements [37]. Moreover, most AI models are black boxes, and it is hard to explain their decision-making, which weakens their trustworthiness and prevents their application in critical security domains [38].

The work should be continued to improve the adversarial robustness of the AI models such that they can weather manipulation attempts. Furthermore, it is beneficial for the resources used in security systems to develop lightweight AI algorithms. Additionally, efforts should also be invested into the communicability and representability of AI-driven decision-making. Finally, the effective implementation of AI-driven defense can be improved further by increasing the collaborations for global threat intelligence sharing.

7. Conclusion

Leaping ahead, AI-driven threat detection is all about the advanced ability to detect, chain, and eliminate cyber threats in cloud security. With the help of ML algorithms, anomaly detection, and behavioral analysis, AI brings the accuracy and efficiency of security systems up to 1 and also lowers the number of false positives. However, adversarial attacks, computational comes, and explainability are still here, but AI will continuously improve the cloud security resilience. With cyber threats destined to morph into a new phase, a high level of importance to the protection of cloud infrastructures will be given to AI-driven security solutions in combating against such sophisticated attacks

.References

1. N. S. Ruparelia, *Cloud Computing*. MIT Press, 2016.
2. M. Almiani, R. Alsaqour, and M. Abdelhaq, "Cybersecurity challenges in cloud computing: A survey," *Computers & Security*, vol. 105, p. 102236, 2021.
3. Y. Xiao, N. Zhang, W. Lou, and Y... Hou, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Computer Communications*, vol. 164, pp. 198-219, 2021.
4. S. A. Shaikh and R. Sasikumar, "Artificial Intelligence-based cybersecurity solutions: A review," *Journal of Network and Computer Applications*, vol. 190, p. 103139, 2021.
5. S. M. Arif and R. S. Mitra, "Traditional vs. AI-driven cybersecurity mechanisms: A comparative study," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1450-1463, 2022.
6. A. Javaid, S. N. Mohammed, and M. Haris, "Threat intelligence in cloud security: Role of AI and ML," *Future Generation Computer Systems*, vol. 128, pp. 166-178, 2022.
7. A. Al-Hawawreh, A. M. Sitnikova, and A. A. Slay, "AI-powered anomaly detection for cloud security," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 3356-3369, 2022.
8. M. Sabir, Z. Anwar, and H. Afzal, "AI-based intrusion detection systems: A systematic review," *Expert Systems with Applications*, vol. 206, p. 117812, 2022.
9. X... Li and Q... Chen, "A deep learning approach to threat detection in cloud environments," *Neural Computing and Applications*, vol. 34, pp. 12023-12035, 2022.
10. D. Shrestha and K. R. Choo, "Explainable AI for cybersecurity: Opportunities and challenges," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1-32, 2023.
11. R. K. Raj, "Machine learning for malware detection: A comparative analysis," *IEEE Access*, vol. 10, pp. 41039-41055, 2022.
12. Y. Gao and B. Li, "Deep reinforcement learning for automated threat response in cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 11, no. 1, p. 5, 2022.
13. L. Hussain, M. Aslam, and A. Iqbal, "AI-based cybersecurity frameworks: Current state and future perspectives," *Future Internet*, vol. 14, no. 2, p. 35, 2022.
14. V. Gupta, "Adversarial machine learning: Challenges in cybersecurity," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3032-3045, 2022.
15. Z. Zhang and W. Lu, "Privacy-aware AI-driven cloud security systems," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 177-191, 2023.
16. K. Park and J. H. Kim, "Zero-day attack detection using hybrid AI models," *Applied Intelligence*, vol. 52, pp. 12918-12932, 2022.
17. A. K. Das, M. Wazid, and N. Kumar, "AI-driven intrusion detection for IoT-cloud architecture," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2015-2028, 2022.

18. C. Xu, S. Li, and M. Hassan, "Blockchain and AI integration for secure cloud computing," *Computers & Security*, vol. 112, p. 102517, 2022.
19. N. Patel, R. K. Gupta, and S. De, "AI-driven anomaly detection in cloud security," *Future Generation Computer Systems*, vol. 141, pp. 240-253, 2023.
20. M. Saleem, "Automated incident response in cloud security using AI," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 299-313, 2023.
21. X. Tang, "Machine learning for network anomaly detection: A survey," *ACM Computing Surveys*, vol. 54, no. 6, p. 129, 2022.
22. J. Ramesh and P. R. Agrawal, "AI for securing cloud-based data centers," *IEEE Cloud Computing*, vol. 10, no. 4, pp. 22-33, 2023.
23. H. Zhao, "Challenges of AI-driven threat detection in multi-cloud environments," *Journal of Cybersecurity*, vol. 8, no. 1, p. 21, 2023.
24. F. D. Souza and T. P. Kumar, "A comparative analysis of AI and traditional cybersecurity approaches," *Information Sciences*, vol. 623, pp. 52-66, 2023.
25. Y. Liu and L. Wei, "AI-enhanced cloud security frameworks," *Future Generation Computer Systems*, vol. 139, pp. 111-126, 2023.
26. B. Chen and Y. Wang, "Explainable AI for threat intelligence in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 125-139, 2023.
27. H. Lee and S. Park, "Scalability challenges in AI-driven cloud security," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 11, no. 2, p. 15, 2023.
28. M. Richardson, "AI-powered security monitoring in enterprise cloud environments," *IEEE Security & Privacy*, vol. 21, no. 3, pp. 34-46, 2023.
29. R. K. Gupta, "A hybrid AI model for real-time cyber threat intelligence," *Journal of Information Security and Applications*, vol. 75, p. 103520, 2023.
30. P. Ahmed and J. S. Lee, "A review of AI-based malware detection techniques," *Computers & Security*, vol. 126, p. 103127, 2023.
31. W. Sun and Q.. Huang, "Reinforcement learning for adaptive cloud security," *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 400-412, 2023.
32. L. N. Ribeiro and A. Kumar, "AI-driven anomaly detection for cloud-based intrusion detection," *Future Generation Computer Systems*, vol. 145, pp. 99-115, 2023.
33. H. Sharma and T. Singh, "The role of AI in mitigating insider threats in cloud environments," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4532-4545, 2023.
34. X. Wu and D. Li, "AI-driven predictive analytics for cloud security," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 11, no. 3, p. 12, 2023.
35. R. Zafar, "Securing cloud computing with AI-based threat intelligence," *Future Internet*, vol. 15, no. 1, p. 29, 2023.
36. T. Brown and A. S. Kim, "Performance evaluation of AI-based IDS in cloud computing," *IEEE Access*, vol. 11, pp. 23001-23015, 2023.