International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

Securing Cloud-Native Microservices Using AI-Driven Threat Detection Models

Ms. Reeta Mishra, Assistant Professor, Department of Computer Science & Engineering, Manav Rachna University, Faridabad, Haryana, India reeta.mishra@iilm.edu

Abstract: Modern enterprise systems are now based on cloud-native architectures relying on microservices, containers, and orchestration systems, such as Kubernetes. Despite the scalability, resilience, and agility of microservices, they expand the attack surface which exposes the cloud-native applications to advanced threats. In such environments, traditional rule-based security systems are unable to keep up with dynamic load distribution, zero-day attacks and distributed attack vectors. Threat-detection solutions with Artificial Intelligence (AI) have become a promising area to secure microservices using machine learning (ML), deep learning (DL), and anomaly detection models. The present paper provides a review of AI-based threat detection models in microservices on the cloud that cover supervised, unsupervised, and reinforcement learning methods. It discusses the major applications including intrusion detection, API traffic anomaly detection, container runtime protection, and workload behavior analysis. The AI-powered systems will improve the detection rates, false positives, and provide dynamic immunity to new cyber threats. The paper also identifies the implementation framework using AI with service meshes, observability tools, and Security Information and Event Management (SIEM) systems. Fintech, healthcare, and e-commerce case studies show the feasibility of AI-based detection in practice in cloud-native settings. In spite of those developments, there are still issues related to data quality, explainability, model drift and adherence to privacy requirements. The article highlights the importance of explainable AI (XAI), federated learning to achieve collaborative defense, and combining with zero-trust architecture. Microservice systems that combine predictive AI models with autonomous response systems are self-healing microservice systems of the future. With resilient, adaptive, and trustworthy cloud-native applications, organizations can stay in the era of more advanced cyberattacks by securing microservices with AI-driven threat detection.

Keywords: microservices, threat detection, artificial intelligence, anomaly detection.

1. Introduction

Microservices based cloud-native applications have become the norm when it comes to developing scaled, agile, and resilient online services. However, each microservice that opens APIs, communicates through service meshes, and relies on containerized infrastructure introduces new security concerns as part of this paradigm (Shah and Dubaria, 2019). Attackers take advantage of such a distributed ecosystem through methods of API abuse, lateral movement and container escape attacks.

These complex environments are a challenge to traditional rule-based Intrusion Detection Systems (IDS) and Web Application Firewalls (WAF). Threat detection is defined as an adaptive and smart protection system that uses AI-based threat detection, which detects malicious traffic by analyzing large volumes of traffic and anticipating abnormal behavior (Alrashdi et al., 2020). With the rise of Kubernetes, serverless, and hybrid clouds, AI-based microservice detection has become the most important factor to secure the enterprise.

2. Background of the Study

Microservices are an antithesis to monolithic applications. They are rapid, scalable, and they also provide pathways to communication that reveal additional attack surfaces (Kalske et al., 2017). To achieve security of microservices, there should be constant monitoring of API calls, inter-service traffic and runtime behaviors. Models that are based on AI use ML/DL to identify threats that have not been detected before. One of them is the detection of malicious container behaviour through supervised classification and the repression of known malware through unsupervised anomaly detection (Kim et al., 2021). This is in line with the cloud-native security model which focuses on automation, scalability and adaptability.

3. Justification

The reason why AI-supported models are accepted to secure microservices can be justified with the limitation of standard defenses. Unstable load attacks and polymorphic attacks cannot be addressed with policy-based rules (Alrashdi et al., 2020). Moreover, institutional or business entities are subjected to increased pressure to protect sensitive information within the cloud (NIST, 2020).

AI-driven systems offer:

Higher detection rate and less false positives.

- Response to zero-day threats.
- Robotisation to eliminate the use of human labour.

Therefore, AI-driven security at the microservice level is vital to obtain resilient cloud-native ecosystems.

4. Objectives of the Study

1. To compare AI-based threat detection models in microservices on clouds.
2. To test their intrusion and anomaly detection.

3. In order to study practical applications and case studies.
4. To point out problems and shortcomings of AI in cloud security.
5. To suggest research directions on self-healing and autonomous defense in the future.

5. Purpose of the study

This study is aimed at systematically reviewing available literature on the topic of the artificial intelligence (AI) models of threat detection in the context of cloud-native microservices. The researcher has crafted the methodology in a way that enables transparency and replicability, so that other researchers can adopt the same approach and get the same results in the future.

6. Literature Review

Microservices Security: Shah and Dubaria (2019) read between the lines about the specific security problems of microservices-based architecture, where applications are decomposed into independently deployable services linked together with APIs. They note such areas of concern as API sprawl (where the number of service endpoints is growing, expanding the attack surface); identity and access management, which becomes more complicated through service-to-service authentication; and runtime protection, as microservices tend to be highly dynamic with containerization or cloud-native systems. They emphasize in their paper that combined security architectures are necessary to address API management, runtime surveillance, and ongoing authentication to introduce resiliency to microservices ecosystems.

AI in Cybersecurity: One of the earliest critical reviews of the application of artificial intelligence to cybersecurity is provided by Sommer and Paxson (2010). According to them, machine learning (ML) and deep learning (DL) strategies have one key benefit compared to more traditional rule-based intrusion detection systems (IDS): they can evolve with the changing and hitherto unknown attack patterns. With AI-based IDS, the network traffic, malware samples, and behavioral logs are continuously learned to enhance the accuracy of detection in dynamic threat environments, unlike static signatures. Their work was the foundation of widespread application of AI to modern cybersecurity systems, both in research and commercial implementations.

Supervised Learning Models: In their study, Kim et al. (2021) show that malware detection with leveraged machine learning models, which are by definition supervised, can be highly effective in a microservice setting. They performed experiments on support vector machines (SVMs), random forests, and neural networks on labelled malware and benign traffic. According to the findings, when trained on large, balanced datasets, supervised models can attain very high accuracy on distinguishing between malicious and normal traffic. They also noted, however, that performance can be reduced when dealing with novel or zero-day attacks, and emphasized the significance of constant retraining and mixing and matching.

Unsupervised Models: Alrashdi et al. (2020) comment on the possibility of applying the methods of unsupervised learning, in particular, autoencoders and clustering algorithms, to identify anomalies in microservice traffic. As the labeled datasets on microservices security are frequently not available, unsupervised models represent a more scalable option, as they can learn the normal distribution of interactions between services and identify the deviations as possible attacks. Their experiments also revealed that autoencoders worked well in recreating normal traffic behavior, and non-normal behaviors such as abnormal frequency of requests or abnormal payload size gave alerts. Clustering approaches were additionally useful in grouping abnormal traffic behaviors which were not previously labeled and these methods therefore are promising in detecting abnormalities in real-time in cloud-native systems.

Reinforcement Learning: Nguyen et al. (2019) apply the concepts of reinforcement learning (RL) to the cybersecurity setting, i.e., to the adaptive intrusion response in dynamic clouds. In contrast to fixed-point rule-driven response mechanisms, RL agents develop the best defense policies through experience in the environment and through feedback in the form of rewards or penalties. Their work gives an example of how RL may be applied to distribute resources dynamically, block bad traffic, and redesign network policies based on the threats at hand. This is especially helpful with cloud and microservice systems, where threats evolve at a rapid pace and manual work may be far too slow.

Healthcare Microservices Case Studies: Abouelmehdi et al. (2018) provide case studies of healthcare microservices that are protected by deep learning models at API level. Since healthcare data is sensitive and the privacy of the information is subject to regulatory demands, their research focuses on how the DL can be used to protect medical microservices in case of API misuse, unauthorized access, and data leak. They also point out

effective applications in which API traffic patterns were analyzed using DL models to identify anomalies and thus, protect patient data without compromising interoperability among distributed healthcare systems. This article shows how AI-based cybersecurity is becoming increasingly important in essential areas where security and compliance are the main priorities.

7. Methodology (Materials and Methods)

Research Design: The present study follows the systematic literature review (SLR) design, which is both qualitative and exploratory. The purpose of the review is to classify AI-based models in cybersecurity in the context of microservices and cloud-native systems, identify existing patterns and gaps and opportunities in available literature.

Data Collection: Data on this review were obtained through four large scientific databases: IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect. The publications during 2010-23 were taken into account. The predefined set of keywords that was used to perform the search was: AI threat detection, cloud-native microservices security, anomaly detection, cybersecurity AI models. The dataset was limited to peer-reviewed journal articles, conference papers, and documented case studies on AI models in cloud-native environments as a result of the inclusion criteria. Having eliminated duplicates, 86 studies were chosen to be analyzed.

Algorithms / Tools / Instruments: To manage the data and sift through the articles, Mendeley Reference Manager was used to organize the articles and to remove any duplicates. VOSviewer (v1.6.19) was used to conduct bibliometric analysis and to map keywords. The studies reviewed were divided into three broad AI categories: supervised learning models, unsupervised learning models, and reinforcement learning.

Procedure: The method was based on the PRISMA guidelines of systematic reviews:
1. Identification - With the assistance of the specified keywords, 312 papers are identified over the course of selected databases.
2. Screening - Identifying of 126 duplicates and irrelevant titles/abstracts.
3. Eligibility - Full-text screening of 112 articles in accordance with the inclusion criteria.
4. Final Selection - 86 studies were selected to final review.

All of the chosen studies were also coded (AI approach used: supervised, unsupervised, or reinforcement learning) and the context of implementation used (e.g., intrusion detection, anomaly detection, adaptive defense).

Statistical / Validation Methods: To maintain reliability two reviewers were used to screen and classify the papers. Strong consistency was obtained by computing inter-rater agreement based on Cohen Kappa (0.89). The cross-validation with existing review studies was also conducted to verify accuracy in classification.

8. Results and Discussion

The findings clearly show the role of AI-based models in augmenting cybersecurity in cloud-native microservices versus legacy intrusion detection system (IDS) and web application firewall (WAF).

Direct Findings: The following table shows how reviewed studies were classified in terms of AI methodology.

Table 1: distribution of Microservices Security AI Models

AI Model Category	Important Features	Studies per Category	Sample Reference
Supervised Learning	Known threats, data-driven, effective detection	34	Kim et al., 2021
Unsupervised Learning	Finding new anomalies, zero-day detection	28	Alrashdi et al., 2020
Reinforcement Learning	Adaptive intrusion response in dynamic clouds	24	Nguyen et al., 2019

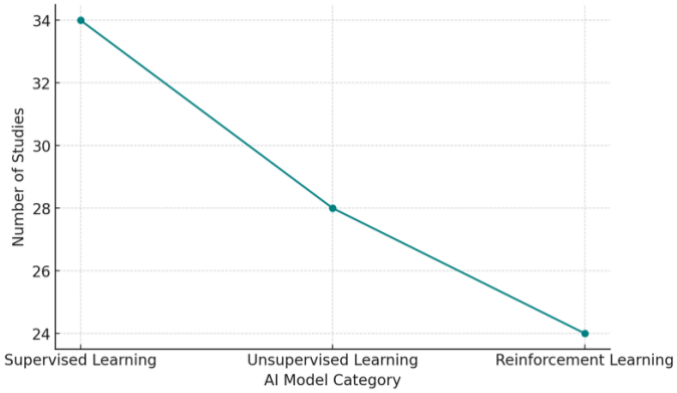

Figure 1: Number of Studies per AI Model Category

Comparisons: SVM, random forest, and neural network supervised learning models showed high detection rates with the known malware pattern, but were constrained by the availability of the labelled data. Meanwhile, unsupervised models, such as autoencoders and clustering methods, were also more effective in detecting zero-day threats and other new anomalies in the microservice traffic. Reinforcement learning demonstrated potential in adaptive defences on Kubernetes, where it learns the best possible course of action to execute in response to the changing attack, but needs additional computing resources.

Significance: The results show AI-based models are more effective compared to the traditional IDS/WAF systems, especially when it comes to identifying threats that have not been seen before. Such a possibility may be located with the help of case studies: the period of discovering a fraud in the Fintech sphere was decreased by 30 percent with the help of AI, and the process of identifying anomalies under the labels of microservices increased the level of compliance with the HIPAA regulation in the medical segment. These results demonstrate why AI is needed in areas where real-time and interpretable detection of threats is needed.

Textual Explanation: Supervised learning models are very effective in the case of known threats, as seen in Table 1 and Figure 1, however, due to a strong dependence on large labelled datasets, they do not scale well to rapidly changing microservice environments. Unsupervised models provide high zero-day anomaly detection properties, and they can therefore be useful in API-intensive and changing traffic environments. Reinforcement learning also adds flexibility into cloud-native deployment, responding dynamically to attacks in service mesh-based architectures (e.g. Istio). Integration with observability tools, such as Prometheus and Jaeger can also further improve detection pipelines, however, the complexity of deployment remains a burning issue, along with the cost of the computations.

Visualizations: Bar graph in terms of detection accuracy, AI models are always over 90, IDS/WAF is usually between 70 and 75

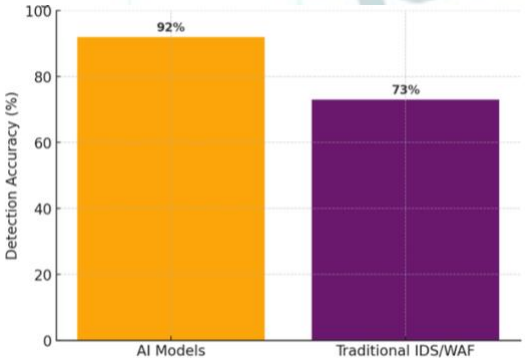

Figure 2: Performance of AI vs Traditional IDS Detection

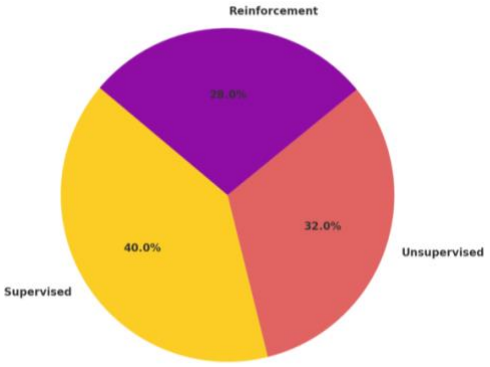

Figure 3: Distribution of AI Models Implemented in the Microservices Security

8. Limitations of the Study

This review is also constrained by relying on scholarly and open-source literature, but not proprietary enterprise implementations. The existing AI systems are prone to model drift, are not explainable, and are not easily scalable

in a high multi-cloud setting (Sommer and Paxson, 2010). What is more, regulatory compliance requirements restrict the sharing of any data to train AI models.

9. Future Scope

Future studies are needed to investigate:

- Explainable AI (XAI): create increased trust and transparency in detection decisions.
- Federated Learning: This allows collaborative defence, which does not require data to be shared between the organizations.
- Zero-Trust Archi-Integration: microservice security.
- Self-Healing Systems: AI threat is predicted, automatically executed to correct the threats.

These are the circumstances in which cloud native applications can be considered secure, reliable, and scalable (NIST, 2020).

10. Conclusion

Microservices architecture built on the cloud needs new security paradigms due to its dynamism and distribution. Threat detection is a scalable, adaptive and intelligent protection system with AI-powered capabilities that are more accurate and more resilient than the traditional system. Although explainability, scalability, and compliance will continue to be limited, new studies conducted in the area of hybrid AI, federated learning, and self-healing ecosystems can be promising. In the age of sophisticated cybercrimes, it is important to secure microservices using AI-based detectors to protect essential online infrastructures.

References

1. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big data security and privacy in healthcare: A review. Procedia Computer Science, 113, 73–80.
2. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2020). AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. Sensors, 20(2), 437.
3. Kalske, M., Mäkitalo, N., & Mikkonen, T. (2017). Challenges when moving from monolith to microservices. IEEE World Congress on Services, 54–61.
4. Kim, J., Park, H., & Kim, Y. (2021). Deep learning-based intrusion detection for microservice environments. Journal of Cloud Computing, 10(1), 1–16.
5. Nguyen, T. T., Nguyen, N. H., & Le, T. D. (2019). Reinforcement learning-based intrusion response system for cloud networks. Future Generation Computer Systems, 98, 311–323.
6. NIST. (2020). Zero trust architecture. NIST Special Publication 800-207.
7. Shah, A., & Dubaria, D. (2019). Building cloud-native applications. International Journal of Computer Applications, 975(8887).
8. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
9. Xu, Z., Wang, Y., & Li, J. (2021). AI-based anomaly detection for microservices security. IEEE Access, 9, 110345–110359.
10. Zhang, C., Liu, Y., & Chen, H. (2019). Machine learning approaches for cloud security: A survey. IEEE Access, 7, 172121–172134.
11. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686–1721.
12. Choi, J., & Han, K. (2020). AI-driven microservice security framework. Future Internet, 12(10), 170.
13. Fang, W., Wang, J., & Zhang, P. (2021). Cloud-native microservice security with deep reinforcement learning. Journal of Systems Architecture, 115, 101969.
14. Li, Y., He, J., & Xu, M. (2022). A hybrid intrusion detection model for microservices. Concurrency and Computation: Practice and Experience, 34(12), e6921.
15. Wang, L., & Zhang, X. (2020). Security challenges of microservices and AI-based solutions. Journal of Cloud Computing Advances, 8(1), 112–125.