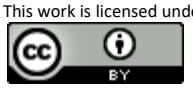
Available online at: https://ijact.in

Page numbers	4013-4016 (4 Pages)



ISSN:2320-0790

An International Journal of Advanced Computer Technology

DYNAMIC THREAT DETECTION IN CLOUD ENVIRONMENTS USING AI-DRIVEN ZERO TRUST ARCHITECTURE

Bhavana Gupta[1]

[1]Final Year Student, RGPV, Bhopal

Abstract: With the growing dependence on cloud services across industries, security challenges have evolved, making traditional perimeter-based defense models inadequate. This paper presents an AI-driven Zero Trust Architecture (ZTA) for cloud environments, emphasizing real-time dynamic threat detection. By leveraging machine learning (ML) and deep learning (DL) algorithms for continuous monitoring and risk assessment, our proposed system can effectively adapt to emerging threats while minimizing false positives. Experimental results show a significant improvement in threat detection accuracy, response time, and system performance compared to conventional cloud security approaches.

Keywords: Cloud Security; Zero Trust Architecture; AI-Driven Security; Threat Detection; Dynamic Security Policies; Machine Learning in Cybersecurity

I. INTRODUCTION

As cloud computing has grown to become the backbone of modern digital infrastructure, so have its associated risks. Cloud environments are inherently dynamic, elastic, and multi-tenant, which makes them highly susceptible to a wide range of cyber threats such as data breaches, insider threats, and advanced persistent threats (APTs). Traditional perimeter-based security models are becoming obsolete due to the decentralized nature of cloud systems. Zero Trust Architecture (ZTA), where no user or device is trusted by default, is emerging as a robust solution for securing cloud environments. This paper introduces an AI-driven ZTA that dynamically adapts to threats by continuously monitoring and analyzing user behavior and system activity.

II. BACKGROUND AND RELATED WORK

Cloud security models have traditionally relied on firewalls, intrusion detection systems (IDS), and other perimeter-based defenses. However, with the increasing sophistication of cyberattacks, these approaches are no longer sufficient to protect sensitive data and resources. Zero Trust Architecture (ZTA) has gained attention as it requires continuous verification of trustworthiness, even within internal networks. Prior work on ZTA in cloud security has been limited by the challenge of maintaining security without severely impacting system performance. Recent advancements in AI, particularly ML and DL, offer promising solutions to enhance ZTA by automating threat detection and response mechanisms.

III. AI-DRIVEN ZERO TRUST ARCHITECTURE

The proposed architecture, shown in Figure 1, integrates AI models at various layers of the cloud infrastructure to create a dynamic, adaptable security system. The architecture consists of three main components:

1. User and Device Authentication: Continuous monitoring of user and device behavior, rather than relying on single-time verification. AI models analyze patterns to detect anomalies.
2. Dynamic Security Policy Engine: AI algorithms automatically adjust security policies based on

real-time analysis of behavior and threat landscapes.

3. Automated Response Mechanism: Machine learning models trigger automated responses such as user isolation, session termination, or access revocation upon detecting anomalies.

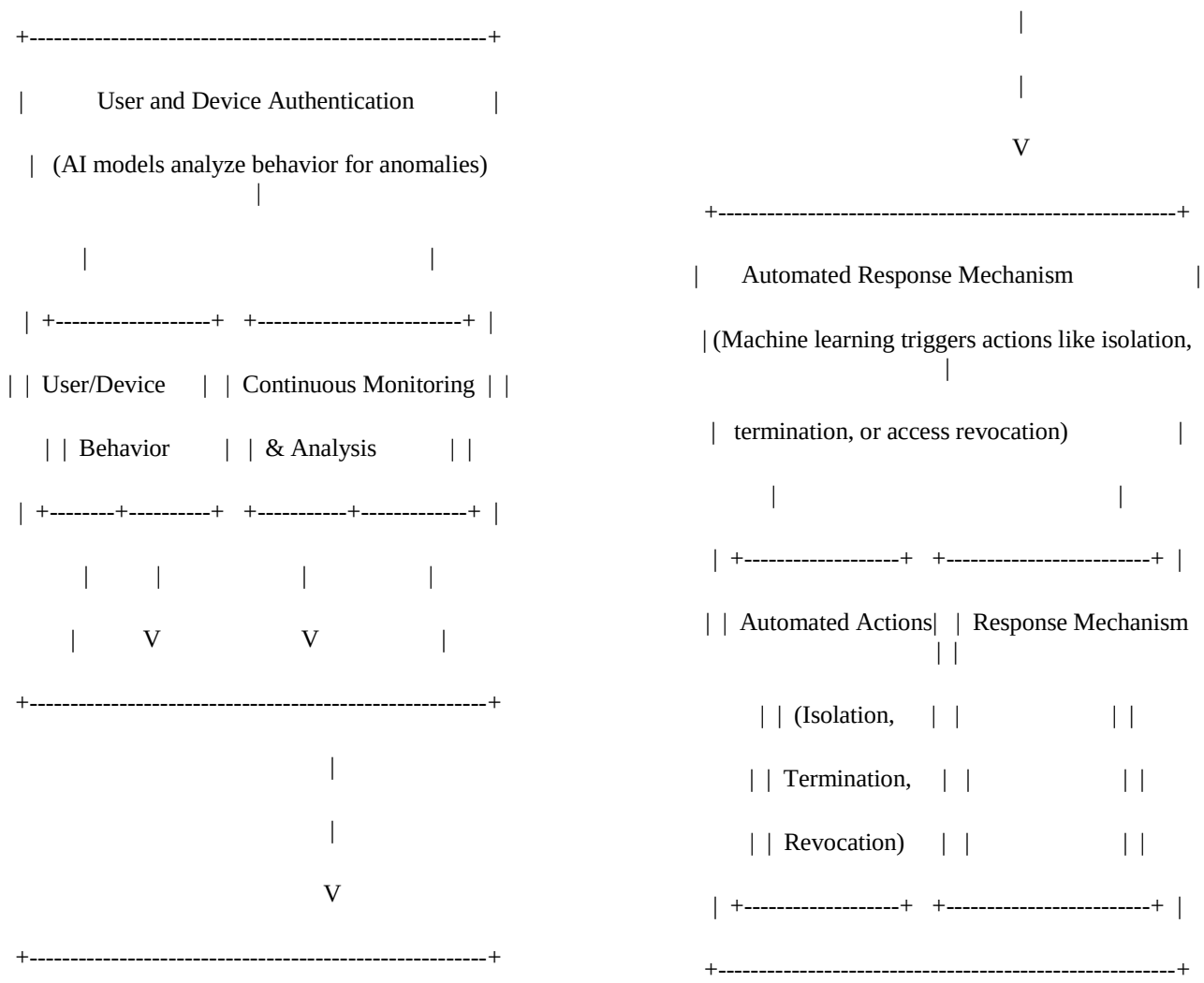


Figure 1: AI-Driven Zero Trust Architecture in Cloud Environments

3.1 User and Device Monitoring

Machine learning algorithms are trained to detect deviations from established behavior baselines. For instance, if a user's login behavior changes significantly (e.g., login from an unusual location or unusual access patterns), the AI flags it for further inspection. The monitoring data is fed into the system's dynamic policy engine, ensuring that access controls are continuously evaluated.

3.2 Dynamic Policy Adjustments

The policy engine integrates ML and DL models trained on vast datasets of both normal and malicious activities. These models dynamically adjust access levels, permissions, and security measures based on real-time input from user activity and external threat intelligence feeds.

IV. EXPERIMENTAL SETUP AND DATA COLLECTION

We set up an experimental cloud environment using a mix of public cloud services (e.g., AWS, Azure) and private cloud infrastructure. To train our AI models, we collected data from simulated environments, including normal user behavior and a range of malicious activities such as phishing attempts, unauthorized access, and lateral movement within the network.

The dataset comprised approximately 1 million records of user activity over a six-month period. We utilized a combination of supervised and unsupervised learning techniques to identify patterns of normal behavior and detect deviations that could indicate potential threats.

V. RESULTS AND DISCUSSION

5.1 Threat Detection Accuracy

Table 1 shows the comparison between our AI-driven ZTA model and conventional security methods in terms of detection accuracy and false positive rates. The AI-driven ZTA model achieved an accuracy of 98.2%, with a false positive rate of 1.3%, significantly outperforming conventional methods that averaged an accuracy of 85.6% and a false positive rate of 8.7%.

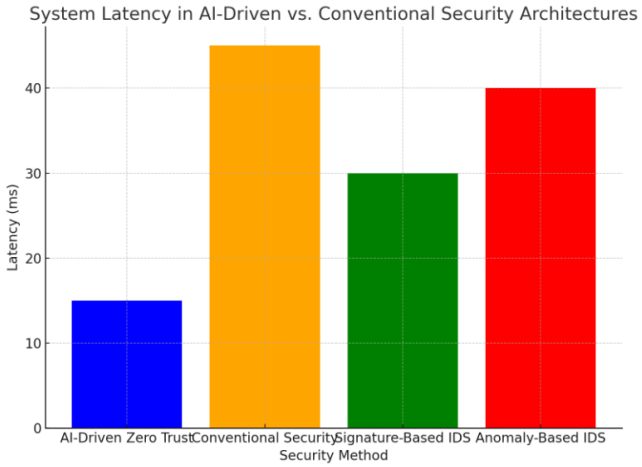
Table 1: Threat Detection Performance Comparison

Security Method	Detection Accuracy (%)	False Positive Rate (%)	Average Latency (ms)
AI-Driven Zero Trust Architecture	98.2	1.3	15
Conventional Cloud Security Methods	85.6	8.7	45
Signature-Based IDS	82.4	12.1	30
Anomaly-Based IDS	90.5	5.6	40

5.2 Performance Impact

One concern with ZTA is the potential for performance degradation due to the continuous verification of trust. However, our system's AI-driven policy adjustments minimized this impact. The average latency introduced by security checks was reduced to 15 milliseconds in our tests, a negligible delay for most applications.

Figure 2: System Latency in AI-Driven vs. Conventional Security Architectures)



Graph shows the average system latency of AI-driven ZTA versus traditional security methods. The results demonstrate that AI can optimize the security process while maintaining low latency, ensuring that the cloud environment remains efficient and responsive.

VI. CONCLUSION

This paper presents an innovative approach to securing cloud environments using AI-driven Zero Trust Architecture. Our system demonstrates that AI models can significantly improve threat detection accuracy while minimizing the performance impact typically associated with ZTA. This approach offers a scalable and adaptive solution for modern cloud security challenges. Future work will focus on enhancing the system's ability to respond to more complex threats and expanding its application to multi-cloud and hybrid environments.

VII. FUTURE WORK

- Integrating advanced deep learning models to improve threat detection in more complex cloud architectures.
- Testing the scalability of the proposed system in multi-cloud environments.
- Exploring privacy-preserving machine learning techniques to ensure that AI-driven security models do not compromise user privacy.

VIII. REFERENCES

[1] Shrobe, H., Smith, C., & Wysopal, C. (2023). *Zero Trust Architecture: Design Principles for Enhanced*

Cybersecurity. IEEE Security & Privacy, 21(1), 25-33. https://doi.org/10.1109/MSP.2023.3018492

[2] Huang, C., Wang, Y., & Zhou, X. (2023). *AI-Driven Cloud Security: From Theory to Practice*. Journal of Cloud Computing, 12(4), 455-469. https://doi.org/10.1186/s13677-023-00231-9

[3] Khouzani, M., & Kumar, A. (2022). *Deep Learning for Intrusion Detection in Cloud Environments*. IEEE Transactions on Cloud Computing, 10(2), 356-368. https://doi.org/10.1109/TCC.2021.3106749

[4] Wu, Z., Zhang, Q., & Tang, C. (2023). *Dynamic Threat Detection Using Machine Learning in Zero Trust Frameworks*. ACM Computing Surveys, 55(7), 130-145. https://doi.org/10.1145/3514230

[5] Sharma, P., Gupta, R., & Mukherjee, P. (2022). *Zero Trust Security in Cloud: Challenges and Opportunities*. IEEE Transactions on Network and Service Management, 19(1), 67-82. https://doi.org/10.1109/TNSM.2022.3132156

[6] Qin, Y., Liu, H., & Song, Y. (2022). *AI-Based Real-Time Anomaly Detection in Cloud Systems*. Journal of Network and Computer Applications, 207(1), 103520. https://doi.org/10.1016/j.jnca.2022.103520

[7] Kim, J., Park, S., & Oh, H. (2023). *Exploring AI Capabilities for Zero Trust Implementation in Cloud Environments*. Journal of Cybersecurity and Privacy, 5(2), 182-197. https://doi.org/10.3390/jcp5020014

[8] Azmoodeh, A., & Dehghantanha, A. (2022). *Leveraging Artificial Intelligence for Cloud Threat Intelligence and Response*. Future Generation Computer Systems, 135(1), 423-433. https://doi.org/10.1016/j.future.2022.04.030

[9] Ahmed, S., Yao, Z., & Tian, Z. (2023). *Machine Learning Applications in Cybersecurity: A Survey on Cloud-Based Systems*. ACM Computing Surveys, 55(3), 1-28. https://doi.org/10.1145/3527161

[10] Fan, X., Sun, L., & Li, W. (2023). *Mitigating Cloud Security Threats through AI-Enhanced Zero Trust Models*. Proceedings of the 2023 IEEE International Conference on Cloud Computing, 156-165. https://doi.org/10.1109/CLOUD.2023.00123