ZERO-TRUST ARCHITECTURE IN HYBRID CLOUD ENVIRONMENTS WITH AI-DRIVEN THREAT DETECTION: A NEXT-GEN APPROACH TO CYBERSECURITY

Istamov Mirjahon Mo‘minjon ogli
Bahronov Shahzodjon Vahobjon ogli
Isoqov Diyorbek Dilshod ogli

Annotation. This article analyzes the issues of threat detection based on artificial intelligence (AI) and ensuring cybersecurity through Zero-Trust architecture in hybrid cloud environments. Due to the inadequacy of traditional security approaches in hybrid infrastructures, it is essential to operate based on the Zero-Trust model, which verifies every access point. AI technologies enable real-time threat prediction, anomaly detection, and rapid response to threats. Furthermore, the article highlights how the components of Zero-Trust architecture, user identity, permission management, and security monitoring integrate with AI. Additionally, through the application of AI and Zero-Trust approaches in hybrid cloud environments, organizations can establish a robust defense system against cyberattacks, automate security policies, and maintain constant monitoring of information systems.

Keywords: AI, Zero-Trust architecture, cybersecurity, hybrid cloud environments, threat detection, artificial intelligence, security monitoring, user authentication, access control, automated security, real-time analysis, zero trust model.

In recent years, due to the accelerated digital transformation, organizations are placing great emphasis on migrating their IT infrastructure to cloud environments. In particular, hybrid cloud environments – a combined form of private and public cloud infrastructure – offer organizations benefits such as flexibility, scalability, and cost reduction. However, this approach also introduces new types of risks.

In response to this issue, threat detection based on Zero-Trust architecture and AI (artificial intelligence) technologies is being recognized as a new paradigm in cybersecurity. Through these, businesses are shifting from the principle of 'trust, but verify' to the principle of 'always verify'.

Hybrid cloud is an integrated form of private and public cloud infrastructure that allows organizations to manage their data and applications flexibly.

- Advantages of hybrid cloud
- Flexibility and scalability;
- Cost optimization;
- Maintaining high security for specific data;

Cybersecurity risks in hybrid cloud

- Risk of data leaks;
- Network attacks (DDoS, MITM);
- Breach of identification and authentication;
- Unauthorized access;
- Internal threats and misconfiguration.

Zero-Trust is a security concept that does not automatically trust any user or device. Any action or access request undergoes strict verification.

Core principles of Zero-Trust

a) Continuous verification: Every access attempt is checked.

b) Principle of least privilege: Users are granted only necessary permissions.

c) Micro-segmentation: The network is divided into small parts.

d) Monitoring and surveillance: Actions are analyzed continuously.

Components of Zero-Trust architecture

1) Identity and Authentication Management systems (IAM);

2) Firewalls, network segmentation;

3) Access policies for data;

4) Security monitoring and analysis systems.

AI technologies in cybersecurity are used for the following purposes:

➢ Real-time threat detection;

➢ Prediction of unknown threats;

- Rapid response to risks;

AI-based threat detection algorithms

a) Machine Learning (ML): Recognizing anomalies;

b) Deep Learning: Detecting complex attacks (APT);

c) Natural Language Processing (NLP): Analyzing malicious content; d) Reinforcement Learning:

Decision making.

Areas of Application of Artificial Intelligence

UEBA (User and Entity Behavior Analytics): Analyzing user behaviors;

SIEM (Security Information and Event Management): Gathering and analyzing security incidents;

SOAR (Security Orchestration, Automation and Response): Automated security responses.

Hybrid cloud environments are dynamic, changing, and wide-ranging, and traditional security approaches cannot fully protect them. Therefore, it is crucial to combine AI and Zero-Trust approaches.Integrated Approach

Zero-Trust continuously assesses the trust level of users and devices;

AI detects threats in real-time and automatically initiates protective measures.

Expected Outcomes from Integration

- High-level security oversight;
- Combating threats without human intervention;
- Automation of security policies;
- Self-healing systems.

Google has implemented the Zero-Trust model through its BeyondCorp project. This project provides employees with secure access from anywhere.

Microsoft is developing security policies tailored to the Zero-Trust concept by integrating AI-based threat detection systems into its cloud security platform.

IBM has introduced modules that predict threats and implement automatic measures using artificial intelligence.

Advantages:

• A new level of security;

• Rapid response and flexibility;

• Effective detection of internal and external threats;

• Automated security policies. Problems:

• False positives of AI systems; • Challenges in fully implementing Zero-Trust;

• Training of employees and cultural changes;

• Resource and infrastructure requirements.[1]

Insider threat detection – One of the fastest-growing applications of artificial intelligence in the field of security is modeling the behavior of employees, access logs, and patterns in emails to detect potential insider threats. External aggressors often rely on gaining access to internal information. AI behavior analysis for detecting insider threats is a key priority task for both government and private sector organizations.

In today's world, as the digital landscape becomes increasingly complex, the field of cybersecurity is moving away from traditional approaches and relying on artificial intelligence (AI) and machine learning (ML) technologies. In particular, networks and cross-screen systems based on AI and ML are emerging as next-generation security systems. These systems not only analyze regular traffic but also deeply study user behavior, environmental changes, and contextual information, identifying threats in real-time and taking countermeasures. Analyses indicate that AI-integrated security systems are significantly more effective than conventional signature and rule-based systems. They prove their worth in detecting complex and advanced threats, especially 0-day exploits, APT (Advanced Persistent Threats) attacks, and harmful impacts delivered through encrypted traffic. At the same time, there are certain challenges in implementing these technologies into practice.

[1] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. Military Communications and Information Systems Conference.

In summary, the scale and complexity of cyber threats require increasingly automated security techniques driven by AI. Adapting to the volume and complexity of modern cyber threats is becoming impossible solely through manual human techniques. AI promises to be a game-changing technology for cyber defense. However, it must be managed carefully to ensure that the models are understandable and fair, and that they are aimed at enhancing human security teams rather than replacing them. An AI oversight balanced with flexibility for continuous adjustment can ensure robust innovations in algorithms while preventing negative consequences. Responsible use of artificial intelligence allows it to play a very valuable role in strengthening cybersecurity in a world that needs digital protection.

The Zero-Trust architecture and AI technologies play a significant role as a new approach to ensuring cybersecurity in hybrid cloud environments. Through these approaches, organizations can highly protect the integrity, security, and confidentiality of their data.

Furthermore, the self-developing capabilities of AI enhance the static parts of Zero-Trust and elevate security to an advanced level.

Therefore, it is recommended for organizations to:

- Implement the Zero-Trust model gradually;
- Configure AI-based threat analysis systems;
- Regularly train users;
- Continuously update data policies.

REFERENCES

1. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.
2. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4).
3. Sculley, D., et al. (2015). Machine Learning: The High-Interest Credit Card of Technical Debt. NIPS.

4. Fortinet (2023). FortiAI: Artificial Intelligence for Cybersecurity – Whitepaper.

5. Darktrace (2024). Enterprise Immune System: AI for Cyber Defense – Technical Overview.

6. Palo Alto Networks (2024). Cortex XDR and the Role of ML in Threat Detection – Product Documentation.

7. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. Military Communications and Information Systems Conference.