Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

AI-Driven Policy Enforcement & Threat Detection

Dr.K.Gomathi[1], Dr. Medhunhashini D R [2], Ms.K.Sutha[3]

[1]*Assistant Professor, Sri Krishna Arts and Science College, Coimbatore*
[2]*Assistant Professor, Sri Krishna Arts and Science College, Coimbatore*
[3]Assistant Professor, Sri Krishna Arts and Science College, Coimbatore

---

Abstract

Utilization of digital technologies in the industry has been very effective in boosting the performance of the organizations. At the same time, it has increased the attack surface available to the cyber criminals. Diversity of cloud services, networks and applications has made it challenging to ensure that there will be effective detection of threats and policy enforcement. Traditional measures have limited scope and cannot effectively tackle cyber threats. AI based policy enforcement and threat detection model that combines the Artificial Intelligence, Data Analytics and Machine Learning to protect the organization and ensures compliance with the regulations.

Purpose of AI-drive policy enforcement is to verify privacy, access control and data governance principles. Models in AI predict accurately on suspected violations, since they learn continuously from the workflow in the organization unlike the traditional systems. Therefore, such system has the capability of automatically blocking any action when the employees try to conduct fraudulent data transfer. Usage of natural language processing in emails and documents ensures that there will be ethical and legal compliance in the communications. Therefore, AI eliminates the manual error prone process in applying policies into intelligent purpose.

AI contributions to threat detection: When machine learning and deep learning models analyze the volume of network traffic, system logs and user activities, they are equally important. AI creates baselines of normal activities and detects the irregularities in form of abnormal logins, erratic data download and abnormal trends in accessing the systems. These irregularities may indicate phishing, ransomware and zero-day threats. AI has the capability of identifying new and hidden threats that are opposite to the traditional signature based systems. Some systems also automatically react to prevent worst attacks by actions such as removing access privileges, blocking malicious IP addresses or isolation of the affected systems.

Models of AI powered detection and enforcement can be seen in several areas. AI enhanced Intrusion system and security information and event management solutions provide visibility for various attack patterns in cyber security. Artificial Intelligence in the Banking Industry provides compliance to anti-money laundering regulations by prohibiting fraud transactions after detecting the unusual patterns. Health care industries use AI in order to protect patients' information and ensure compliance with regulations such as HIPPA. Cloud infrastructure uses the AI capability in detecting configuration errors, policy infractions and unusual access activity where traditional monitoring proves insufficient. Similarly, Business sectors use AI to ensure compliance across geographically distributed IT Systems, access control and prevention of data leakages.

The advantage of this strategy is immense. Scalability – processing massive amount of information beyond the capabilities of human beings - and adaptability – learning new attack methods and changes in regulations - are two of the advantages of artificial intelligence. With such abilities, it becomes possible to implement proactive defense measures by identifying and eliminating threats in advance. Moreover, it helps to eliminate the inconsistencies which occur in the manual monitoring by minimizing human errors. AI based solutions offer enterprises a comprehensive defensive solution which helps to increase resilience and trust by integrating governance and security.

The enormous possible of AI powered threat detection and policy enforcement is obvious; however, there are challenges in terms of false alarms, privacy concerns and necessity of frequent updates. AI can provide adaptive security, ensure compliance and be the base of secure and resilient digital ecosystems under correct supervision and moral usage.

***Key Words*: Attack, IOT, Defence, Artificial Intelligence, NLP**

1. INTRODUCTION

Adopting new technologies like cloud computing, distributed business systems, big data platforms, and the Internet of Things (IoT) has greatly improved productivity and efficiency in organizations. However, these changes have also led to a rise in potential cybercrime attacks. Modern organizations operate in an environment with numerous cloud service providers, complex networks, and various applications. This adds complexity to policy implementation and threat identification.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Traditional cyber security solutions that depend on signature-based detection and static rules are not enough to defend against modern threats. These methods have a limited scope, are slow, and fail to adjust to new attack types. In this context, using artificial intelligence (AI) is becoming an essential method for enhancing threat detection and enforcing policies.

AI-enabled policy enforcement and threat detection involve using artificial intelligence, data analytics, and machine learning to meet regulations, safeguard critical information, and reduce cyber threats. The ideology, plan, application, advantages, and challenges of the AI-based threat detection and policy enforcement in different areas are analyzed in this chapter.

2. TRADITIONAL POLICY ENFORCEMENT AND THREAT DETECTION'S LIMITATIONS

The key components of classical security system approaches are reactive monitoring, manual audit, and rule-based methods. Despite being partially effective, they are not enough in large, dynamic environments.

Limitations include:

- The high frequency of false positives, which overloads security experts.
- Manual implementation of policies, causing inconsistencies and human errors.
- Dependency on static rules, thus making such systems vulnerable to zero-day attacks.
- Scalability issues, preventing handling massive network traffic and data volumes.
- Lack of timely reaction, thus allowing attackers to exploit vulnerabilities.

Such drawbacks require automated and intelligent security solutions capable of dealing promptly with modern cyber threats.

3. AI-DRIVEN POLICY ENFORCEMENT: PROCESSES AND CONCEPTS

The overarching principle of AI-driven policy enforcement is the automation of verifications and policy implementation related to access control, corporate privacy and data governance policies.

3.1 Automated Compliance Assurance

AI tools continuously audit organizational processes, access logs, data consumption, and workflows for compliance with company policies and legal regulations. Instead of static and rules-based systems, AI is adept at predicting future policy violations by learning about the normal flow of business.

3.2 Intelligent Access Management

Machine learning algorithms continuously monitor user access patterns and context (time, location, and device) to dynamically implement context-aware access controls. Suspicious activities such as unauthorized data transfers or abnormal access attempts are automatically prohibited.

3.3 NLP for policy enforcement

With NLP technologies used to monitor email, documents, and messages for any potential ethical, legal, or company policy violations, AI helps in curbing insider threats, data leakage and other non-compliant communication patterns, replacing inefficient manual and error-prone enforcement.

4. HOW AI IS CHANGING THE GAME IN THREAT DETECTION

In the face of an overwhelming volume of data, AI has the capability of analysing security information beyond what's physically possible for any human.

4.1 Anomaly Detection with ML & Deep Learning

AI, Machine learning, or Deep Learning is trained using system logs, user behaviour and network traffic information to create the patterns and behaviours of what is a' Normal system'. Any new activity that drifts from this baseline might be a cause for alarm: This includes:
Anomaly detection with Machine Learning (ML) or Deep Learning: Malicious activities will stand out from normal behaviour patterns like – unusual logins, downloads, access and elevated privilege levels.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

4.2 Advanced & Zero Day Threat detection

The advantage of using ML-driven AI for this is that the models will identify any new and unfamiliar behavior pattern without the need for signature definition, unlike traditional systems, the ML-driven will be capable of identifying: Malicious files and processes Phishing attacks, Ransom ware and Zero-Day Exploits.

4.3 Automation of Incident Response

Once anomalies or security threats are flagged, complex AI Systems will initiate pre-programmed responses, including: Remove any associated malicious user agents, or browser extension Block associated IP addresses Isolate the affected computers automatically create incident alerts for the security team this automates the response process and reduces the possibility of further escalation.

5. DESIGN Of AI-POWERED THREAT DETECTION AND POLICY ENFORCEMENT SYSTEMS

Typical AI security infrastructure consists of the following layers:

a) Data Collection Layer: Gathers data from various sources such as cloud, users, networks, and logs.

b) Data Processing Layer: This layer cleanses, aggregates, and normalizes security data.

c) AI Analytics Layer Leverages: AI-based machine learning and deep learning, and natural-language-processing (NLP).

d) Decision Engine: The decisions engine detects dangers and policy violations.

e) Response and Enforcement Layer: Take dedicated actions and sends automated notifications.

f) This tiered approach ensured that there is a security layer that offers scalability, flexibility, and real-time nature of operations.

6. DOMAIN-SPECIFIC APPLICATIONS

6.1 IT infrastructure and cyber security

AI-driven SIEM and IDS systems enhance real-time visibility into attack patterns infrastructure vulnerabilities.

6.2 Financial Services and Banking

Ensure Compliance with AML regulations; AI stops fraudulent activities and anomalies in transactions.

6.3 The Healthcare Industry

Protect sensitive patient information from unauthorized access while comply with data privacy policies such as HIPAA.

6.4 Enterprise and Cloud Systems

- Monitor distributed cloud infrastructures for configuration issues, unauthorized activity, access breaches, and unusual patterns that traditional tools fail to monitor.
- Benefits of AI-Powered Threat Identification and Policy Enforcement

AI security solutions offer numerous benefits, including:

- Scalability: The system is able to scale up and analyze vast amounts of data that is beyond human ability.
- Adaptability: The system continually Learns about changing policies and emerging threats.
- Proactive Defense: Identifies and neutralizes risk and threats prior to damaging activities taking place.
- Reduced Human Error: Avoid inconsistency in manual monitoring procedures.
- Integrated Governance and Security: This enhances trust worthiness and organizational resilience.
- These are some of the key areas where artificial intelligence is used extensively in the cyber security landscape today.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

6.5. Challenges and Ethical Concerns

Despite the promise, there are several challenges to AI-driven security, including: false positives and alert fatigue; data privacy concerns; AI model bias; need for continuous learning and updates; ethics and compliance issues; Organizations can tackle these challenges with explainable AI, robust governance, and human oversight.

7. CONCLUSIONS

AI-driven threat detection and policy enforcement are revolutionizing cyber security. By integrating AI into security architectures and governance policies, organizations can achieve proactive threat prevention, regulatory compliance, and agile defenses. Despite remaining challenges, the ethical deployment of AI will result in secure and reliable digital environments.

8. FUTURE DIRECTIONS

Future trends in AI-driven security include: explainable AI for transparency in decisions; federated learning for privacy-preserving threat detection; automated security orchestration; block chain integration for immutable logs; This progress will lead to increased digital resilience and trust.

REFERENCES

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
2. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
5. 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.
6. Shackleford, D. (2019). Security Governance, Risk Management, and Compliance. Syngress.
7. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
8. Behl, A., & Behl, K. (2017). Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press.
9. Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.
10. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
11. IBM Security. (2022). Artificial Intelligence and Cybersecurity. IBM White Paper.
12. Gartner. (2023). Market Guide for AI-Based Threat Detection and Response. Gartner Research.
13. Ahmad, Z., Shahid Khan, A., Shiang, H., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1).
14. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. International Organization for Standardization.
15. European Union. (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union.