World Journal of Multidisciplinary Research and Development
worldsubjectjournal.com
Online ISSN: 3107-9598
Received: 09-09-2026, Accepted: 09-10-2026, Published: 24-10-2026
Volume 2, Issue 4, 2026, Page No. 20-23

AI-based cybersecurity frameworks for real-time threat detection and automated incident response

Fabien Charmet
National Institute of Information, Communications Technology (NICT), Koganei, Tokyo, Japan

Abstract
The rapid expansion of cloud computing, Internet of Things (IoT) technologies, interconnected networks, and digital services has increased the complexity of modern cybersecurity environments. Conventional cybersecurity mechanisms based primarily on predefined rules and signatures can be effective against known threats but may have limitations when confronted with rapidly evolving and previously unseen attacks. Artificial intelligence (AI), particularly machine learning (ML) and deep learning, provides new opportunities for developing cybersecurity frameworks capable of real-time threat detection, behavioral analysis, incident prioritization, and automated response. AI-based systems can analyze large volumes of security events and identify abnormal patterns that may indicate malicious activity. Recent research shows that AI can support multiple cybersecurity functions, including detection, protection, response, and recovery (Kaur *et al*., 2023).[2] NIST's emerging Cyber AI Profile similarly identifies advanced threat detection, anomaly detection, user and entity behavior analytics, and automated incident response as important applications of AI for cybersecurity. This article examines the architecture, applications, benefits, challenges, and future directions of AI-based cybersecurity frameworks for real-time threat detection and automated incident response.

Keywords: Artificial intelligence, cybersecurity, real-time threat detection, machine learning, automated incident response, anomaly detection

Introduction

India's tribunal system has repeatedly generated the same constitutional anxiety: bodies created to exercise judicial or quasi-judicial power have often remained administratively dependent on the executive departments whose decisions the increasing dependence on digital infrastructure has transformed cybersecurity into an essential component of organizational operations. Businesses, financial institutions, healthcare organizations, educational institutions, and government agencies increasingly rely on interconnected systems to store information and deliver services. While digital transformation provides significant benefits, it also creates an expanding attack surface that can be exploited by cybercriminals.

Traditional cybersecurity approaches frequently rely on signatures, predefined rules, and manually configured security policies. These approaches remain important, but they may be less effective when attackers use unfamiliar techniques or modify known attack patterns. Artificial intelligence provides an opportunity to complement these mechanisms by enabling cybersecurity systems to learn from data and identify patterns associated with suspicious behavior. A comprehensive review of AI in cybersecurity found that AI can automate repetitive activities, accelerate threat detection and response, and support security teams in addressing cyber threats (Kaur *et al*., 2023) [2]. AI-based cybersecurity frameworks therefore seek to combine intelligent data analysis with automated security operations. Such frameworks can collect security information from multiple sources, analyze events in real time, identify potential threats, prioritize incidents, and initiate predefined responses. The objective is not simply to automate cybersecurity but to create a more adaptive and responsive security architecture.

Architecture of an AI-Based Cybersecurity Framework

An AI-based cybersecurity framework can be conceptualized as a multilayer architecture consisting of data collection, preprocessing, intelligent analysis, threat detection, decision-making, response, and continuous monitoring. The data collection layer gathers information from network traffic, endpoint devices, authentication systems, firewalls, applications, cloud services, and security logs. Because cybersecurity environments generate large volumes of heterogeneous information, the ability to integrate multiple data sources is an important characteristic of an effective framework. The data-processing layer transforms raw security information into useful representations for AI models. This may involve feature extraction, normalization, filtering, and correlation. Poor-quality or incomplete data can negatively affect model performance, making data preparation an important part of the framework.

The intelligent analysis layer applies machine-learning, deep-learning, anomaly-detection, or other AI techniques to identify patterns associated with suspicious activities. AI-based intrusion detection research has demonstrated the use of machine learning, deep learning, and ensemble learning for detecting network attacks. The decision and response layer evaluates detected events and determines appropriate actions. Depending on organizational policies and the severity of an incident, responses may involve generating alerts, isolating affected systems, initiating predefined incident-response workflows, or escalating the event to cybersecurity professionals. Finally, the continuous monitoring layer evaluates system performance and incorporates new information to support model improvement. This is particularly important because cyber threats and normal system behavior can change over time.

Real-Time Threat Detection

Real-time threat detection is one of the central objectives of AI-based cybersecurity frameworks. Modern organizations may generate thousands or millions of security events, making it difficult for human analysts to examine every event individually. AI can assist by processing these events rapidly and identifying patterns that require attention. Machine-learning models can classify network traffic into legitimate and potentially malicious categories. Unsupervised learning can identify anomalous behavior without requiring every possible attack to be represented in the training dataset. Deep-learning models can also analyze complex patterns across large volumes of security data. A recent review of AI-based intrusion detection systems found that machine learning, deep learning, and ensemble approaches have demonstrated potential for improving automated attack detection. However, real-time detection remains challenging because cybersecurity environments are dynamic and legitimate activities can sometimes resemble malicious behavior. Therefore, AI-based detection should incorporate contextual information and multiple indicators rather than relying exclusively on a single prediction.

Automated Incident Response

Detecting a threat is only one stage of cybersecurity. Once a suspicious event has been identified, an organization must determine its severity and take appropriate action. AI can support this process by correlating alerts, prioritizing incidents, summarizing relevant information, and initiating predefined response procedures. NIST's Cyber AI Profile identifies automated incident response as an AI application that can support actions such as automated lockdown, incident playbooks, and consistency in incident responses. This demonstrates the potential for AI to reduce the time between detection and response. Automated response can be particularly useful for repetitive and clearly defined security events. For example, a framework could apply an established response procedure when a high-confidence security condition is identified. More complex or uncertain incidents can instead be escalated to human analysts. This combination of automation and human oversight can help reduce response delays while limiting the risks associated with fully autonomous decision-making.

Threat Intelligence and Behavioral Analysis

AI-based cybersecurity frameworks can also incorporate threat intelligence and behavioral analysis. Threat intelligence provides contextual information about potential threats, while behavioral analysis examines how users, devices, applications, and networks normally operate. Machine-learning models can establish behavioral baselines and identify deviations from expected patterns. For example, unusual authentication behavior, unexpected network communication, or abnormal data transfers may trigger additional investigation. Recent research on AI-driven cybersecurity emphasizes behavioral analysis and threat intelligence as important components of intelligent security systems. AI can integrate information from different sources and identify relationships that may be difficult to detect through manual analysis alone (Ali *et al*., 2025) [5].

Benefits of AI-Based Cybersecurity Frameworks

AI-based cybersecurity frameworks provide several potential benefits. First, they can improve the speed of threat detection by processing security information continuously. Second, they can support scalability, allowing organizations to analyze security events that would be difficult to process manually. Third, AI can improve alert prioritization by helping security teams distinguish potentially significant events from lower-priority activities. Fourth, automated response capabilities can reduce the time required to initiate predefined defensive procedures. Another important benefit is the ability to support adaptive cybersecurity. Traditional rule-based systems generally require security professionals to define specific rules, whereas machine-learning systems can identify patterns from data. This can help complement conventional security technologies in environments where attack patterns change frequently. Research on AI and ML in network security indicates that these technologies can contribute to threat detection, automated response, and prediction of potential vulnerabilities, although their successful implementation requires integration with existing security architectures.

Challenges and Limitations

Despite their potential, AI-based cybersecurity frameworks face several challenges. One major challenge is data quality. Machine-learning systems require appropriate training and evaluation data. Inaccurate, incomplete, outdated, or imbalanced datasets can reduce detection performance. Another challenge is false positives. A system that generates excessive false alarms can overwhelm security analysts and reduce operational efficiency. Conversely, false negatives can allow genuine threats to remain undetected. Therefore, cybersecurity AI systems should be evaluated using multiple measures, including precision, recall, F1-score, detection rate, and false-positive rate. Model generalization is another concern. An AI system trained in one network environment may not perform equally well in another environment because network configurations, users, applications, and attack patterns differ. AI systems also face adversarial threats. Attackers may attempt to manipulate inputs or training data to influence model decisions. NIST's 2025 adversarial machine-learning taxonomy identifies multiple attack categories and emphasizes the need for appropriate mitigation throughout the AI lifecycle.

Explainability and Human Oversight

Explainability is particularly important when AI systems are used for security decisions. Cybersecurity professionals may need to understand why an event was classified as malicious before initiating a response. Explainable AI techniques can provide information about the factors influencing model predictions. This can improve analyst confidence and make it easier to investigate incorrect classifications. Human oversight also remains important. Automated systems can process large volumes of information quickly, but human analysts can provide contextual judgment when security events are ambiguous or have significant operational consequences. A balanced framework can therefore assign routine and high-confidence activities to automation while escalating uncertain or high-impact incidents to security professionals

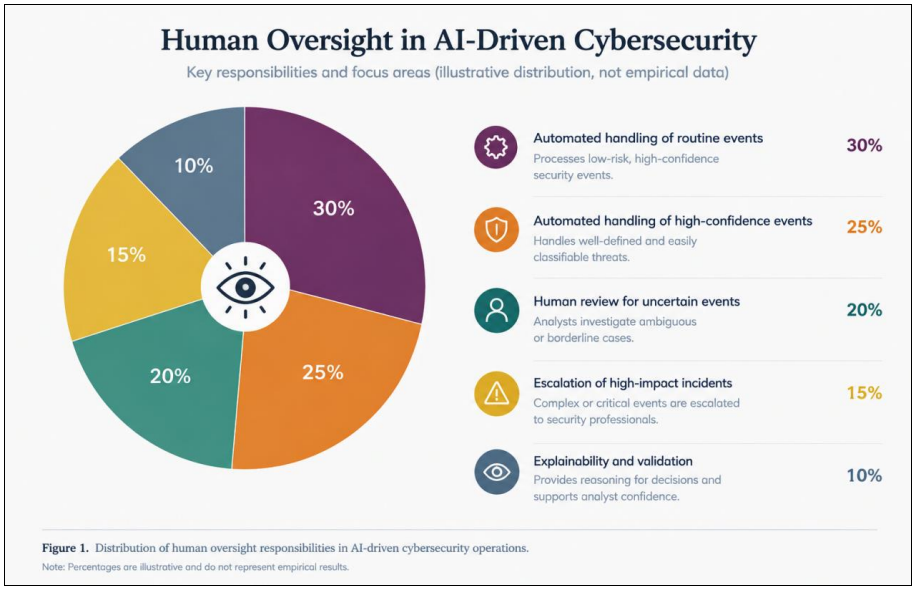

Figure 1. Distribution of human oversight responsibilities in AI-driven cybersecurity operations.
Note: Percentages are illustrative and do not represent empirical results.

Future Directions

The future development of AI-based cybersecurity frameworks is likely to focus on adaptive, explainable, privacy-conscious, and resilient systems. Continual learning may allow models to adapt to changing threat environments, while federated learning could support collaborative security analysis without requiring organizations to centralize all raw data. Generative AI is also emerging as a cybersecurity technology. Recent research indicates that generative AI can support anomaly detection, incident response, attack simulation, and security analysis, while simultaneously creating new risks such as sophisticated phishing, adversarial exploitation, and model manipulation. Another emerging direction is the development of self-adaptive and self-healing cybersecurity architectures. Such systems could continuously monitor their environments, detect changes, and recommend or implement appropriate security adjustments. NIST's Cyber AI Profile further illustrates the direction of current cybersecurity research by connecting AI-related security risks with opportunities to use AI for cybersecurity capabilities, including advanced detection and automated response.

Conclusion

AI-based cybersecurity frameworks provide an important approach for improving real-time threat detection and automated incident response. Through machine learning, deep learning, behavioral analysis, and intelligent automation, these frameworks can process large volumes of security information, identify suspicious activities, prioritize threats, and support faster responses. However, AI should not be viewed as a complete replacement for traditional cybersecurity technologies or human expertise. Data quality, false positives, model generalization, explainability, privacy, and adversarial attacks remain significant challenges. The security of the AI systems themselves must also be considered as organizations increasingly depend on automated decision-making. An effective AI-based cybersecurity framework should therefore integrate intelligent detection with established security controls, continuous monitoring, human oversight, and clearly defined response policies. The continued development of trustworthy and adaptive AI technologies can contribute to cybersecurity infrastructures that respond more effectively to increasingly complex digital threats.

References

1. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials,2016:18(2):1153–1176.
2. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion,2023:97:101804.
3. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity,2019:2:20.
4. Vassilev A, Oprea A, Fordyce A, Anderson H, Davies X, Hamin M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. National Institute of Standards and Technology, 2025.
5. Ali S, Wang J, Leung VCM. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms—A comprehensive review. Information Fusion,2025:118:102922.
6. Bhatta RP. Ensemble based machine learning model for prediction of diabetes. NPRC Journal of Multidisciplinary Research,2026:3(2):116–129.
7. Paulraj J, Raghuraman B, Gopalakrishnan N, Otoum Y. Autonomous AI-based cybersecurity framework for critical infrastructure: Real-time threat mitigation. In: 2025 IEEE/ACIS 29th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, 2025, 925–931.
8. Biswas S. Artificial Intelligence–Enhanced Cybersecurity Frameworks for Real-Time Threat Detection In Cloud And Enterprise. ASRC Procedia: Global Perspectives in Science and Scholarship,2025:1(01):737–770.
9. Kaium R, Alasa L, Robert K, Kaium O, Diana K. Artificial Intelligence-Based Cyber Threat Detection and Response for Critical Infrastructure Security. The

Eastasouth Journal of Information System and Computer Science,2026:4(01):1–16.
10. Zhang J, Li S, Huang W, Jing H, Zhang Q, Xia X. Design and Computational Modeling of an AI-Based Automated Cybersecurity Incident Response System. IEEE Access,2025.
11. Chirra DR. Towards an AI-Driven Automated Cybersecurity Incident Response System. International Journal of Advanced Engineering Technologies and Innovations,2023:1(01):429–451.
12. Ndibe OS. AI-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. International Journal of Research Publication and Reviews,2025:6(5):389–411.
13. Khalaf NZ, Barazanchi A, Ibraheem I, Radhi AD, Shah P, Sekhar R. Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. Mesopotamian Journal of CyberSecurity,2025:5(2):501–513.
14. Aramide OO. AI-driven automated incident response and remediation in networks. International Journal of Technology, Management and Humanities,2025:11(02):1–9.
15. Tanimu JA, Bendiab G, Kanta A, Shiaeles S. AI-Driven Threat Detection and Automated Incident Response for Enhancing Network Security. Network,2026:6(2):32.