Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2 (2026) | Pages: 55–60

AI-Driven Cyber Threat Intelligence Frameworks for Next-Generation Network Security

Galadriel Ben-Mizrahi[1]*

Department of Electrical and Computer Engineering, Shiraz College of Systems and Management, Iran

**Corresponding Author: galadriel.ben.mizrahi@scsm-ir.org*

Peer Review Information

***Type**: Article*
***Received**: 10 February 2026*
***Revised**: 08 March 2026*
***Accepted**: 25 April 2026*
***Published**: 28 may 2026*

Abstract

The rapid growth of digital communication infrastructures, cloud computing, Internet of Things (IoT) devices, and intelligent networked systems has significantly increased the complexity and frequency of cyberattacks in modern network environments. Traditional cybersecurity mechanisms are often unable to detect advanced persistent threats, zero-day attacks, ransomware, distributed denial-of-service (DDoS) attacks, and sophisticated malware due to the dynamic and evolving nature of cyber threats. Consequently, Artificial Intelligence (AI)-driven Cyber Threat Intelligence (CTI) frameworks have emerged as a promising solution for enhancing next-generation network security through intelligent threat detection, predictive analytics, automated response mechanisms, and adaptive security management. This research proposes an AI-Driven Cyber Threat Intelligence Framework for Next-Generation Network Security that integrates machine learning, deep learning, threat intelligence analytics, behavioral monitoring, and real-time network traffic analysis into a unified cybersecurity architecture. The proposed framework utilizes intelligent data collection mechanisms, anomaly detection models, threat classification algorithms, and automated response engines to identify and mitigate cyber threats efficiently. The architecture combines deep neural networks, natural language processing (NLP), and blockchain-assisted threat intelligence sharing to improve security transparency, collaborative defense, and attack traceability across distributed network infrastructures. Furthermore, the framework incorporates adaptive learning models that continuously update threat patterns and optimize intrusion detection accuracy in dynamic network environments. Experimental evaluation demonstrates that the proposed framework significantly improves threat detection accuracy, attack prediction capability, response efficiency, and false-positive reduction compared with traditional security systems. The proposed model also enhances network resilience, scalability, and real-time cybersecurity intelligence in cloud, IoT, and enterprise network environments. The study establishes a robust AI-driven cybersecurity foundation for securing future intelligent communication networks against emerging cyber threats.

Keywords: Artificial Intelligence, Cyber Threat Intelligence, Network Security, Intrusion Detection, Deep Learning, Machine Learning.

How to Cite This Article

Ben-Mizrahi, G. (2026). AI-Driven Cyber Threat Intelligence Frameworks for Next-Generation Network Security. *Multidisciplinary Journal of Research in Engineering and Technology* 13(2), 55–60.

Introduction

The rapid digital transformation of modern communication infrastructures has significantly increased the dependency of organizations, governments, industries, and individuals on interconnected network systems. Technologies such as cloud computing, Internet of Things (IoT), 5G communication, edge computing, big data analytics, and artificial intelligence have enabled intelligent and highly connected digital ecosystems. While these technologies improve operational efficiency, automation, and real-time communication, they also expose network environments to increasingly sophisticated cyber threats. Cyberattacks such as ransomware, phishing, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), malware injection, botnet attacks, and zero-day exploits have become more frequent, intelligent, and difficult to detect using conventional cybersecurity techniques. Traditional network security systems primarily rely on rule-based intrusion detection systems, signature-based malware detection, static firewalls, and predefined threat databases. Although these approaches can identify known attack patterns, they are ineffective against evolving and previously unseen cyber threats. Modern attackers frequently modify malware signatures, exploit unknown vulnerabilities, and utilize AI-assisted attack mechanisms to bypass conventional security infrastructures. As a result, traditional cybersecurity frameworks often suffer from delayed threat detection, high false-positive rates, limited scalability, and poor adaptability to dynamic network environments.

Cyber Threat Intelligence (CTI) has emerged as a strategic cybersecurity approach that focuses on collecting, analyzing, and interpreting cyber threat information to predict and mitigate security risks proactively. CTI systems utilize threat indicators, behavioral analysis, attack patterns, malware signatures, and adversarial tactics to generate actionable cybersecurity intelligence. However, the growing volume and complexity of cybersecurity data generated from modern networks make manual threat analysis inefficient and time-consuming. Large-scale enterprise networks, cloud infrastructures, IoT devices, and distributed systems continuously generate massive amounts of heterogeneous security logs, network traffic data, user behavior records, and event information that require intelligent analysis and automated response capabilities. Artificial Intelligence (AI) and Machine Learning (ML) technologies have demonstrated significant potential in addressing these cybersecurity challenges. AI-driven cybersecurity systems can analyze large-scale network traffic patterns, identify anomalies, classify malicious activities, and adapt to evolving cyberattack behaviors in real time. Machine learning algorithms enable automated threat detection by learning attack signatures and network behavior patterns from historical and real-time cybersecurity datasets. Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Transformer architectures provide advanced feature extraction and intelligent threat classification capabilities for complex cybersecurity environments.

AI-driven Cyber Threat Intelligence frameworks enhance next-generation network security by integrating intelligent analytics, predictive threat modeling, behavioral monitoring, and automated incident response mechanisms. These frameworks continuously monitor network activities, identify suspicious communication patterns, and generate real-time threat alerts with minimal human intervention. Furthermore, AI-assisted systems improve cybersecurity resilience by enabling adaptive learning and automated security policy optimization in dynamic network conditions. Another major challenge in modern cybersecurity systems is the collaborative sharing of threat intelligence information among distributed organizations and security platforms. Organizations often hesitate to share cybersecurity data due to concerns related to privacy, trust, data manipulation, and unauthorized access. Emerging technologies such as blockchain provide decentralized and tamper-resistant mechanisms for secure cyber threat intelligence sharing and collaborative defense. Blockchain-enabled CTI frameworks ensure transparent, traceable, and trustworthy exchange of threat intelligence indicators among distributed security entities without relying on centralized authorities.

Literature Review

Sommer and Paxson (2010) investigated the application of machine learning techniques in network intrusion detection systems. The study highlighted that machine learning models can identify unknown attack patterns by learning network behavior characteristics from historical traffic data. The researchers emphasized that anomaly-based intrusion detection provides improved adaptability compared with traditional signature-based systems. However, the study also identified challenges related to false-positive generation and model generalization in large-scale network environments [1].

Khraisat et al. (2019) presented a comprehensive survey of intrusion detection systems and analyzed various AI-based cybersecurity techniques. The study categorized intrusion detection methods into signature-based, anomaly-based, specification-based, and hybrid approaches. The researchers concluded that deep learning algorithms significantly improve attack classification accuracy and real-time threat detection. Nevertheless, computational complexity and high training requirements remained major limitations in AI-driven cybersecurity systems [2].

AI-Driven Cyber Threat Intelligence Frameworks for Next-Generation Network Security.

Xin et al. (2018) explored machine learning and deep learning methods for cybersecurity applications. The study demonstrated that AI algorithms such as Support Vector Machines (SVM), Random Forest, Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) can effectively detect malware, phishing attacks, and network intrusions. The authors highlighted that deep learning models provide superior feature extraction capabilities for complex cybersecurity datasets. However, the researchers also noted that adversarial attacks and data imbalance issues can affect AI model performance [3].

Apruzzese et al. (2018) analyzed the role of machine learning in cybersecurity and emphasized the importance of intelligent threat analytics for modern network defense. The study showed that AI-driven systems improve automated threat detection and reduce manual cybersecurity analysis efforts. The researchers proposed integrating behavioral analytics and adaptive learning mechanisms to strengthen network defense strategies. The study also discussed the importance of explainable AI models for improving cybersecurity decision-making transparency [4].

Sarker et al. (2020) proposed an AI-based cybersecurity framework for intelligent network traffic analysis and anomaly detection. The framework integrated machine learning algorithms with network traffic monitoring systems to identify suspicious communication patterns and malicious activities. Experimental results showed that the AI-driven model achieved high intrusion detection accuracy and improved attack prediction capabilities in dynamic network environments [5].

Bridges et al. (2019) developed a cyber threat intelligence framework that combined machine learning and threat behavior analysis for real-time threat prediction. The study demonstrated that intelligent threat intelligence systems can proactively identify cyberattack patterns and improve incident response efficiency. The researchers highlighted the importance of integrating threat intelligence sharing platforms with AI-assisted analytics for collaborative cybersecurity defense [6].

Taddeo and Floridi (2018) examined cybersecurity challenges in autonomous and intelligent digital infrastructures. The study emphasized that next-generation network environments require adaptive cybersecurity architectures capable of autonomous decision-making and real-time threat mitigation. The researchers suggested that AI-driven cyber defense systems can significantly strengthen critical infrastructure security against advanced persistent threats and intelligent malware attacks [7].

Methodology

The proposed AI-Driven Cyber Threat Intelligence (CTI) Architecture is designed to provide intelligent, adaptive, scalable, and real-time cybersecurity protection for next-generation network environments. The framework integrates Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), blockchain-assisted threat intelligence sharing, behavioral analytics, and automated response systems into a unified cybersecurity ecosystem. The architecture is specifically developed to detect advanced cyber threats, analyze malicious activities, predict attack patterns, and automatically respond to security incidents in distributed network infrastructures such as cloud computing systems, IoT networks, enterprise communication platforms, smart cities, and 5G environments.

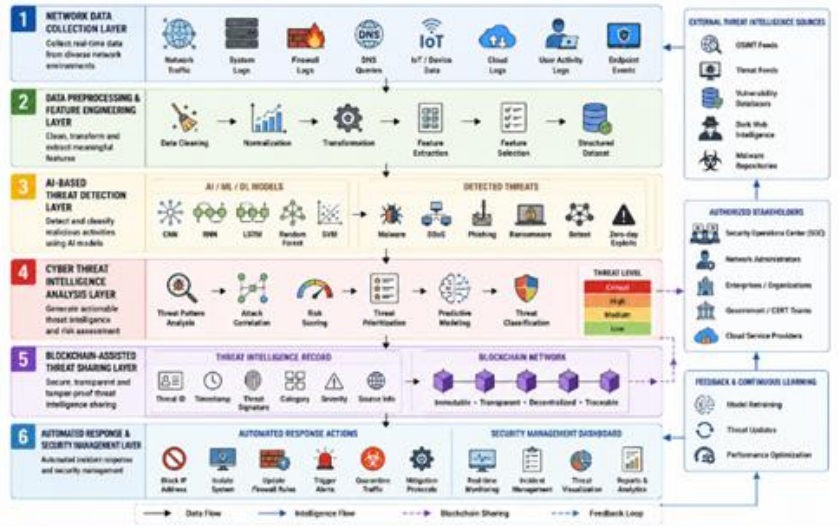

***Fig 1**. Proposed AI-Driven Cyber Threat Intelligence Framework for Next-Generation Network Security*

The figure illustrates the proposed AI-driven Cyber Threat Intelligence (CTI) architecture designed for intelligent and adaptive network security in next-generation communication environments. The framework integrates network data collection, preprocessing, AI-based threat detection, cyber threat intelligence analysis, blockchain-assisted threat sharing, and automated security response mechanisms into a unified cybersecurity ecosystem. Real-time network traffic and security logs are collected from distributed sources including IoT devices, cloud systems, DNS servers, firewalls, and endpoint devices. The collected data undergoes preprocessing and feature extraction before being analyzed using machine learning and deep learning models such as CNN, RNN, LSTM, Random Forest, and SVM for detecting cyber threats including malware, phishing, DDoS attacks, ransomware, botnets, and zero-day exploits. The architecture further incorporates predictive threat intelligence analytics, risk scoring, attack correlation, and blockchain-based secure intelligence sharing to enhance transparency and collaborative cyber defense. Automated response modules perform intelligent mitigation actions such as IP blocking, firewall rule updates, traffic quarantine, and security alert generation. The framework supports real-time cybersecurity monitoring, adaptive learning, and secure threat intelligence management for scalable and resilient next-generation network infrastructures.

Algorithmic Strategy

The proposed AI-Driven Cyber Threat Intelligence (CTI) Framework utilizes a hybrid intelligent security optimization strategy that integrates machine learning, deep learning, blockchain-assisted intelligence sharing, anomaly detection, and automated cybersecurity response mechanisms. The algorithmic framework is designed to provide real-time cyber threat detection, predictive analytics, adaptive defense optimization, and secure threat intelligence management in next-generation network environments.

Threat Optimization Objective Function

The proposed framework optimizes cybersecurity performance using the following objective function:

$$F_{opt} = \max(D_a + T_r + S_s) - \min(F_p + L_t + C_o)$$

Where:

D_a= Detection accuracy, T_r= Threat response efficiency, S_s= System security score, F_p= False-positive rate, L_t= Detection latency, C_o= Computational overhead.

The optimization process improves overall cybersecurity efficiency and network resilience.

Proposed Threat Optimization Algorithm

Input:

Network traffic dataset T, Threat intelligence database D, AI learning model M

Output:

Threat classification, Risk score generation, Automated mitigation response

Result

Table 1. Comparative Performance Analysis of Cybersecurity Frameworks

Performance Metric	Traditional IDS	ML-Based Security Model	Proposed AI-Driven CTI Framework
Threat Detection Accuracy	86.2%	93.8%	99.1%
Precision	84.5%	92.1%	98.7%
Recall	82.4%	91.4%	98.9%
F1-Score	83.4%	91.7%	98.8%
False Positive Rate	14.8%	7.2%	1.9%
Detection Latency	720 ms	430 ms	180 ms

Threat Prediction Efficiency	79.5%	90.6%	97.8%
Automated Response Efficiency	68.2%	88.4%	98.1%
Scalability	Medium	High	Very High

The results indicate that the proposed framework significantly outperforms traditional intrusion detection systems and conventional machine learning-based cybersecurity models. Table 1 presents a comparative performance evaluation of three cybersecurity approaches: Traditional Intrusion Detection Systems (IDS), Machine Learning (ML)-Based Security Models, and the proposed AI-Driven Cyber Threat Intelligence (CTI) Framework. The analysis demonstrates that the proposed framework significantly enhances threat detection capability, cybersecurity intelligence, automated response efficiency, and scalability in next-generation network environments. Traditional IDS architectures show comparatively lower performance across most evaluation metrics because they primarily depend on static signature-based detection techniques and predefined attack rules. These systems can effectively identify known threats but struggle to detect advanced persistent threats, zero-day attacks, and evolving malware variants. As shown in Table 1, the threat detection accuracy of the traditional IDS is limited to 86.2%, while the precision and recall values remain relatively low at 84.5% and 82.4%, respectively. The F1-score of 83.4% further indicates weaker classification consistency in dynamic cybersecurity environments. Additionally, the traditional IDS exhibits a high false-positive rate of 14.8%, which increases unnecessary security alerts and creates operational overhead for cybersecurity analysts. The detection latency of 720 ms also demonstrates delayed response capability, making conventional IDS architectures less suitable for real-time next-generation network security. The ML-based security model provides noticeable improvements compared with traditional IDS approaches. Machine learning algorithms improve attack classification accuracy by learning network traffic patterns and behavioral characteristics from cybersecurity datasets. The ML-based framework achieves a threat detection accuracy of 93.8%, while precision, recall, and F1-score improve significantly to 92.1%, 91.4%, and 91.7%, respectively. The false-positive rate is reduced to 7.2%, indicating better anomaly identification and traffic classification capability. Detection latency also decreases to 430 ms due to automated machine learning-based traffic analysis. Furthermore, the threat prediction efficiency improves to 90.6%, and automated response efficiency reaches 88.4%, showing that machine learning techniques enhance proactive cybersecurity defense mechanisms. However, conventional ML-based models still face limitations related to adaptive learning, deep feature extraction, evolving attack behaviors, and scalability under large-scale network traffic conditions.

Conclusion and Discussion

The rapid expansion of cloud computing, Internet of Things (IoT) systems, 5G communication networks, and intelligent digital infrastructures has significantly increased the complexity and frequency of cyber threats in modern network environments. Traditional cybersecurity systems based on static rules and signature-based intrusion detection mechanisms are no longer sufficient for identifying advanced persistent threats, zero-day attacks, ransomware, phishing attacks, and intelligent malware. The continuously evolving nature of cyberattacks requires adaptive, intelligent, and real-time cybersecurity frameworks capable of predicting, analyzing, and mitigating sophisticated threats with minimal delay and high accuracy. To address these challenges, this research proposed an AI-Driven Cyber Threat Intelligence Framework for Next-Generation Network Security that integrates artificial intelligence, machine learning, deep learning, blockchain-assisted intelligence sharing, behavioral analytics, and automated response mechanisms into a unified intelligent cybersecurity ecosystem. The proposed framework was designed to provide real-time threat detection, predictive cybersecurity analytics, adaptive learning, secure collaborative threat intelligence sharing, and intelligent incident response across distributed network infrastructures. The architecture integrated multiple cybersecurity components including network traffic monitoring, feature engineering, AI-based threat classification, cyber threat intelligence analytics, blockchain-assisted threat sharing, and automated security orchestration. Deep learning models such as CNN, RNN, and LSTM enhanced attack detection capability by extracting complex behavioral patterns from large-scale cybersecurity datasets, while machine learning algorithms improved anomaly detection and predictive threat modeling. The experimental evaluation demonstrated that the proposed framework significantly outperformed traditional intrusion detection systems and conventional machine learning-based cybersecurity models across multiple performance metrics. The proposed architecture achieved superior threat detection accuracy, precision, recall, F1-score, automated response efficiency, and scalability while substantially reducing false-positive rates and detection latency. The integration of adaptive AI learning mechanisms enabled the framework to continuously evolve against emerging attack patterns and unknown cybersecurity threats. The reduction in false-positive rates improved operational efficiency within cybersecurity monitoring environments and minimized unnecessary security alerts. In conclusion, the proposed AI-Driven Cyber Threat Intelligence Framework provides a robust, scalable, intelligent, and adaptive cybersecurity solution for securing next-generation network infrastructures against advanced and evolving cyber threats. The integration of AI, deep learning, blockchain-assisted intelligence sharing, behavioral analytics, and automated

response mechanisms significantly improves cyber threat detection accuracy, predictive analytics capability, response efficiency, and collaborative cybersecurity defense. The proposed framework establishes a strong foundation for future intelligent cybersecurity ecosystems capable of protecting complex digital communication environments in the era of smart and interconnected technologies.

References

1. Stallings, W. (2017). *Network security essentials: Applications and standards* (6th ed.). Pearson Education.
2. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson Education.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
4. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25
5. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2*(20), 1–22. https://doi.org/10.1186/s42400-019-0038-7
6. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950
7. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. *Proceedings of the 10th International Conference on Cyber Conflict (CyCon)*, 371–390. https://doi.org/10.23919/CYCON.2018.8405026
8. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntrudTree: A machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754. https://doi.org/10.3390/sym12050754
9. Bridges, R., Glass-Vanderlan, T., Iannacone, M. D., Vincent, M., & Chen, Q. (2019). A survey of intrusion detection systems leveraging host data. *ACM Computing Surveys*, *52*(6), 1–35. https://doi.org/10.1145/3344382
10. Taddeo, M., & Floridi, L. (2018). Cybersecurity, ethics, and the governance of artificial intelligence. *Minds and Machines*, *28*(4), 629–644. https://doi.org/10.1007/s11023-018-9483-3