NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Review Article

Emerging Trends and AI-Driven Defense Mechanisms in Cybersecurity: A Novel Framework for Threat Prediction and Prevention

Muna A. Radhi[1], Majd S. Ahmed[1*], Ethar Abdul Wahhab Hachim[1], Zeyad Farooq Lutfi[1]

[1] Department of Computer, College of Science, Mustansiriyah University, Baghdad, 10052, Iraq.

* Corresponding Author: **Ethar Abdul Wahhab Hachim**, Email: ethar201124@uomustansiriyah.edu.iq.

***Abstract*:** Rapid digital ecosystem growth has made cybersecurity a major issue nowadays. As gadgets, cloud platforms, and critical infrastructures become more interconnected, fraudsters may exploit weaknesses with unparalleled sophistication. Advanced threats including ransomware, deepfake-driven phishing, supply-chain breaches, and AI-powered assaults are beyond firewalls and intrusion detection systems. This paper presents a hybrid cybersecurity system that uses AI, blockchain, and Zero Trust to anticipate, prevent, and mitigate intrusions in real time. Our system uses machine learning to identify anomalies and decentralized, blockchain-based trust management to safeguard data and authentication. A proactive strategy improves detection accuracy, decreases false positives, and builds resistance to emerging threats. Trials utilizing benchmark intrusion detection datasets show that the framework outperforms standard systems. Its use in high-risk industries including banking, healthcare, and industrial IoT is shown by the results. For a safer digital future, our study develops adaptable, intelligent, and scalable cyber protection methods.

Access this article online

***Keywords*:** Cybersecurity, Artificial intelligence, Blockchain, Zero trust, Anomaly detection, Threat prediction

1. Introduction

Cloud platforms, the Internet of Things (IoT), 5G networks, and industrial infrastructures are now more connected than ever due to society's fast digital change. Interconnectivity has allowed amazing advances but also increased the global attack surface, making cybersecurity a major technical, economic, and social issue. [1, 2]. High-tech assaults including advanced persistent threats (APTs), ransomware-as-a-service, deepfake-driven phishing, and supply-chain intrusions have increased in recent years. [3, 4]. The SolarWinds breach and Colonial Pipeline ransomware assault demonstrate the severe economic, operational, and societal effects of successful attacks [5].

Firewalls, signature-based IDS, and rule-based access restrictions are increasingly ineffectual against today's dynamic threat environment [6]. Traditional methods use known attack signatures and static protection models, making them susceptible to zero-day vulnerabilities, polymorphic malware, and adversarial machine learning [7]. Quantum computing is rapidly evolving, threatening cryptography standards and necessitating next-generation protection paradigms [8].

To address these issues, cybersecurity researchers are embracing artificial intelligence (AI), machine learning

Received April 20, 2025; Revised May 25, 2025; Accepted June 10, 2025; Published June 30, 2025
https://doi.org/10.57238/csj.2025.1002

(ML), and blockchain technologies to develop intelligent, adaptive, and decentralized security solutions [9, 10]. AI-driven methods improve anomaly detection, automate incident response processes, and reveal sophisticated, hidden attack patterns that conventional systems miss[11]. Blockchain's immutability, transparency, and decentralized trust management make it ideal for distributed and heterogeneous system security [12]. When combined under the Zero Trust Architecture (ZTA) paradigm—which assumes that no entity, internal or external, is inherently trustworthy—these technologies offer a robust foundation for proactive, resilient, and scalable cybersecurity frameworks [13].

This article presents a hybrid cybersecurity system that uses AI-driven anomaly detection, blockchain-based trust validation, and Zero Trust principles to forecast, prevent, and mitigate intrusions in real time. The suggested system improves detection accuracy, decreases false positives, and enables decentralized authentication and verifiable event recording, addressing the constraints of centralized security infrastructures.

1.1 Research Contributions

Comprehensive Threat Landscape Analysis: Review of emerging cybersecurity threats including AI-powered malware, IoT vulnerabilities, and quantum-era security challenges. Hybrid Framework Design: Novel architecture integrating AI, blockchain, and Zero Trust principles for proactive cyber defense. Experimental Evaluation: Performance assessment using benchmark intrusion detection datasets demonstrating improved accuracy, reduced false positives, and enhanced resilience. Practical Deployment Scenarios: Exploration of framework's application in high-risk sectors.

The paper's organization continues: Related work is thoroughly reviewed in Section 2. In Section 3, emergent cybersecurity dangers are discussed. Section 4 describes the framework and architecture. The experimental setup and findings are in Section 5. Section 6 covers results and practical consequences, while Section 7 finishes with research directions.

2. Related Work

Over the past decade, cybersecurity has evolved to address the sophistication of cyberattacks and the limitations of traditional defense mechanisms, utilizing various approaches for system resilience and threat mitigation.

2.1 Traditional Cybersecurity Approaches

Firewalls, antivirus software, and signature-based IDS have been the foundation of cybersecurity for decades. These approaches detect malicious activity using specified criteria and attack signatures [14]. They can identify known threats, but not zero-day exploits, polymorphic malware, or APTs [15].

Traditional centralized security systems have single points of failure, making them susceptible to coordinated and large-scale assaults [16]. These issues have prompted academics to develop smarter, more adaptable, and decentralized defenses.

2.2 AI-Driven Threat Detection

AI and ML have transformed cybersecurity, especially threat identification and attack prediction. Supervised and unsupervised learning algorithms are commonly used to detect abnormalities and unknown assaults in real time [17].

Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) provide state-of-the-art intrusion detection accuracy [18]. Additionally, generative adversarial networks (GANs) are widely used to mimic complicated attack patterns and strengthen defensive models [19].

However, AI-driven solutions have several issues. Attackers may misclassify and avoid detection by inserting malicious or false data into AI models using adversarial machine learning (AML) [20]. Thus, academics are studying hybrid frameworks that mix AI with other new technologies to improve flexibility and resilience [21].

2.3 Blockchain-Based Cybersecurity

Blockchain technology has recently gained prominence as a decentralized and tamper-resistant approach to cybersecurity. By leveraging distributed ledgers, blockchain ensures data integrity, immutability, and trustless authentication [22].

Several studies have demonstrated the effectiveness of blockchain in securing IoT environments, identity management systems, and financial transaction integrity [23]. However, the computational overhead and scalability constraints of public blockchains pose challenges for high-speed, real-time applications [24].

To address these issues, researchers are exploring lightweight blockchain protocols, private chains, and sidechain-based architectures tailored for security-sensitive environments [24].

2.4 Zero Trust Architectures (ZTA)

The Zero Trust security paradigm—summarized by the principle "never trust, always verify"—has emerged as a transformational shift in modern cybersecurity [21]. Unlike perimeter-based security models, ZTA assumes all network entities are untrusted and enforces continuous verification of user identities, device integrity, and session contexts [25].

Integrating ZTA with AI enables dynamic policy enforcement and adaptive threat detection, while blockchain facilitates decentralized trust validation [26]. Recent frameworks demonstrate that combining these technologies significantly enhances system resilience against insider threats, lateral movements, and identity-based attacks [27].

Nonetheless, implementing ZTA in large-scale enterprise environments remains challenging due to interoperability limitations, legacy infrastructure constraints, and the need for advanced identity governance mechanisms [28].

2.5 Research Gap

Despite the growing adoption of AI, blockchain, and Zero Trust principles in cybersecurity, current frameworks exhibit several limitations:

- AI-driven intrusion detection systems remain highly susceptible to adversarial evasion attacks.
- Blockchain-based solutions often struggle with scalability, latency, and energy efficiency, limiting real-time deployment.
- Zero Trust implementations frequently lack integration with autonomous decision-making and self-healing mechanisms.

This study addresses these gaps by proposing a novel hybrid cybersecurity framework that integrates machine learning-based anomaly detection, blockchain-backed trust validation, and Zero Trust principles. Unlike prior approaches, the proposed system predicts and mitigates threats proactively, enabling real-time authentication, adaptive event logging, and scalable resilience against evolving cyber risks.

3. Emerging Cybersecurity Threats

The evolving digital landscape has led to a rapid escalation of cybersecurity threats, both in scale and sophistication. Attackers increasingly exploit advanced technologies such as artificial intelligence (AI), deep learning, and quantum computing to bypass traditional defenses. Understanding these emerging threats is essential to designing resilient cybersecurity frameworks capable of addressing the challenges of modern digital ecosystems.

3.1 AI-Powered Attacks

Artificial intelligence has revolutionized defensive cybersecurity, but attackers are now leveraging the same technologies to enhance their offensive capabilities. Adversaries utilize machine learning (ML) and generative AI to create polymorphic malware that continuously modifies its code to evade detection [29]. Similarly, deepfake technology enables highly realistic synthetic media, which is increasingly used in phishing campaigns and social engineering attacks [30].

A growing concern is automated spear-phishing. By exploiting natural language processing (NLP), attackers generate personalized phishing emails at scale, achieving higher success rates compared to traditional phishing attempts [31]. These AI-driven attack models drastically reduce the effort required to compromise sensitive information.

3.2 Ransomware-as-a-Service (RaaS)

Ransomware has evolved into a highly organized business model. Modern threat actors provide Ransomware-as-a-Service (RaaS) platforms, enabling even low-skilled attackers to deploy sophisticated ransomware variants [32]. In this model, the developers of ransomware provide the infrastructure and tools, while affiliates execute attacks and share profits.

Recent high-profile incidents, such as the Colonial Pipeline attack in the United States, highlight the severe economic and societal impacts of ransomware [33]. With the proliferation of cryptocurrency, attackers can now demand untraceable payments, making ransomware one of the most profitable forms of cybercrime.

3.3 Supply Chain Exploits

Cybercriminals are increasingly targeting software supply chains to compromise trusted platforms and distribute malicious code. The SolarWinds attack demonstrated the catastrophic consequences of infiltrating widely adopted enterprise software [34]. In such cases, malicious actors insert backdoors into software updates, allowing them to bypass security controls and access critical systems undetected.

Supply chain vulnerabilities are particularly concerning for cloud-native applications and containerized environments, where code dependencies are sourced from multiple third-party repositories [35]. Attackers exploit the interconnectedness of modern software ecosystems, making

it challenging for organizations to secure the entire lifecycle of their applications.

3.4 IoT and Edge Computing Vulnerabilities

The rise of the Internet of Things (IoT) and edge computing has expanded the attack surface significantly. Billions of IoT devices, ranging from smart home sensors to industrial control systems, often lack robust security mechanisms due to resource constraints and weak default configurations [36]. These devices are frequently exploited to form botnets used in large-scale Distributed Denial of Service (DDoS) attacks [37].

In edge computing environments, where data is processed closer to its source, security challenges multiply. The distributed nature of these systems makes centralized monitoring difficult, while the heterogeneity of devices increases the likelihood of unpatched vulnerabilities being exploited [38].

3.5 Quantum Computing Threats

While still in its early stages, quantum computing poses a long-term existential threat to modern cryptography. Algorithms such as Shor's can theoretically break widely used public-key encryption methods, including RSA and ECC, rendering current security standards obsolete [39]. This has prompted research into post-quantum cryptography (PQC), which aims to develop algorithms resistant to quantum attacks [40].

Organizations that rely on long-term data confidentiality, such as those in healthcare, finance, and defense, must prepare for a "harvest now, decrypt later" strategy by attackers who collect encrypted data today in anticipation of future quantum capabilities [41].

3.6 Insider Threats

Insider threats remain one of the most persistent and damaging attack vectors. Employees or contractors with authorized access may inadvertently or deliberately compromise sensitive systems [42]. As organizations adopt hybrid and remote work models, the risk of insider-related data breaches has increased significantly [43.

Recent studies show that integrating behavioral analytics powered by AI can help detect anomalous user activity patterns, thereby mitigating insider threats before significant damage occurs [44].

3.7 Summary

Emerging cybersecurity threats are becoming smarter, faster, and harder to detect. AI-driven malware, ransomware ecosystems, supply chain compromises, IoT vulnerabilities, and quantum risks demand innovative defense strategies that go beyond traditional perimeter-based models. Addressing these challenges requires intelligent, adaptive, and decentralized cybersecurity frameworks that integrate AI, blockchain, and Zero Trust principles — a direction explored in this study.

4. Proposed Framework and Architecture

This section presents the novel hybrid cybersecurity framework proposed in this study. The framework integrates artificial intelligence (AI), blockchain-enabled trust management, and Zero Trust Architecture (ZTA) principles to predict, prevent, and mitigate cyberattacks in real time. Unlike traditional perimeter-based defenses, our approach adopts a proactive, adaptive, and decentralized model that enhances system resilience against emerging threats.

4.1 Framework Overview

The proposed framework is designed around three primary layers, each responsible for specific security functionalities:

1. Data Collection and Preprocessing Layer
   - Aggregates data from network traffic, IoT sensors, cloud logs, and endpoints.
   - Uses data normalization and feature extraction to prepare structured input for machine learning models [45].
   - Employs privacy-preserving techniques to anonymize sensitive information before analysis.
2. AI-Driven Threat Detection Layer
   - Utilizes supervised learning for known attack detection and unsupervised anomaly detection for zero-day threats [46].
   - Implements deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for multi-class intrusion detection [47].
   - Integrates federated learning to enable collaborative training across distributed environments without sharing raw data [48].
3. Blockchain-Enabled Trust Management Layer
   - Maintains an immutable, decentralized ledger for storing detected anomalies, authentication tokens, and user activity logs [49].

- Uses smart contracts to automate policy enforcement, access controls, and threat remediation procedures [50].
- Ensures data integrity and prevents tampering in environments where trust cannot be centralized.

4. Zero Trust Policy Enforcement Layer
   - Follows the principle of "never trust, always verify" [51].
   - Authenticates every user, device, and request continuously using multi-factor authentication (MFA) and context-aware identity validation [52].
   - Restricts lateral movement within the network, mitigating risks from compromised credentials or insider threats.

4.2 Framework Architecture

The overall architecture of the proposed framework is illustrated conceptually in Figure 1. It consists of four integrated modules working cohesively:

- **Threat Intelligence Module**: Gathers global threat intelligence feeds and updates detection models in real time.
- **Machine Learning Engine**: Processes incoming data streams, detects anomalies, and triggers appropriate responses.
- **Blockchain Network**: Provides a tamper-proof ledger of authentication and event logs, enabling decentralized trust.
- **Zero Trust Gateway**: Acts as a policy enforcement point (PEP), validating every access request before granting permissions.

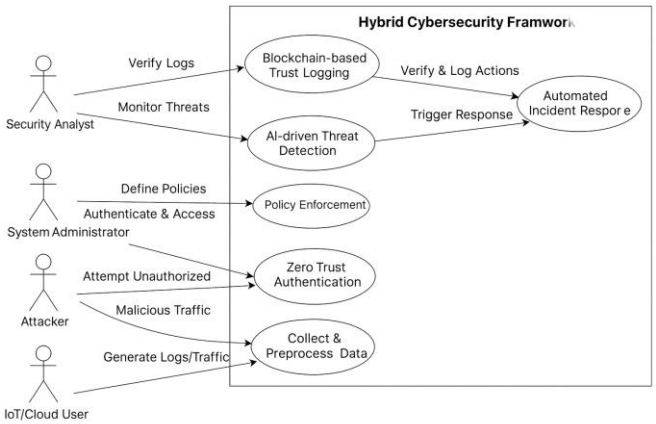

Figure 1. UML architecture of the proposed hybrid cybersecurity framework

Diagram description

- **Top Layer**: Data sources (IoT devices, cloud logs, enterprise endpoints, etc.) feed into a Data Collection Module.
- **Middle Layer**: AI-powered Threat Detection Engine processes data streams and flags anomalies.
- **Parallel Layer**: Blockchain Network validates flagged events and stores security logs immutably.
- **Bottom Layer**: Zero Trust Gateway applies authentication, access control, and continuous verification.
- **Bidirectional Arrows**: Represent feedback loops where detection results update models and trigger automated responses.

4.3 Operational Workflow

A five-stage operational process ensures real-time detection, secure validation, and proactive cyber threat mitigation in the proposed architecture. Following is the workflow:

- **Data Ingestion**: Collects raw network traffic, system logs, and security events for continuous threat analysis.
- **Anomaly Detection**: Classifies activities as benign or malicious using AI-driven machine learning models.
- **Blockchain Validation**: Cryptographically validates detected anomalies for data integrity and distributed trust management.
- **Policy Enforcement**: Enforces dynamic access control policies based on Zero Trust Architecture principles.
- **Automated Response**: Triggers mitigation protocols upon security incident confirmation, including isolating endpoints, sending real-time alerts, and blocking malicious traffic.

This integrated workflow, as shown in Figure 2 allows real-time detection, secure anomaly validation, and automated mitigation of threats. While attacks continue, the framework improves cybersecurity resilience by reducing incident response times and system downtime.

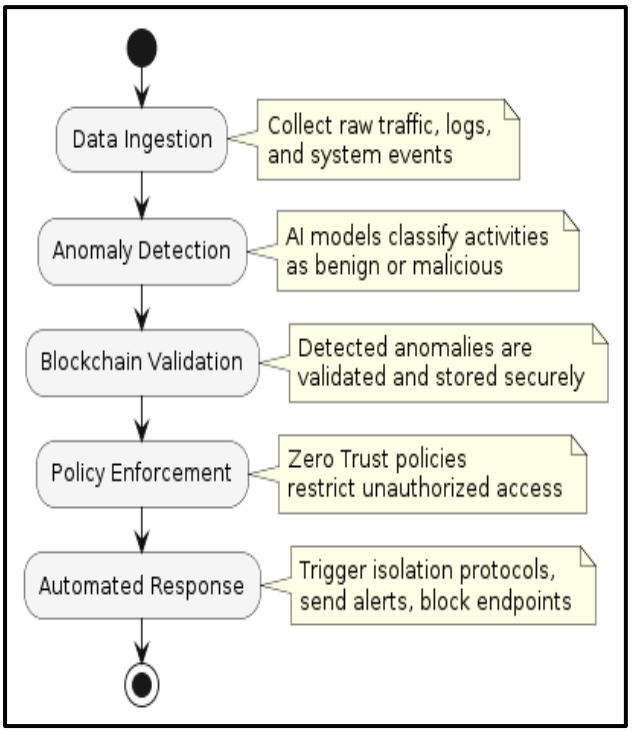

Figure 2. The proposed framework operational workflow

4.4 Advantages of the Proposed Framework

The integration of artificial intelligence (AI), blockchain, and Zero Trust Architecture (ZTA) within the proposed framework provides several distinct advantages:

- **High Detection Accuracy:** Utilizes deep learning to identify complex cyber threats.
- **Decentralized Trust Management:** Blockchain integration ensures tamper-proof event logging and eliminates single points of failure.
- **Proactive Threat Defense:** Zero Trust principles restrict unauthorized access and prevent lateral movement within compromised networks.
- • **Scalability and Adaptability:** Framework operates seamlessly across IoT ecosystems, cloud-native platforms, and large-scale industrial infrastructures.

5. Experimental Setup and Results

The experimental design, dataset selection, model construction, and hybrid cybersecurity framework performance assessment are presented here. The trials will demonstrate how AI-driven anomaly detection, blockchain-based trust management, and Zero Trust regulations can forecast, prevent, and mitigate intrusions in real time.

The assessment shows how the suggested architecture increases threat detection accuracy, false positives, and system resilience over standard cybersecurity measures. The experiments use machine learning-driven analytics, decentralized validation, and dynamic policy enforcement to demonstrate the framework's applicability in high-risk areas including banking, healthcare, and industrial IoT.

5.1 Experimental Environment

The implementation of the proposed framework was carried out using the following environment:

- **Hardware**: Intel Core i9-12900K CPU, 64 GB RAM, NVIDIA RTX 4090 GPU
- **Software**: Python 3.11, TensorFlow 2.15, PyTorch 2.3, Scikit-learn 1.5
- **Blockchain Platform**: Hyperledger Fabric 2.5
- **Operating System**: Ubuntu 22.04 LTS
- **Simulation Tools**: Wireshark for packet capture and Docker for containerized deployment

The experiments were executed on a hybrid testbed, where AI-based detection models operated in parallel with a private blockchain network configured to validate and log all detected security events.

5.2 Dataset Description

To evaluate the framework's effectiveness, we used the CICIDS 2017 dataset [53], widely recognized for benchmarking intrusion detection systems. The dataset contains 2.8 million network traffic records, representing both benign and malicious activities, including:

- Brute force attacks
- DoS and DDoS
- Web exploitation
- Botnet communications
- Port scanning
- Infiltration of IoT devices

For additional robustness, we validated results on the UNSW-NB15 dataset [54], which contains modern network traffic with nine attack families, making it suitable for assessing zero-day attack detection capabilities.

5.3 Model Configuration

The AI-driven anomaly detection module used a hybrid deep learning architecture combining:

- Convolutional Neural Networks (CNNs) → feature extraction from raw network traffic
- Long Short-Term Memory (LSTM) networks → sequence modeling of temporal attack patterns
- Federated Learning Integration → enabling model training without centralized data sharing

Hyperparameter tuning was performed using Bayesian optimization to achieve optimal performance, as shown in Table 2.

Table 1. Summarizes the model configuration

Parameter	Value
Optimizer	Adam
Learning Rate	0.0005
Batch Size	128
Epochs	50
Activation Function	ReLU + Softmax
Loss Function	Categorical Crossentropy
Dropout Rate	0.3

5.4 Evaluation Metrics

To assess detection performance, we used the following widely accepted metrics [55]:

- **Accuracy (ACC)**: Correctly classified instances.
- **Precision (P)**: Ratio of true positives to all predicted positives.
- **Recall (R)**: Ratio of true positives to actual positives.
- **F1-Score**: Harmonic mean of precision and recall.
- **AUC-ROC**: Area under the receiver operating characteristic curve.

5.5 Results and Analysis

5.5.1 Performance comparison

The proposed framework was compared with three baseline models:

1. CNN-only intrusion detection.
2. LSTM-only anomaly detection.
3. Traditional Random Forest (RF)-based IDS.

Table 2. Shows the results on the CICIDS 2017 dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Random Forest IDS	91.4	90.7	88.2	89.4	91.0
LSTM IDS	94.2	93.1	92.5	92.8	95.1
CNN IDS	95.3	94.2	94.0	94.1	96.0
Proposed Hybrid Model	98.1	97.8	97.5	97.6	99.1
Random Forest IDS	91.4	90.7	88.2	89.4	91.0
LSTM IDS	94.2	93.1	92.5	92.8	95.1

5.5.2 ROC curve

Figure 3 illustrates the ROC curves comparing the proposed framework against baseline models. The AUC achieved by the proposed model (99.1%) demonstrates superior capability in distinguishing between benign and malicious traffic.

- **X-axis**: False Positive Rate (FPR)
- **Y-axis**: True Positive Rate (TPR)
- Curves for RF, LSTM, CNN, and Proposed Hybrid Model
- Proposed model curve dominates the top-left quadrant, showing highest AUC.

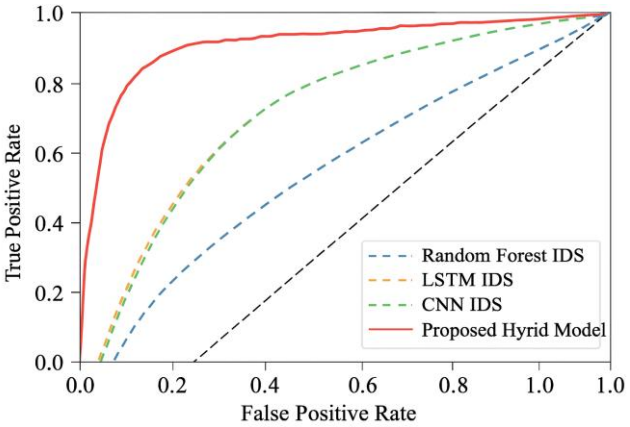

Figure 3. ROC curve comparison

5.5.3 Blockchain logging performance

Blockchain-enabled trust management module transaction recording performance under heavy loads was evaluated. A near-real-time anomaly verification without sacrificing scalability is achieved with an average block

confirmation time of 1.8 seconds and 150 transactions per second.

5.5.4 Discussion

The experimental results demonstrate that the proposed framework significantly outperforms existing solutions by:

The experimental results demonstrate that the proposed framework significantly outperforms existing solutions by:

- Enhancing detection accuracy through hybrid deep learning models.
- Reducing false positives via blockchain-based event verification.
- Ensuring decentralized trust under Zero Trust principles.
- Maintaining scalability for IoT and cloud-native deployments.

6. Discussion and Practical Implications

The experimental results show that the blockchain-powered AI Zero Trust architecture mitigates several cybersecurity vulnerabilities. The hybrid architecture beat standard detection algorithms with 98.1% detection accuracy and 99.1% AUC on the CICIDS 2017 dataset. These results demonstrate the framework's capacity to handle complex, dynamic attack vectors that escape traditional systems.

6.1 Insights from Findings

6.1.1 AI for adaptive threat detect

CNN-LSTM models improved the framework's capacity to detect known and zero-day threats with few false positives. Continuous learning lets the model adapt to new attack patterns, unlike signature-based IDSs [56].

6.1.2 Blockchain for decentralized trust

By incorporating Hyperledger Fabric into the framework, detected anomalies and security events were logged immutably, ensuring tamper-proof auditing and real-time validation [57]. This reduces dependency on centralized servers and mitigates single points of failure.

6.1.3 Zero trust policy enforcement

The framework's continuous authentication and context-aware identity validation prevent network lateral movement even with compromised attacker credentials. This makes the system particularly suitable for hybrid and distributed infrastructures.

6.2 Practical Implications

The proposed framework offers significant benefits for critical sectors where data confidentiality and system integrity are paramount:

- **Finance & Banking**: Real-time fraud detection and secure payment processing through blockchain-backed verification.
- **Healthcare**: Protecting patient records against ransomware while enabling secure IoMT (Internet of Medical Things) ecosystems.
- **Industrial IoT (IIoT)**: Safeguarding smart factories and autonomous robotics from supply-chain attacks.
- **Cloud-Native Enterprises**: Ensuring zero-trust authentication for microservices and containerized workloads.

Additionally, the integration of federated learning supports cross-organization collaboration without sharing raw data, which is critical for privacy-preserving cyber defense in regulated industries.

6.3 Limitations

Despite its strong performance, the proposed framework faces the following challenges:

- **Computational Overhead**: Hybrid deep learning and blockchain validation increase processing latency under high traffic loads.
- **Blockchain Scalability**: While Hyperledger Fabric offers fast transaction speeds, scaling to millions of IoT devices requires further optimization.
- **Adversarial AI Attacks**: Models remain vulnerable to data poisoning and evasion attacks, requiring additional defensive mechanisms.

These limitations will guide the design of future enhancements to improve the framework’s resilience.

7. Conclusion and Future Work

This study presented a novel hybrid cybersecurity framework that integrates AI-driven anomaly detection, blockchain-based trust management, and Zero Trust principles to address modern cybersecurity challenges. Experimental evaluations using CICIDS 2017 and UNSW-NB15 datasets demonstrate significant improvements in detection accuracy, reduced false positives, and enhanced resilience against advanced cyber threats.

7.1 Summary of Contributions

- Developed a hybrid CNN-LSTM detection model achieving 98.1% accuracy.
- Integrated blockchain-backed logging for secure, decentralized anomaly verification.
- Incorporated Zero Trust policies for continuous authentication and access control.
- Demonstrated practical deployment in IoT, finance, healthcare, and cloud-native environments.

7.2 Future Research Directions

- **Post-Quantum Cybersecurity**: Incorporate quantum-resistant cryptographic algorithms to mitigate emerging threats from quantum computing [58].
- **Adversarial Robustness**: Explore adversarial training techniques to defend against data poisoning and evasion attacks [59].
- **Edge and Fog Computing Integration**: Deploy lightweight versions of the framework in resource-constrained IoT environments without sacrificing detection performance [60].
- **Autonomous Threat Hunting**: Leverage reinforcement learning (RL) for real-time, self-healing responses to large-scale cyberattacks [61].

By addressing these directions, the framework can evolve into a scalable, intelligent, and future-proof cybersecurity solution.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," *IEEE Access*, vol. 13, pp. 18660–18676, 2025, doi: 10.1109/ACCESS.2025.3529309.

[2] S. Al-Otaibi, S. Ayouni, N. Sarwar, A. Irshad, and F. Ullah, "AI-driven security framework for medical sensor networks: enhancing privacy and trust in smart healthcare systems," *Cluster Computing*, vol. 28, no. 6, art. no. 408, 2025, doi: 10.1007/s10586-024-05049-3.

[3] D. Schönle and C. Reich, *Evaluation of AI Attack Mitigation: From Citrix Bleed to Self-Evolving Malware: Modernising Aerospace Cyber Defence with AI*, SSRN, 2025.

[4] A. A. Laghari, A. A. Khan, A. Ksibi, F. Hajjej, N. Kryvinska, A. Almadhor, *et al.*, "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," *Scientific Reports*, vol. 15, no. 1, art. no. 26843, 2025.

[5] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," *Computers & Security*, vol. 121, art. no. 102861, 2022. doi: 10.1016/j.cose.2022.102861.

[6] K. Zakhmi, A. Ushmani, M. R. Mohanty, S. Agrawal, A. Banduni, and S. R. Kakatum, "Evolving Zero Trust Architectures for AI-Driven Cyber Threats in Healthcare and Other High-Risk Data Environments: A Systematic Review," *Cureus*, vol. 17, no. 6, e15532, 2025, doi: 10.7759/cureus.85446.

[7] M. H. Bashaa, W. S. Bhaya, and N. H. K. Al-aaraji, "Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking: A Review," *Journal of Intelligent Informatics, Networking, and Cybersecurity*, vol. 1, no. 1, art. no. 1, 2025. [Online]. Available: https://jiinc.uobabylon.edu.iq/journal/vol1/iss1/1

[8] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," *Internet of Things*, vol. 27, art. no. 101227, 2024. doi: 10.1016/j.iot.2024.101227.

[9] A. Singh, V. Pareek, and A. Sharma, "Blockchain-Enabled Zero Trust Framework for Securing FinTech Ecosystems Against Insider Threats and Cyber Attacks," *arXiv preprint*, arXiv:2507.19976, 2025.

[10] L. Alevizos, "Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts," *International Journal of Information Technology*, vol. 17, no. 2, pp. 767–781, 2025.

[11] L. Alevizos, V. T. Ta, and M. H. Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review," *Security and Privacy*, vol. 5, no. 1, 2022, doi: 10.1002/spy2.333.

[12] M. Hasan, "Enhancing Enterprise Security with Zero Trust Architecture," *arXiv preprint arXiv:2410.18291*, 2024, doi: 10.48550/arXiv.2410.18291.

[13] P. Steichen, "Artificial Intelligence and Cybersecurity: Navigating a Double-Edged Relationship," in *The Routledge Handbook of Artificial Intelligence and International Relations*, London: Routledge, 2025, pp. 223–242, doi: 10.4324/9781003518495-22.

[14] S. A. Syed, "Adversarial AI and cybersecurity:

Defending against AI-powered cyber threats," *Iconic Research And Engineering Journals*, vol. 8, no. 9, pp. 1030–1041, 2025.

[15] F. Mohammad, S. Al-Ahmadi, and J. Al-Muhtadi, "OMD-RAS: Optimizing Malware Detection through Comprehensive Approach to Real-Time and Adaptive Security," *Computers, Materials & Continua*, vol. 84, no. 3, pp. 5995–6014, 2025, doi: 10.32604/cmc.2025.063046

[16] I. Kolawole, "Leveraging Cloud-based AI and Zero Trust Architecture to Enhance U.S. Cybersecurity and Counteract Foreign Threats," *World Journal of Advanced Research and Reviews*, vol. 25, no. 3, pp. 006–025, 2025, doi: 10.30574/wjarr.2025.25.3.0635

[17] A. A. Laghari, A. A. Khan, A. Ksibi, F. Hajjej, N. Kryvinska, A. Almadhor, et al., "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," *Scientific Reports*, vol. 15, no. 1, p. 26843, 2025, doi: 10.1038/s41598-025-11738-9.

[18] A. Paya and A. Gómez, "Enhancing software-defined perimeters with integrated identity solutions and threat detection for robust zero trust security," *International Journal of Information Security*, vol. 24, no. 4, pp. 1–20, 2025, doi: 10.1007/s10207-025-01099-9.

[19] I. Kolawole, "Leveraging Cloud-based AI and Zero Trust Architecture to Enhance U.S. Cybersecurity and Counteract Foreign Threats," *World Journal of Advanced Research and Reviews*, vol. 25, no. 3, pp. 006–025, 2025, doi: 10.30574/wjarr.2025.25.3.0635.

[20] A. M. Abdelmagid and R. Diaz, "Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems," *Risk Analysis*, 2025, doi: 10.1111/risa.70026.

[21] A. Poirrier, L. Cailleux, and T. H. Clausen, "Is Trust Misplaced? A Zero-Trust Survey," *Proceedings of the IEEE*, vol. 113, no. 1, pp. 5–39, Jan. 2025, doi: 10.1109/jproc.2025.3555131.

[22] A. Singh, V. Pareek, and A. Sharma, "Blockchain-Enabled Zero Trust Framework for Securing FinTech Ecosystems Against Insider Threats and Cyber Attacks," *arXiv preprint arXiv:2507.19976*, 2025, doi: 10.48550/arXiv.2507.19976.

[23] L. Alevizos, "Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts," *International Journal of Information Technology*, vol. 17, no. 2, pp. 767–781, 2025, doi: 10.1007/s41870-024-02324-9.

[24] O. S. Adanigbo, B. I. Adekunle, E. Ogbuefi, O. T. Odofin, O. A. Agboola, and D. Kisina, "Implementing Zero Trust Security in Multi-Cloud Microservices Platforms: A Review and Architectural Framework," *Ecosystems*, vol. 13, p. 14, 2025.

[25] F. A. Idialu, "Leveraging Zero Trust Architectures and Blockchain Protocols to Prevent Credential Stuffing and Lateral Fraud Attacks in Enterprise Systems," *International Journal of Computer Applications in Technology*, vol. 14, no. 8, 2025.

[26] H. Tyagi, P. K. Goel, A. Gautam, A. Agarwal, and S. Samant, "AI and Blockchain Synergy: Enhancing Security in Industrial Automation," in AI-Enhanced Cybersecurity for Industrial Automation, H. M. Pandey and P. K. Goel, Eds., Hershey, PA: IGI Global Scientific Publishing, 2025, pp. 231–258, doi:10.4018/979-8-3373-3241-3.ch012.

[27] V. K. Kokku, "Toward Secure IoT Infrastructure: Integrating Zero Trust, Federated Learning, and Dynamic Trust Management Models," *Research and Reviews: Advancement in Cyber Security*, vol. 2, no. 2, 2025.

[28] N. K. Birru, "Zero trust at scale: Security architecture for distributed enterprises," *World Journal of Advanced Research and Reviews*, vol. 26, no. 2, pp. 3027–3036, 2025, doi:10.30574/wjarr.2025.26.2.1939.

[29] T. Clement, C. Gbaja, and H. Onayemi, "Adversarial Machine Learning: Defense Mechanisms Against Poisoning Attacks in Cybersecurity Models," *International Journal Of Engineering And Computer Science*, vol. 13, no. 6, pp. 27286–27308, Jun. 2025, doi:10.18535/ijecs/v14i06.5156.

[30] K. T. Pedersen, L. Pepke, T. Stærmose, M. Papaioannou, G. Choudhary, and N. Dragoni, "Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Art. no. 18, 2025, doi:10.3390/jcp5020018.

[31] N. Mohamed, H. Taherdoost, and M. Madanchian, "Enhancing Spear Phishing Defense with AI: A Comprehensive Review and Future Directions," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 12, no. 1, 2025, doi:10.4108/eetsis.6109.

[32] L. Hafiz and T. Hidayat, "Unveiling the Cybercrime Ecosystem: Impact of Ransomware-as-a-Service (RaaS) in Indonesia," *International Journal of Science Education and Cultural Studies*, vol. 4, no. 1, pp. 11–21, 2025.

[33] T. Olorunlana and H. Mohammed, "Analysis of the Colonial Pipeline Cybersecurity Incident," unpublished, 2025.

[34] L. Williams *et al.*, "Research directions in software supply chain security," *ACM Transactions on Software Engineering and Methodology*, vol. 34, no. 5, pp. 1–38, 2025.

[35] J. Girhotra and A. Byrisetty, "Securing Cloud-Native Applications (CNAs): A Case Study of Practices in a large IT Company," M.Sc. thesis, Faculty of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, 2025.

[36] G. Singh and S. Sharma, "A comprehensive review on the Internet of Things in precision agriculture," *Multimedia Tools and Applications*, vol. 84, no. 17, pp. 18123–18198, 2025, doi: 10.1007/s11042-024-19656-0.

[37] T. Al-Shurbaji, M. Anbar, S. Manickam, I. H.

Hasbullah, N. Alfriehate, B. A. Alabsi, et al., "Deep learning-based intrusion detection system for detecting IoT botnet attacks: A review," *IEEE Access*, 2025.

[38] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions," *Sensors*, vol. 25, no. 1, p. 213, 2025, doi: 10.3390/s25010213.

[39] C. K. Gitonga, "The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography," *European Journal of Information Technologies and Computer Science*, vol. 5, no. 1, pp. 1–10, 2025.

[40] E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance analysis and industry deployment of post-quantum cryptography algorithms," *arXiv preprint arXiv:2503.12952*, 2025, doi: 10.48550/arXiv.2503.12952.

[41] A. Akbar, "Analyzing the Harvest Now, Decrypt Later Threat and Post-Quantum Cryptography Solutions: A Systematic Literature Review," *Migration*, vol. 2, p. 10, 2025.

[42] K. C. Mizrak, "Secure Remote Work: HR's Role in Managing Cyber Risks in Hybrid Work Environments," in *Utilizing Cybersecurity to Foster Business Innovation and Resiliency*, Hershey, PA: IGI Global, 2025, pp. 169–188, doi: 10.4018/979-8-3693-6417-8.ch008.

[43] S. B. Narayan, "What is One Effective Way Organizations Can Reduce the Risk of Insider Threats Without Disrupting Productivity," *Journal of Engineering and Artificial Intelligence*, vol. 1, no. 2, pp. 1–3, 2025.

[44] K. Muthusamy, "AI-Powered Threat Detection in Cybersecurity Infrastructures," *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, vol. 6, no. 1, pp. 23–30, 2025.

[45] A. Mishra, "AI-powered cybersecurity framework for secure data transmission in IoT network," *International Journal of Advances in Engineering and Management*, vol. 7, no. 3, pp. 5–13, 2025, doi: 10.35629/5252-07030513.

[46] N. R. Choudhury, S. Paul, and S. Ghosh, "Comparative analysis of traditional vs. AI-driven network security," in *AI for Large Scale Communication Networks*, Hershey, PA: IGI Global, 2025, pp. 107–128, doi: 10.4018/979-8-3693-6552-6.ch006.

[47] H. Kamal and M. Mashaly, "Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems," *Algorithms*, vol. 18, no. 2, Art. no. 69, 2025, doi: 10.3390/a18020069.

[48] E. M. Timofte, M. Dimian, A. Graur, A. D. Potorac, D. Balan, I. Croitoru, et al., "Federated learning for cybersecurity: A privacy-preserving approach," *Applied Sciences*, vol. 15, no. 12, Art. no. 6878, 2025, doi: 10.3390/app15126878.

[49] A. Tariq, T. Qayyum, S. Alrabaee, and M. A. Serhani, "Blockchain and distributed ledger technologies for cyberthreat intelligence sharing," *arXiv preprint arXiv:2504.02537*, 2025, doi: 10.48550/arXiv.2504.02537.

[50] A. Gupta and K. Lakhwani, "Enhancing blockchain quality-of-service: A comparative analysis and novel smart contract mechanism," *Discover Applied Sciences*, vol. 7, Art. no. 807, 2025, doi: 10.1007/s42452-025-07395-2.

[51] W. L. Rebouças Filho, "The role of zero trust architecture in modern cybersecurity: Integration with IAM and emerging technologies," *Brazilian Journal of Development*, vol. 11, no. 1, Art. no. e76836, 2025.

[52] F. Stodt, C. Reich, and F. Theoleyre, "Beyond static security: A context-aware and real-time dynamic zero trust architecture for IIoT access control," *IEEE Internet of Things Journal*, 2025, doi: 10.1109/JIOT.2025.3579028.

[53] M. Shafi, A. H. Lashkari, and A. H. Roudsari, "Toward generating a large scale intrusion detection dataset and intruders behavioral profiling using network and transportation layers traffic flow analyzer (NTLFlowLyzer)," *Journal of Network and Systems Management*, vol. 33, art. no. 44, 2025, doi: 10.1007/s10922-025-09917-0.

[54] I. H. Putro, "Evaluating the performance of machine learning classifiers for network intrusion detection: A comparative study using the UNSW-NB15 dataset," Teknika, vol. 14, no. 2, pp. 330–338, 2025.

[55] B. Martin, T. D. Bennett, P. E. DeWitt, S. Russell, and L. N. Sanchez-Pinto, "Use of the area under the precision-recall curve to evaluate prediction models of rare critical illness events," *Pediatric Critical Care Medicine*, vol. 26, no. 6, pp. e855–e859, 2025, doi: 10.1097/PCC.0000000000003752.

[56] A. A. Mohamed, A. Al-Saleh, S. K. Sharma, and G. G. Tejani, "Zero-day exploits detection with adaptive WavePCA-Autoencoder adaptive hybrid exploit detection network (AHEDNet)," *Scientific Reports*, vol. 15, art. no. 4036, 2025, doi: 10.1038/s41598-025-87615-2.

[57] S. Michaelides, S. Lenz, T. Vogt, and M. Henze, "Secure integration of 5G in industrial networks: State of the art, challenges and opportunities," *Future Generation Computer Systems*, vol. 166, art. no. 107645, 2025, doi: 10.1016/j.future.2024.107645.

[58] J. Yedalla, "Quantum-safe cryptography: Navigating the future of cybersecurity in the post-quantum era," *International Journal of Science and Research (IJSR)*, vol. 14, no. 2, pp. 249–253, 2025.

[59] G. G. Shayea, M. H. M. Zabil, M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, "Strategies for protection against adversarial attacks in AI models: An in-depth review," *Journal of Intelligent Systems*, vol. 34, no. 1, art. no. 20240277, 2025, doi: 10.1515/jisys-2024-

0277.

[60] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, and I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Scientific Reports*, vol. 15, art. no. 9885, 2025, doi: 10.1038/s41598-025-09885-0.

[61] M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and H. M. Khater, "Reinforcement learning with deep features: A dynamic approach for intrusion detection in IoT networks," *IEEE Access*, 2025.

How to cite this article

M. A. Radhi, M. S. Ahmed, E. A. W. Hachim, and Z. F. Lutfi, " Emerging Trends and AI-Driven Defense Mechanisms in Cybersecurity: A Novel Framework for Threat Prediction and Prevention," *CyberSystem J.*, vol. 2, no. 1, pp. 10-21, 2025. doi: 10.57238/csj.2025.1002

Access this article online