ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Design Perspectives On Intelligent and Blockchain-Enabled Cybersecurity Systems

R. Saranya[1]; Dr. Sumathy Kingslin[2]

[1]Research Scholar PG & Research Department of Computer Science Quaid-E-Millath Government College for Women Annasalai, Chennai-02.

[2]Associcate Professor PG & Research Department of Computer Science Quaid-E-Millath Government College for Women Annasalai, Chennai-02.

DOI: https://doi.org/10.51583/IJLTEMAS.2026.15020000020

Received: 16 February 2026; Accepted: 21 February 2026; Published: 03 March 2026

ABSTRACT

Recent advances in digital infrastructures, cloud services, blockchain platforms, Internet of Things (IoT), and artificial intelligence (AI) have significantly increased the complexity of cybersecurity threats while intensifying concerns related to data privacy and system trust.

In response, contemporary research has focused on integrating intelligent data-driven techniques with secure and privacy-aware mechanisms to counter sophisticated cyberattacks.

This literature review systematically analyzes and synthesizes selected peer-reviewed studies with an emphasis on AI-driven intrusion detection systems and blockchain-enabled security architectures. The reviewed works are examined in terms of their underlying methodologies, algorithms, tools, strengths, and limitations.

A comparative analysis identifies key trends, persistent challenges, and research gaps, particularly in explainable AI, system scalability, and secure analytics. The findings highlight the need for unified and deployable cybersecurity frameworks that balance detection accuracy, transparency, and operational efficiency.

This review provides a structured foundation to support future research on intelligent and trustworthy cybersecurity systems.

Keywords: Cybersecurity, Artificial Intelligence, Blockchain Security, Intrusion Detection, Explainable AI

INTRODUCTION

The rapid growth of data-centric technologies has reshaped modern cybersecurity landscapes. Systems deployed in financial networks, cloud infrastructures, and distributed digital platforms generate large volumes of sensitive data, making them attractive targets for cyberattacks [1], [2].

Traditional rule-based and perimeter-oriented security mechanisms are increasingly insufficient against sophisticated threats such as advanced persistent attacks and data-driven exploitation strategies [3], [5].

Consequently, recent research has shifted toward intelligent cybersecurity solutions that leverage machine learning (ML), deep learning (DL), and blockchain technologies to improve detection accuracy, system trust, and operational transparency [1], [6], [7].

This literature review consolidates and critically examines peer-reviewed studies drawn from the selected dataset [1]–[10], with the objective of identifying strengths, limitations, and open challenges in intelligent cybersecurity system design.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

AI-Driven Intrusion Detection and Cyber Threat Analysis

Artificial intelligence has become a cornerstone of modern intrusion detection systems. Ghosh et al. [1] proposed an AI-driven financial cybersecurity framework combining recurrent neural networks (RNNs) with scaled gated recurrent units (SGRUs) and explainable AI techniques.

Their approach demonstrates strong capability in modeling sequential transaction behavior while offering interpretability for security analysts. However, the framework introduces increased computational overhead, raising concerns regarding scalability and real-time deployment.

Other studies within the selected literature explore supervised machine learning techniques for cyberattack detection in financial and distributed environments [2], [7].

These approaches demonstrate improved detection accuracy compared to traditional methods but rely heavily on labeled datasets, which limits adaptability to evolving and previously unseen attacks [3], [5].

Blockchain-Based Security and Trust Mechanisms

Blockchain technology has emerged as a promising solution for enhancing trust, immutability, and transparency in cybersecurity systems [6], [10]. Han et al.

[2] investigated machine learning–based detection mechanisms using blockchain-derived features, employing classifiers such as Random Forests, Support Vector Machines, and Decision Trees. Their results indicate that blockchain-aware feature engineering can effectively support anomaly detection with relatively low training complexity.

Despite these advantages, existing blockchain-based security solutions face challenges related to scalability, latency, and system integration [4], [6], [9].

Several studies emphasize that blockchain alone does not provide intelligent threat detection and must be combined with AI-driven analytics to address complex cyberattack

Explainability and Secure Analytics

Explainability has emerged as a critical requirement for intelligent cybersecurity systems, particularly in financial and regulatory-sensitive domains.

The work by Ghosh et al. [1] demonstrates the benefits of explainable AI in improving analyst trust and decision transparency. Similarly, conceptual studies highlight the importance of governance, accountability, and system interpretability in AI-driven cybersecurity solutions [3], [6].

While the selected literature acknowledges the importance of secure and trustworthy analytics, most existing studies focus primarily on detection performance, with limited discussion on balancing explainability, system efficiency, and deployment feasibility [5], [7].

COMPARATIVE ANALYSIS AND DISCUSSION

Comparative analysis of the reviewed studies indicates that AI-driven intrusion detection systems consistently outperform traditional rule-based approaches in identifying complex attack patterns [1], [7].

Deep learning models are effective in capturing sequential and high-dimensional behaviours, whereas classical machine learning techniques offer advantages in interpretability and computational efficiency [2].

Blockchain-enabled frameworks enhance trust, auditability, and data integrity but introduce latency and scalability challenges that limit real-time applicability [4], [6].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Furthermore, most studies evaluate system performance using accuracy-centric metrics, with limited attention to deployment constraints and system-level efficiency [5], [9].

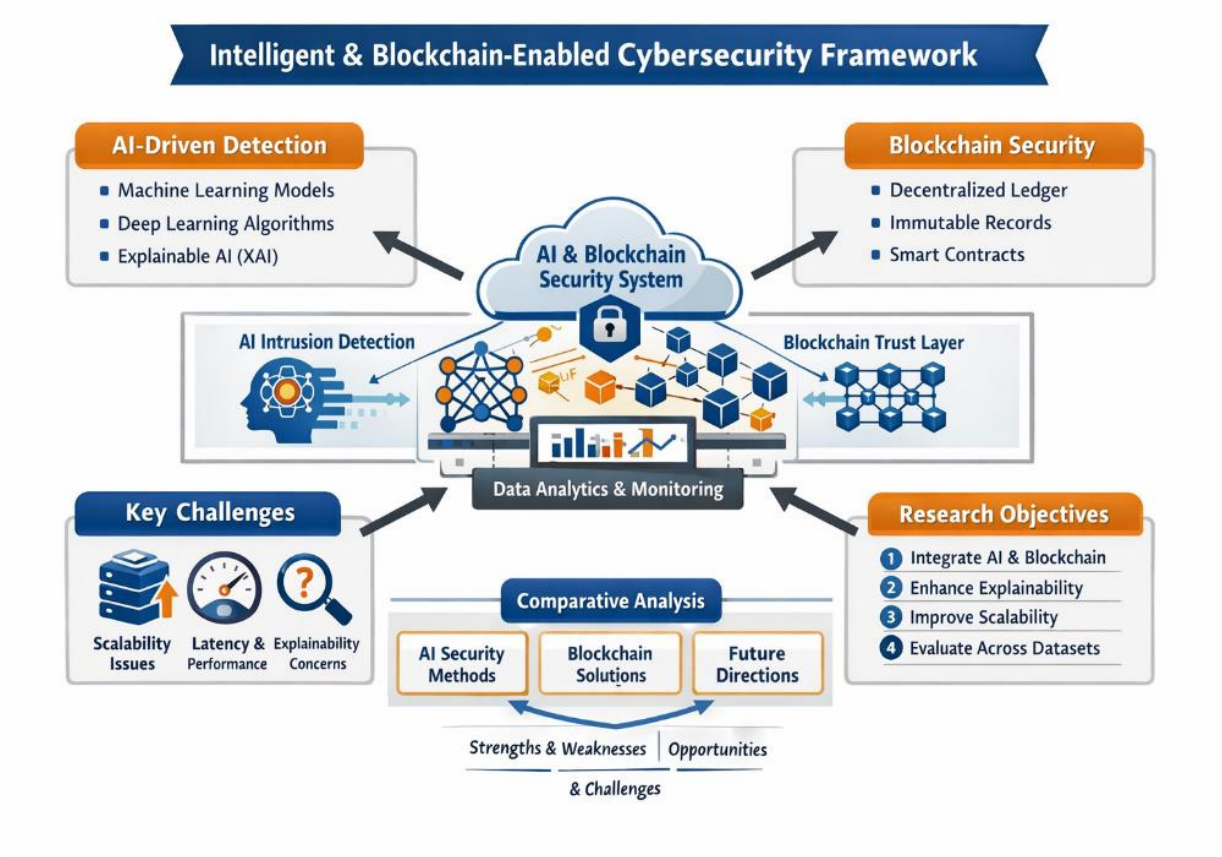

Fig 1.AI-Driven and Blockchain-Based Approaches for Secure and Trustworthy Cybersecurity

Evaluation of Existing Intelligent Cybersecurity Techniques

This section provides a detailed evaluation of existing intelligent and privacy-aware cybersecurity techniques reported in the literature. The selected studies are systematically compared based on their core methodologies, datasets, advantages, limitations, and identified research gaps.

The analysis highlights the growing adoption of artificial intelligence and blockchain technologies in addressing cybersecurity challenges, while also revealing unresolved issues related to explainability, scalability, computational complexity, and real-world applicability.

Table I presents a comprehensive comparative analysis of these approaches and serves as a reference for identifying opportunities for future research.

Table I. Comparative Analysis of Existing Intelligent and Privacy-Aware Cybersecurity Approaches

Paper	Method	Dataset	Pros	Cons	Research Gap
Ghosh et al. [1]	RNN + SGRU + XAI	Financial data	High accuracy; explainable	High computation	Scalability limits
Han et al. [2]	RF, SVM, DT	Blockchain finance	Interpretable; fast	Label dependency	Limited adaptability

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Asmar & Tuqan [3]	ML governance survey	Survey	Policy insight	No experiments	Needs validation
Ehsan et al. [4]	Blockchain architecture	Transaction systems	Tamper resistance	Latency	No AI detection
Darem et al. [5]	Threat taxonomy	Survey	Comprehensive	Descriptive	Needs operational IDS
Abbas & David [6]	AI + blockchain model	Conceptual	Strong vision	No datasets	No implementation
Feng & Li [7]	Ledger anomaly detection	Blockchain ledgers	On-chain visibility	Limited scope	Robustness issues
Maram et al. [8]	EfficientNet + FFNN	Ransomware data	High accuracy	Heavy model	Resource awareness
Albakri et al. [9]	Metaheuristic ML	IDS benchmarks	Robust tuning	Runtime cost	Scalability
Alohali et al. [10]	ML + blockchain	Cyber datasets	Auditability	Integration cost	Latency trade-offs

Problem Statement and Research Motivation

A. Problem Statement

Although AI-driven and blockchain-enabled cybersecurity solutions significantly improve detection accuracy and system trust, existing approaches largely emphasize performance while overlooking scalability, explainability, and deployment feasibility as unified objectives [1], [6], [7]. Deep learning–based models demonstrate strong capability in capturing complex attack behaviours but incur high computational overhead and system complexity [1], [8].

Conversely, blockchain-assisted security frameworks enhance auditability and integrity but struggle with latency, scalability, and intelligent attack detection when deployed in real-time environments [4], [6], [9]. Furthermore, current evaluation practices focus predominantly on accuracy metrics, limiting insight into system robustness and operational effectiveness [5], [7].

B. Research Motivation

The motivation for this research arises from the growing demand for cybersecurity systems that are not only accurate but also interpretable, scalable, and deployable in real-world settings. Prior studies highlight the need for integrating explainable AI techniques with blockchain-based trust models to improve transparency and system reliability [1], [6], [10].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

By addressing these challenges, future research can bridge the gap between conceptual security models and practical cybersecurity deployments.

Research Objectives and Contributions

A. Research Objectives

1. To design an intelligent cybersecurity framework that integrates AI-driven detection with blockchain-based trust mechanisms [1], [6].
2. To improve system interpretability through explainable AI techniques suitable for security analysts [1], [3].
3. To enhance scalability and efficiency while maintaining high detection accuracy [2], [8].
4. To evaluate system performance across heterogeneous datasets and attack scenarios [7], [9].

B. Research Contributions

1. A unified intelligent cybersecurity architecture combining AI-driven detection and blockchain-enabled trust.
2. A structured comparative analysis of existing AI and blockchain-based cybersecurity approaches.
3. Identification of key limitations and deployment challenges in current intelligent security systems.
4. Practical insights to support the development of scalable and trustworthy cybersecurity solutions.

CONCLUSION

This literature review examined recent advances in intelligent and blockchain-enabled cybersecurity systems based on selected peer-reviewed studies. The findings confirm that AI-driven intrusion detection techniques provide superior capability in identifying complex and evolving cyber threats compared to traditional security approaches. Blockchain-based mechanisms further strengthen system trust through transparency, immutability, and secure data sharing. However, the review also reveals that many existing solutions prioritize detection accuracy while neglecting scalability and deployment feasibility. Deep learning models often introduce high computational overhead, limiting their use in real-time environments. Similarly, blockchain architectures suffer from latency and integration challenges. Explainability remains an underexplored area despite its importance for analyst trust and regulatory compliance. The lack of standardized evaluation metrics further complicates performance assessment. Most studies rely on accuracy-centric measures without considering system efficiency. The review highlights the need for integrated frameworks that balance intelligence, trust, and practicality. Future research should emphasize lightweight AI models and optimized blockchain designs. Adaptive and explainable security analytics are essential for handling evolving attacks. Addressing these challenges will enable the development of robust and trustworthy cybersecurity systems. Overall, this review provides a strong foundation for next-generation intelligent cybersecurity research.

REFERENCES

1. S. Ghosh, *et al.*, “A Novel Framework for Financial Cybersecurity Using Explainable Artificial Intelligence,” IEEE Access, vol. 13, pp. 1–15, 2025.
2. J. Han, L. Li, and J. Hu, “Research on Security Detection of Blockchain Financial Systems Based on Machine Learning,” International Journal of Network Security, vol. 27, no. 2, pp. 215–228, 2025.
3. R. Asmar and R. Tuqan, “Integrating Machine Learning for Sustaining Cybersecurity: Challenges, Opportunities, and Governance,” Heliyon, vol. 10, no. 4, pp. 1–14, 2024.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

4. S. B. Ehsan, *et al.*, "Blockchain-Based Cybersecurity Solutions for Secure Transactions," International Journal of Computer Applications, vol. 186, no. 12, pp. 25–33, Dec. 2024.
5. A. Darem, A. A. Abugabah, and F. Saeed, "Cyber Threats: Classifications, Detection Techniques, and Countermeasures—A Comprehensive Survey," IEEE Access, vol. 11, pp. 45612–45635, 2023.
6. M. Abbas and J. David, "Artificial Intelligence and Blockchain: A Combined Approach for Cybersecurity," Technical Report, 2024.
7. Z. Feng and Y. Li, "Blockchain-Oriented Approach for Detecting Cyber Attacks in Financial Systems," Financial Innovation, vol. 9, no. 1, pp. 1–18, 2023.
8. R. Maram, *et al.*, "Hybrid EfficientNet Feed-Forward Neural Network for Ransomware Detection," Engineering Applications of Artificial Intelligence, vol. 124, pp. 1–13, 2025.
9. A. Albakri, *et al.*, "Blockchain-Assisted Machine Learning with Hybrid Metaheuristic Optimization for Cyberattack Detection," Sustainability, vol. 14, no. 3, pp. 1–20, 2022.
10. M. Alohali, *et al.*, "Blockchain-Assisted Optimal Machine Learning–Based Cyberattack Detection Framework," Computer Systems Science and Engineering, vol. 44, no. 2, pp. 987–1002, 2023.