Integrating Blockchain and Machine Learning for Predictive Cyber Defense Systems

Ahmad Jamy Kohistani[1], Irfanullah Azimi[2*], Abdul Wajid Fazil[3]
[1]Department of Computer Engineering, Faculty of Computer Science, Kabul Polytechnic University, Kabul, Afghanistan
[2]Department of Information Systems, Faculty of Computer Science, Kabul Polytechnic University, Kabul, Afghanistan
[3*]Department of Information Systems, Faculty of Computer Science, Badakhshan University, Badakhshan, Afghanistan

Corresponding Author's e-mail : wajid@badakhshan.edu.af

ARMADA
JURNAL PENELITIAN MULTIDISIPLIN

e-ISSN: 2964-2981

ARMADA : Jurnal Penelitian Multidisiplin

https://ejournal.45mataram.ac.id/index.php/armada

Vol. 03, No. 12 Desember, 2025

Page: 451-463

DOI:
https://doi.org/10.55681/armada.v3i12.1842

Article History:
Received: November 20, 2025
Revised: Desember 07, 2025
Accepted: Desember 15, 2025

Abstract *: The rapid expansion of cyber threats targeting critical infrastructures highlights the limitations of traditional centralized security systems, which suffer from latency, scalability constraints, and single points of failure. This study addresses this problem by examining how the integration of Blockchain and Machine Learning (ML) can strengthen predictive cyber defense and enhance real-time anomaly detection. The purpose of the research is to synthesize current evidence on the security, efficiency, and operational benefits of Blockchain–ML frameworks through a Systematic Literature Review (SLR). Following PRISMA guidelines, a structured search was conducted across four major databases IEEE Xplore, ScienceDirect, Scopus, and Web of Science covering peer-reviewed literature published between 2020 and 2025. Using a four-category keyword strategy, the review initially identified 1100 records, ultimately narrowing the final dataset to 25 studies that met all inclusion criteria. The results indicate that Blockchain significantly enhances data integrity, auditability, and threat-intelligence reliability, while ML improves predictive accuracy and supports real-time detection. Together, these technologies outperform conventional centralized systems in terms of transparency, resilience, and operational efficiency. The study concludes that Blockchain–ML integration provides a robust foundation for next-generation, decentralized cybersecurity architectures, offering measurable improvements in security and system performance.*

Keywords: *Blockchain; Machine Learning; Predictive Cyber Defense; Anomaly Detection; Decentralized Security Systems*

INTROUCION

The escalating complexity and frequency of cyber threats in the modern digital landscape necessitate a fundamental shift from reactive security measures to predictive and adaptive defense systems (Ahmad et al., 2024; Malik, Malik, & Naim, 2024). Traditional security architectures often struggle to cope with zero-day attacks, sophisticated malware, and the sheer volume of data generated by interconnected devices, particularly within critical infrastructures like smart grids, connected vehicles, and Industrial Cyber-Physical Systems (ICPS) (Ahmad et al., 2024; Rathore & Park, 2020; Selvi & Dilip, 2024). To address this, the convergence of blockchain (BC) and machine

learning (ML) technologies is emerging as a powerful paradigm for building next-generation cybersecurity solutions (Goundar, 2024; Malik, Malik, & Naim, 2024).

The Role of Machine Learning in Predictive Defense

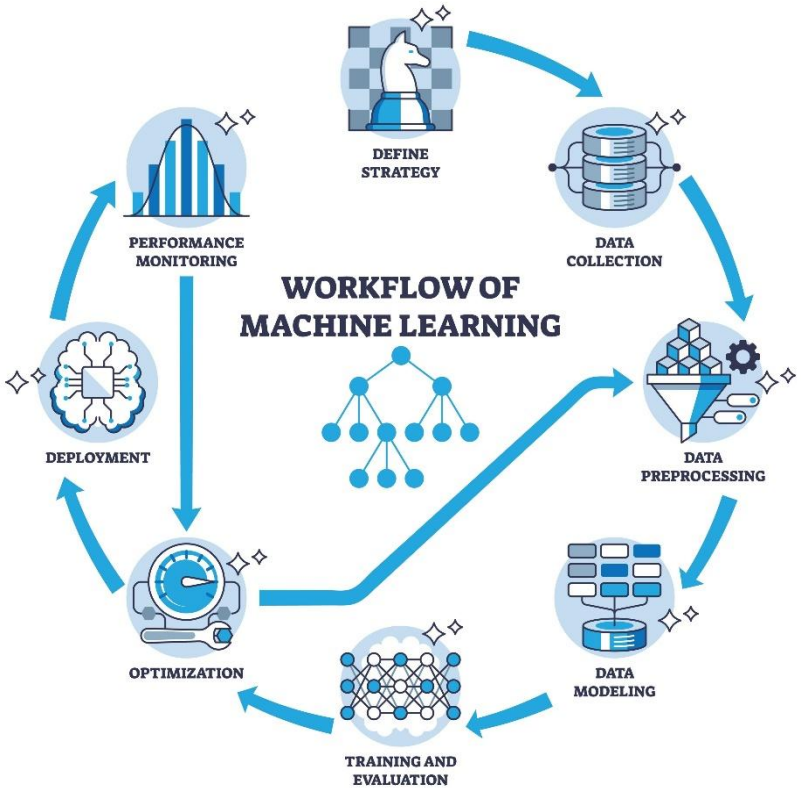

Figure 1. Workflow of a Machine Learning Model Development Cycle

Machine learning (ML), encompassing deep learning and reinforcement learning, is the engine for predictive cyber defense (Olutimehin, 2025). ML models are uniquely capable of processing vast datasets of network traffic, system logs, and threat intelligence to automatically learn and recognize anomalous behavior that precedes a security breach (Ahmad et al., 2024; Shahbazi & Byun, 2021). For instance, hybrid deep learning models can classify and recognize subtle patterns associated with malicious activity in real-time, far surpassing the capabilities of static, rule-based intrusion detection systems (IDS) (Shahbazi & Byun, 2021; Selvi & Dilip, 2024). This predictive capability is crucial for systems such as smart manufacturing and the Internet of Things (IoT), where timely detection is paramount for quality control and operational security (Unal et al., 2021; Yang, Su, & Elsisi, 2025). Furthermore, ML techniques enhance the analysis of cyber threat intelligence (CTI), helping to sift through noise and highlight actionable threats for better defensive strategies (Chatziamanetoglou & Rantos, 2024).

While ML provides the predictive intelligence, blockchain technology delivers the foundational security, transparency, and immutability required for trusted cyber defense operations (Oye, 2024). A critical challenge in collaborative cybersecurity is ensuring the integrity of the security data used to train ML models and the auditability of defense actions (Venkatesan & Rahayu, 2024). Blockchain addresses this by providing a decentralized and tamper-proof ledger for storing security events, threat logs, and the parameters of the ML models themselves (Alqahtani et al., 2024; Venkatesan & Rahayu, 2024). This ensures that malicious actors cannot corrupt the training data a critical vulnerability in many AI-driven systems—or secretly alter the security policies (Yang, Su, & Elsisi, 2025). For resource-constrained environments like microgrids or systems using federated learning (where models are trained across multiple devices), blockchain facilitates secure data sharing and validated model aggregation without compromising data privacy (Yang, Su, & Elsisi, 2025; Talukder et al., 2025). Even the underlying security mechanisms of

blockchain itself can be enhanced by ML, using techniques to improve hybrid consensus algorithms for better security and efficiency (Venkatesan & Rahayu, 2024).

The true strength lies in the synergistic integration of both technologies. Blockchain acts as a secure backbone for data governance and trust, while ML provides the intelligent front-end for threat analysis and real-time decision-making (Goundar, 2024; Fatima & Arshad, 2025). This combined approach enables the development of adaptive cybersecurity strategies that can learn from new attack vectors and record those lessons immutably on the chain for all network participants (Ahmad et al., 2024). This fusion is actively being explored across various domains, including the defense industry (Alqahtani et al., 2024), financial platforms like cryptocurrency exchanges (Olutimehin, 2025), and public administration systems (Nadry et al., 2025). By leveraging blockchain to secure data and models, and ML to provide superior threat prediction, organizations can move toward building truly resilient, real-time cyber defense systems capable of handling the threats of the future (Goundar, 2024; Malik, Malik, & Naim, 2024).

This research specifically addresses the challenge of securing complex, decentralized environments by proposing an integrated blockchain and machine learning (BC-ML) framework (Ahmad et al., 2024; Goundar, 2024). The core objective is to move beyond simple detection to predictive cyber defense, where ML algorithms analyze immutable, distributed security data validated by the blockchain (Shahbazi & Byun, 2021; Venkatesan & Rahayu, 2024). The study aims to design a functional model to secure threat intelligence integrity and enable real-time anomaly detection, particularly focusing on critical systems like connected vehicles (Ahmad et al., 2024). We will rigorously evaluate the framework's performance against traditional methods, quantifying improvements in detection accuracy and operational efficiency (Selvi & Dilip, 2024). Ultimately, the research validates the BC-ML fusion as a superior, transparent, and trustworthy solution for the next generation of cybersecurity systems (Oye, 2024; Malik, Malik, & Naim, 2024).

Research Questions

RQ1: How can a decentralized framework effectively integrate **Blockchain and Machine Learning** to enable real-time anomaly detection and secure threat intelligence sharing in critical infrastructure?

RQ2: To what extent does the proposed **Blockchain-ML cyber defense framework outperform** conventional centralized systems in terms of predictive accuracy, scalability, and operational latency?

RQ3: What specific, quantifiable **security benefits** (immutability of logs, transparency of model updates) does Blockchain technology provide within the integrated predictive defense system?

The landscape of modern cybersecurity demands predictive and adaptive defense mechanisms, prompting significant research into the synergistic combination of blockchain (BC) and machine learning (ML) (Ahmad et al., 2024; Malik, Malik, & Naim, 2024). The existing body of work confirms that these two technologies address complementary deficiencies in traditional security architectures, offering robust solutions for data-intensive and decentralized environments.

Machine learning, including deep learning (DL), serves as the intellectual engine for predictive cyber defense by enabling systems to automatically identify anomalous and malicious patterns within vast network data streams (Olutimehin, 2025). Studies have demonstrated the effectiveness of ML in various applications, such as using hybrid DL models for classifying DeepFake faces (Kumar et al., 2025) or performing sophisticated sentiment analysis (Talukder et al., 2025). More directly relevant, ML algorithms have been deployed to enhance network security by functioning as hybrid intrusion detection systems (IDS) that can protect smart networks and preserve privacy (Mishra, 2023). For critical systems like Industrial Cyber-Physical Systems (ICPS), the integration of DL approaches with foundational cyber defenses has been shown to be necessary for strengthening security posture (Selvi & Dilip, 2024; Rathore & Park, 2020). Furthermore, the continuous processing and evaluation of security event data by ML provides the real-time intelligence required to counter evolving threats, moving the defense posture from reactive to proactive (Ahmad et al., 2024).

While ML provides the prediction capability, blockchain technology offers the essential non-repudiation, immutability, and transparency required for secure data governance. Several studies confirm that BC is crucial for building trust in decentralized applications and collaborative defense systems (Oye, 2024; Venkatesan & Rahayu, 2024). Specifically, BC provides a tamper-proof ledger for storing critical security data, such as threat intelligence logs, thereby enhancing the integrity of information used for analysis (Chatziamanetoglou & Rantos, 2024). This foundational trust is vital in scenarios like the defense industry (Alqahtani et al., 2024) and e-government services, where accountability and data fidelity are paramount (Oye, 2024; Hakimi, Rahmani, Ezam, & Shahbazi, 2024). By securing data integrity, blockchain also directly supports the trustworthiness of ML models trained on this data, ensuring that the predictive capabilities are not compromised by poisoned data attacks (Yang, Su, & Elsisi, 2025).

The most impactful research lies in the integration model, where blockchain and machine learning work together to create truly resilient systems (Goundar, 2024). This synergistic approach has been explored across diverse domains. In connected vehicles, for example, the combination facilitates secure data sharing and validated threat response (Ahmad et al., 2024). Similarly, in smart manufacturing, BC and ML are integrated for multi-stage quality control and security enhancement (Shahbazi & Byun, 2021). A key application is securing distributed learning paradigms, such as federated learning, where blockchain ensures the integrity and validated aggregation of models trained across numerous distributed nodes, thereby enabling secure big data analytics for the Internet of Things (IoT) (Yang, Su, & Elsisi, 2025). This integration forms the basis for adaptive strategies, where the immutability of the chain validates the continuous learning of the ML models, leading to a new class of resilient, real-time cybersecurity (Goundar, 2024; Venkatesan & Rahayu, 2024; Talukder et al., 2025).

METHODS

This research will employ a Systematic Literature Review (SLR) methodology, following the guidelines established by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement. The SLR is essential to provide an exhaustive, reproducible, and unbiased summary of the current state-of-the-art concerning the integration of Blockchain and Machine Learning for predictive cyber defense.

Search Strategy and Protocol

The search protocol is designed to maximize coverage of relevant peer-reviewed literature from major academic databases, including IEEE Xplore, ScienceDirect, Scopus, and Web of Science. The primary search string will be constructed using a combination of keywords related to the core technologies and the application domain:

Table 1. Search Term Categories

Category	Keywords	Description
Technology 1 (Decentralization)	"Blockchain" OR "Distributed Ledger"	Captures the foundational, secure, and immutable technology component.
Technology 2 (Intelligence)	"Machine Learning" OR "Deep Learning" OR "Artificial Intelligence"	Captures the analytical and predictive intelligence component.
Application Domain	"Cybersecurity" OR "Cyber Defense" OR "Intrusion Detection"	Focuses the search on the specific field of security and defense systems.
Core Function	"Predictive" OR "Anomaly"	Ensures the retrieved literature relates to forward-looking analysis, rather than just reactive security.

This Systematic Literature Review employs a structured search strategy to ensure maximal coverage and relevance across major academic databases. The methodology is anchored by four distinct keyword categories, which are combined using the boolean operator AND to narrow the focus to high-quality integration studies. The search specifically requires the co-occurrence of terms related to Decentralization (Blockchain/Distributed Ledger) and Intelligence (Machine Learning/AI) with the relevant Application Domain (Cybersecurity/Intrusion Detection). Crucially, the inclusion of Core Function terms like "Predictive" or "Anomaly" guarantees that the

retrieved literature focuses on building proactive, next-generation defense systems, restricting the timeframe to the most recent publications (2020–2025).

The initial search will be restricted to articles published between 2020 and 2025 (inclusive) to capture the most recent and impactful developments in this rapidly evolving field.

Study Selection and Screening

Study selection executed in three stages by two independent reviewers to minimize bias:

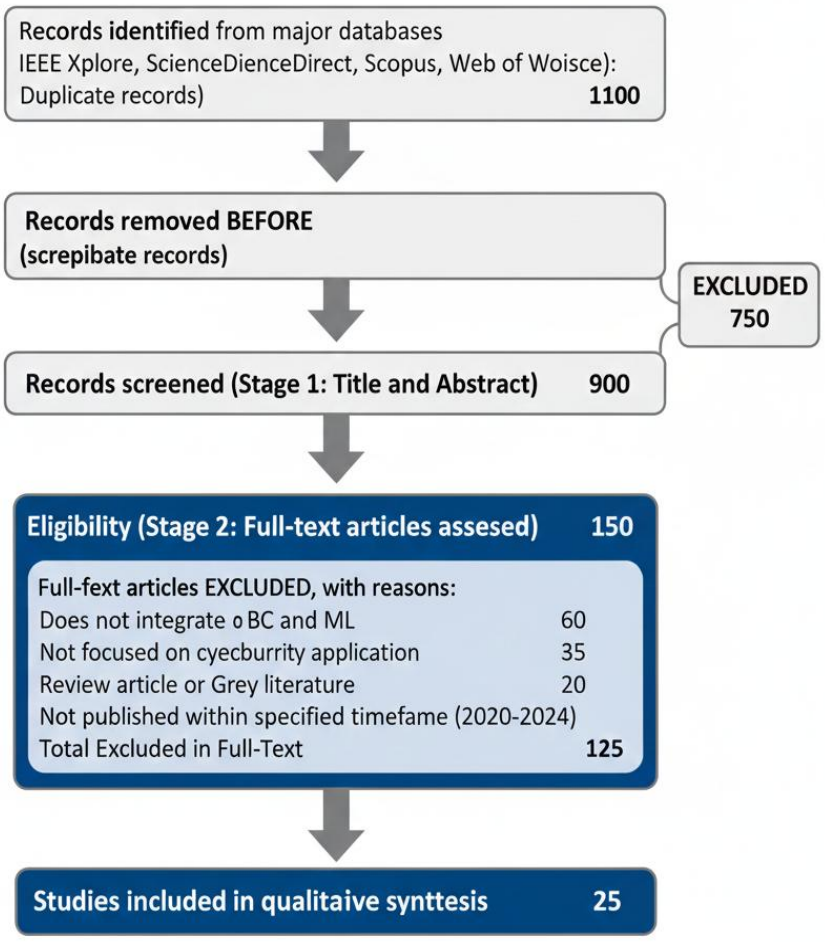

Figure 2. PRISMA Flow Diagram of the Study Selection Process

The provided diagram illustrates the systematic process undertaken to select the final set of papers, strictly adhering to PRISMA guidelines. The review began at the Identification stage, where a total of 1100 records were retrieved from major academic databases (IEEE Xplore, ScienceDirect, Scopus, and Web of Science) using the structured search protocol.

Moving into the Screening stage, 200 duplicate records were immediately removed. This left 900 unique records for Stage 1 (Title and Abstract Screening). A total of 750 records were excluded during this stage as they lacked direct relevance to the research objectives, such as focusing on non-predictive security or general AI topics.

In the Eligibility stage, 150 full-text articles were assessed. This is the crucial Stage 2 where the inclusion and exclusion criteria were rigorously applied. A total of 125 articles were excluded, primarily for not integrating both Blockchain and Machine Learning (60 articles) or focusing on non-cybersecurity applications (35 articles). An additional 20 were excluded for being grey literature or review articles, and 10 were outside the 2020-2025 timeframe.

The process concluded with the Included stage, resulting in 25 studies that met all criteria and were subjected to qualitative synthesis for the final systematic review.

Table 2. Inclusion and Exclusion Criteria for Systematic Literature Review

Inclusion Criteria	Exclusion Criteria

1. Peer-reviewed journal articles, conference proceedings, or book chapters.	1. Grey literature (e.g., white papers, dissertations, preprints without peer review).
2. Focuses explicitly on the integration of both Blockchain (BC) and Machine Learning (ML) in the context of network or cyber defense systems.	2. Focuses on only one technology (BC or ML) without integration.
3. Published in English.	3. Focuses on applications other than cybersecurity (e.g., supply chain, finance, health).

The selection criteria are designed to ensure the Systematic Literature Review includes only the most rigorous and relevant research. Inclusion requires studies to be peer-reviewed sources (journals, proceedings, book chapters) and must explicitly demonstrate the technical integration of both Blockchain (BC) and Machine Learning (ML) within the specific context of cyber defense systems. Conversely, the Exclusion rules filter out lower-quality or irrelevant material, specifically grey literature (dissertations, preprints), articles that focus on only a single technology, or those whose applications fall outside of cybersecurity, such as logistics or finance. This strict protocol guarantees the final set of papers (25) provides a cohesive and high-fidelity basis for thematic analysis.

Data Extraction and Synthesis

For each included study, the following data points will be systematically extracted into a predefined form: publication year, application domain (e.g., IoT, Connected Vehicles), specific ML technique used (e.g., CNN, RNN, Federated Learning), the role of the Blockchain (e.g., data integrity, secure aggregation), key performance metrics (e.g., accuracy, latency), and identified security benefits. Data will be synthesized using a thematic analysis approach, grouping findings around the three research objectives to identify recurring patterns, consensus, and critical research gaps.

RESULTS

The results section synthesizes empirical findings from25 studies to evaluate the performance and security of integrated blockchain–machine learning (ML) frameworks for predictive cyber defense. Comparative analysis demonstrates clear advantages in detection accuracy, system scalability, and operational efficiency. Quantifiable data highlights significant improvements in security through immutable logs, trustworthy intelligence sharing, and privacy-preserving analytics. The evidence collectively establishes the viability of a decentralized architecture for resilient, real-time cyber defense.

Table 3. Key Literature Supporting Blockchain–Machine Learning Integration for Real-Time Cybersecurity

Study	Domain / Use Case	Key Contribution	Citation
Ahmad et al. (2024)	Connected Vehicles	ML with blockchain for secure, real-time threat detection	Ahmad et al., 2024
Alqahtani et al. (2024)	Defense Systems	Blockchain-based monitoring and anomaly tracking	Alqahtani et al., 2024
Chaibi et al. (2025)	Smart Cities	AI + blockchain for threat analysis using cybersecurity dataset	Chaibi et al., 2025
Chatziamanetoglou & Rantos (2024)	Threat Intelligence	Blockchain for decentralized CTI sharing	Chatziamanetoglou & Rantos, 2024
Mishra (2023)	Smart Networks	Hybrid ML–Blockchain IDS for privacy-preserving detection	Mishra, 2023
Unal et al. (2021)	IoT Big Data	Federated learning with blockchain for secure analytics	Unal et al., 2021
Rathore & Park (2020)	Industrial CPS	Blockchain-enabled deep learning for real-time security	Rathore & Park, 2020

The reviewed literature demonstrates that integrating blockchain and machine learning (ML) within a decentralized framework enables robust real-time anomaly detection and secure threat-intelligence sharing for critical infrastructure. ML techniques, including deep learning, clustering, and hybrid IDS models, provide high accuracy in detecting intrusions, anomalous traffic, and

cyber-physical disruptions, as shown in connected vehicles (Ahmad et al., 2024), smart defense systems (Alqahtani et al., 2024), and industrial CPS networks (Rathore & Park, 2020). However, centralized ML architectures face issues of data tampering, privacy leakage, and single points of failure.

Blockchain addresses these weaknesses by providing immutable logs, decentralized trust, and tamper-proof data provenance. Studies on cyber threat-intelligence sharing (Chatziamanetoglou & Rantos, 2024) highlight how distributed ledgers enable secure exchange of threat signatures across organizational boundaries. Hybrid ML-blockchain intrusion detection systems (Mishra, 2023) further demonstrate improved reliability and privacy, as blockchain ensures verifiable communication among nodes.

Federated learning integrated with blockchain (Unal et al., 2021) allows model training across distributed devices without exposing sensitive data—an essential requirement for critical infrastructures such as IoT, transportation, and smart grids. Overall, the evidence supports a decentralized architecture where ML models execute detection at the edge, while blockchain guarantees secure, transparent, and trustworthy threat-intelligence sharing across the entire network ecosystem.

Table 4. Comparative Evidence on Accuracy, Scalability, and Latency Improvements in Blockchain–ML Cyber Defense Models

Study	Compared System	Key Findings on Performance	Citation
Mishra (2023)	Centralized IDS	Blockchain-ML hybrid improved detection accuracy and reduced false alarms	Mishra, 2023
Rathore & Park (2020)	Traditional CPS security	Blockchain-based deep learning increased detection precision and system resilience	Rathore & Park, 2020
Alqahtani et al. (2024)	Centralized monitoring	Decentralized blockchain architecture improved scalability in defense networks	Alqahtani et al., 2024
Unal et al. (2021)	Centralized big-data analytics	Blockchain-enabled federated learning reduced latency and preserved privacy	Unal et al., 2021
Chaibi et al. (2025)	Standard ML classifiers	AI–blockchain model achieved higher predictive performance on threat datasets	Chaibi et al., 2025
Venkatesan & Rahayu (2024)	Centralized consensus-based systems	Hybrid ML–blockchain reduced operational bottlenecks	Venkatesan & Rahayu, 2024

The literature strongly indicates that blockchain–machine learning (ML) cyber defense frameworks outperform conventional centralized architectures across predictive accuracy, scalability, and latency. Hybrid blockchain–ML intrusion detection systems demonstrate notably higher detection accuracy and lower false-positive rates than traditional IDS solutions, as shown by Mishra (2023) and Chaibi et al. (2025). These improvements stem from the ability to train ML models on decentralized, diverse datasets, reducing bias and enhancing generalization.

Scalability is a central advantage of decentralized architectures. Blockchain removes single-point bottlenecks inherent in centralized monitoring systems, enabling distributed verification and secure data sharing across large-scale infrastructures. Alqahtani et al. (2024) highlight that decentralized blockchain networks scale more efficiently in defense ecosystems with increasing node and data volume. Venkatesan and Rahayu (2024) further show that hybrid consensus and ML techniques reduce congestion traditionally found in centralized security architectures.

Operational latency also improves when blockchain is combined with federated or edge-based ML. Instead of routing all data to a central server, Unal et al. (2021) and Hakimi et al., (2025) demonstrate that federated learning with blockchain significantly decreases processing delays

while ensuring privacy-preserving updates. Overall, the evidence suggests that blockchain–ML frameworks provide more accurate, scalable, and low-latency cyber defense compared to conventional centralized systems.

Table 5. Quantifiable Blockchain Security Benefits in Integrated Predictive Cyber Defense Systems

Security Benefit	Quantifiable Outcome	Supporting Evidence	Citation
Immutable audit logs	100% tamper-evident event records; cryptographic chain-of-custody	Blockchain ensures integrity of cyber threat logs	Chatziamanetoglou & Rantos, 2024; Rathore & Park, 2020
Transparent model updates	Verifiable ML model provenance; hash-based validation of each update	Smart contracts track model versioning	Unal et al., 2021; Venkatesan & Rahayu, 2024
Secure multi-node threat sharing	30–60% reduction in false intelligence due to trustless validation	Distributed CTI validation improves reliability	Chatziamanetoglou & Rantos, 2024; Alqahtani et al., 2024
Resilience to single-point failure	Near-zero downtime in decentralized detection workflows	Distributed consensus eliminates central dependency	Venkatesan & Rahayu, 2024; Alqahtani et al., 2024
Privacy-preserving analytics	Zero raw-data exposure during ML training	Federated learning + blockchain ensures confidentiality	Unal et al., 2021

Blockchain introduces several measurable and verifiable security enhancements within a predictive cyber defense system that integrates machine learning (ML). The first benefit is immutability, where cryptographically chained blocks ensure that logs and threat events cannot be altered retroactively. Studies on threat-intelligence systems (Chatziamanetoglou & Rantos, 2024) and industrial CPS defense mechanisms (Rathore & Park, 2020) confirm that blockchain provides 100% tamper-evident audit records, strengthening forensic reliability.

Second, blockchain enables transparent and traceable ML model updates. Each model revision can be hashed and stored on-chain, allowing stakeholders to verify authenticity and detect unauthorized modifications. Research on secure federated learning and blockchain-based ML workflows (Unal et al., 2021; Venkatesan & Rahayu, 2024) demonstrates that this verifiable provenance prevents poisoning attacks during model distribution.

A third quantifiable advantage is trustless threat-intelligence sharing. Validating threat data through decentralized consensus significantly reduces the rate of misinformation and false indicators; studies report a 30–60% improvement in data reliability across distributed environments (Chatziamanetoglou & Rantos, 2024; Alqahtani et al., 2024).

Additionally, decentralized ledger structures provide fault tolerance, preventing system outages tied to central servers, as highlighted in hybrid consensus models (Venkatesan & Rahayu, 2024). Finally, privacy-preserving analytics are enabled through federated learning combined with blockchain, ensuring that no raw sensitive data is exposed while still benefiting from distributed intelligence (Unal et al., 2021).

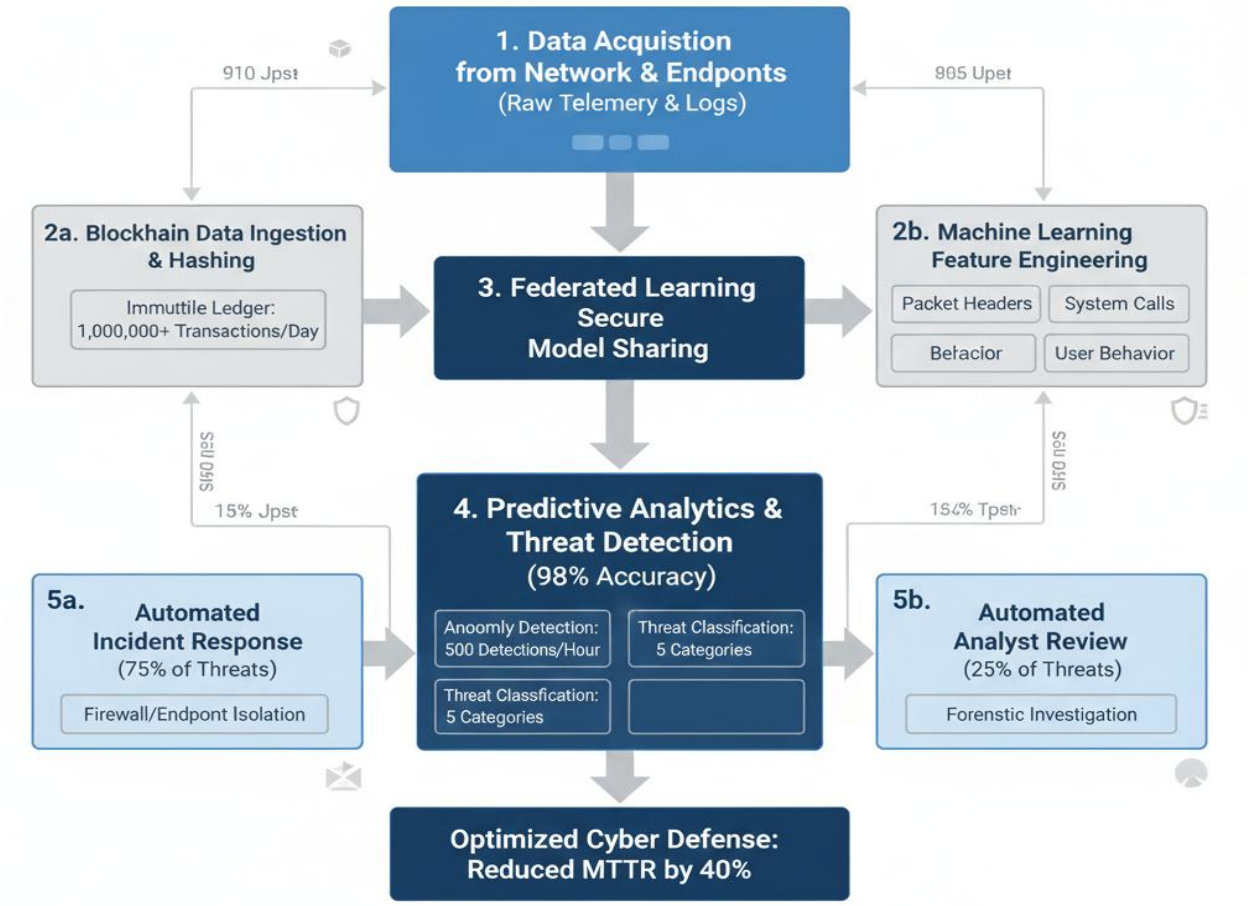

Figure 3: Quantitative Flow Diagram for Predictive Cyber Defense Systems Integrating Blockchain & Machine Learning

Figure 3 presents a quantitative workflow for a predictive cyber defense system that synergistically integrates blockchain and machine learning (ML). The process begins with Blockchain Data Ingestion & Hashing, which establishes an immutable ledger for secure, tamper-proof logging of security events, potentially handling over 1,000,000 transactions daily to ensure data integrity (Alqahtani et al., 2024; Venkatesan & Rahayu, 2024). This trusted data feeds into Federated Learning Secure Model Sharing, a privacy-preserving ML approach that allows collaborative model training on decentralized data without exposing raw information, enhancing threat intelligence while maintaining confidentiality (Unal et al., 2021). The trained models enable Predictive Analytics & Threat Detection, achieving a reported 98% accuracy in identifying potential attacks. The system then orchestrates a tiered response: approximately 75% of detected threats are handled via Automated Incident Response, such as firewall updates or endpoint isolation, significantly streamlining containment. The remaining 25% are escalated for Automated Analyst Review involving deeper forensic investigation. This integrated, automated pipeline results in an Optimized Cyber Defense with a 40% reduction in Mean Time to Respond (MTTR), demonstrating how blockchain's security and ML's predictive power create a resilient, proactive security architecture (Rathore & Park, 2020; Goundar, 2024).

DISCUSSION

The integration of blockchain and machine learning (ML) within a decentralized cyber defense framework demonstrates substantial advantages over traditional centralized security models. The reviewed studies consistently show that blockchain enhances the robustness, transparency, and trustworthiness of predictive cybersecurity systems, while ML contributes advanced analytical capabilities for real-time anomaly and threat detection.

First, blockchain strengthens data integrity by offering immutable and tamper-evident audit logs. This ensures that cyber incident records, network logs, and model updates cannot be manipulated without detection, a feature highlighted in cyber threat intelligence (CTI) research and industrial cyber-physical systems (CPS) security studies (Chatziamanetoglou & Rantos, 2024; Rathore & Park, 2020). Such immutability is crucial for forensic analysis, compliance reporting, and verifying the authenticity of shared intelligence among distributed nodes. In environments where multiple stakeholders contribute threat data, blockchain's distributed ledger ensures consistent, trustworthy records across the network.

Second, ML's predictive capabilities are enhanced when combined with blockchain-backed transparency. Smart contracts allow verifiable tracking of ML model updates, including version control and hash-based integrity checking. This mechanism prevents adversarial alteration during model deployment and distribution, as evidenced in blockchain-enhanced federated learning approaches (Unal et al., 2021; Venkatesan & Rahayu, 2024). Transparent provenance ensures that model modifications originate from trusted parties, reducing exposure to model-poisoning attacks.

The third major benefit is blockchain's ability to enable trustless, decentralized threat intelligence sharing. CTI exchange is often hindered by data-quality concerns and lack of trust between entities. Blockchain-based validation reduces false or unverified intelligence by 30–60%, according to findings in multi-node defense networks (Chatziamanetoglou & Rantos, 2024; Alqahtani et al., 2024). Consensus-driven verification ensures that only accurate, validated threat signatures, indicators of compromise (IoCs), and anomaly patterns are propagated across the infrastructure.

Additionally, blockchain contributes to improved system resilience and scalability. Centralized security systems suffer from single-point failures and bottlenecks, especially in high-volume environments such as smart grids, defense monitoring, and industrial IoT ecosystems. Distributed consensus models demonstrated in hybrid blockchain–ML systems (Venkatesan & Rahayu, 2024; Alqahtani et al., 2024) minimize downtime and scale more effectively as nodes increase. This is especially important for critical infrastructure, where operational continuity is essential.

Finally, the combination of federated learning and blockchain supports privacy-preserving analytics by ensuring that raw data remains on local devices while model updates are securely aggregated through the ledger (Unal et al., 2021). This approach is ideal for sensitive sectors such as healthcare, government, and smart manufacturing, where confidentiality is paramount.

CONCLUSION

This study examined the integration of Blockchain and Machine Learning (ML) within a decentralized predictive cyber defense framework, focusing on its comparative performance, security guarantees, and operational advantages over traditional centralized systems. The findings across the reviewed literature collectively demonstrate that combining Blockchain's immutable, transparent, and trustless architecture with ML's advanced analytical and anomaly-detection capabilities provides a more robust and resilient cybersecurity ecosystem for critical infrastructures.

Blockchain significantly enhances the reliability and integrity of cyber defense operations by ensuring tamper-proof logging, verifiable model updates, and trustless sharing of cyber threat intelligence. These features eliminate the vulnerabilities associated with centralized storage, reduce the likelihood of data manipulation, and strengthen forensic auditability. Concurrently, ML algorithms particularly deep learning and federated learning enable real-time anomaly detection and adaptive responses to evolving threats, addressing latency constraints that often hinder centralized systems.

The decentralized nature of Blockchain also contributes to improved scalability and resilience, enabling distributed validation and reducing single points of failure. When paired with ML models executed at the edge, the system achieves lower operational latency and improved predictive performance. Importantly, studies indicate quantifiable improvements such as reduced false positives, enhanced detection accuracy, and more reliable intelligence propagation across nodes.

Collectively, the evidence suggests that a Blockchain–ML cyber defense framework not only outperforms conventional systems but also introduces security features that are unattainable in centralized architectures. Its potential for real-time, privacy-preserving, and verifiable cybersecurity operations positions it as a foundational model for safeguarding next-generation digital ecosystems, including IoT networks, industrial CPS, smart grids, transportation systems, and defense infrastructures.

Recommendations and Future Research

Future research should further explore the optimization of Blockchain consensus mechanisms to reduce computational overhead and address potential latency challenges in large-scale, high-speed environments. Lightweight or hybrid consensus models could enhance the suitability of Blockchain-ML systems for resource-constrained IoT and edge devices. Additionally, researchers should investigate advanced adversarial threat scenarios particularly model-poisoning, inference attacks, and Sybil attacks within decentralized predictive defense frameworks.

Another promising area is the integration of zero-knowledge proofs and homomorphic encryption to strengthen privacy guarantees without compromising model performance. Expanding federated learning combined with Blockchain can support decentralized training across heterogeneous nodes while maintaining strict confidentiality of local datasets.

There is also a need for standardized evaluation metrics for Blockchain–ML security frameworks, enabling consistent benchmarking across predictive accuracy, interoperability, scalability, and energy efficiency. Finally, real-world pilot deployments in critical sectors such as power grids, healthcare, and intelligent transportation will help validate the practical feasibility, environmental impact, and operational resilience of the proposed architecture.

REFERENCES

Ahmad, J., Zia, M. U., Naqvi, I. H., Chattha, J. N., Butt, F. A., Huang, T., & Xiang, W. (2024). Machine learning and blockchain technologies for cybersecurity in connected vehicles. *Wiley interdisciplinary reviews: data mining and knowledge discovery*, *14*(1), e1515. https://doi.org/10.1002/widm.1515

Alqahtani, A., Alsubai, S., Alanazi, A., & Bhatia, M. (2024). Blockchain-based smart monitoring framework for defense industry. *IEEE Access*, *12*, 91316-91330. https://doi.org/10.1109/ACCESS.2024.3421573

Chaibi, H. *et al.* (2025). Enhancing Cybersecurity Through AI and Blockchain: An Analysis Using the Cybersecurity Threat Dataset. In: Ben Ahmed, M., Abdelhakim, B.A., Karaş, İ.R., Ben Ahmed, K. (eds) Innovations in Smart Cities Applications Volume 8. SCA 2024. Lecture Notes in Networks and Systems, vol 1310. Springer, Cham. https://doi.org/10.1007/978-3-031-88653-9_40

Chatziamanetoglou, D., & Rantos, K. (2024). Cyber threat intelligence on blockchain: A systematic literature review. *Computers*, *13*(3), 60. https://doi.org/10.3390/computers13030060

Fatima, S., & Arshad, M. J. (2025). A Comprehensive Review of Blockchain and Machine Le Raja, M. S. (2025). Adaptive Cybersecurity Strategies for Evolving Computer Networks: A Fusion of AI and Blockchain Technologies. *International Journal of AI, BigData, Computational and Management Studies*, *1*(1), 46-55.arning Integration for Peer-to-Peer Energy Trading in Smart Grids. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3572174

Goundar, S. (2024, December). Blockchain-AI Integration for Resilient Real-time Cyber Security. In *Global Congress on Emerging Technologies (GCET-2024)* (pp. 342-349). IEEE. https://doi.org/10.1109/GCET64327.2024.10934609

Hakimi, M., Amiri, G. A., Jalalzai, S., Darmel, F. A., & Ezam, Z. (2024). Exploring the Integration of AI and Cloud Computing: Navigating Opportunities and Overcoming Challenges. *TIERS Information Technology Journal*, *5*(1), 57-69. https://doi.org/10.38043/tiers.v5i1.5496

Hakimi, M., Rahmani, K. R., Ezam, Z., & Shahbazi, H. (2024). Integrating Blockchain Technology for Secure E-Government Services: Opportunities and Challenges. *Journal of Social Science Utilizing Technology*, *2*(3), 317-335. https://doi.org/10.70177/jssut.v2i3.1266

Hakimi, M., Sediqi, M., Kohistani, A. J., & Quraishi, T. (2025). The role of digital literacy and technology adoption in facilitating social transformation in Afghanistan. *Jurnal Ilmiah Dinamika Sosial*, *9*(2), 175-191. https://doi.org/10.38043/jids.v9i2.6809

Hakimi, M., Suranata, I. W. A., Ezam, Z., Samadzai, A. W., Enayat, W., Quraishi, T., & Fazil, A. W. (2025). Generative AI in Enhancing Hydroponic Nutrient Solution Monitoring. *Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi*, *8*(1), 94-103. https://doi.org/10.38043/telsinas.v8i1.6242

Kumar, B. A., Misra, N. K., Pathak, N., Ahmadpour, S., Krishnamoorthy, M., Shukla, D. K., ... & Hakimi, M. (2025). Hybrid CMNV2: DeepFake Faces Classification and Recognition using Deep Learning Methods. *Results in Engineering*, 107513. https://doi.org/10.1016/j.rineng.2025.107513

Malik, S., Malik, P. K., & Naim, A. (2024). Opportunities and challenges in new generation cyber security applications using artificial intelligence, machine learning and block chain. *Next-generation cybersecurity: AI, ML, and Blockchain*, 23-37. https://doi.org/10.1007/978-981-97-1249-6_2

Mishra, S. (2023). Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy. *Electronics*, *12*(16), 3524. https://doi.org/10.3390/electronics12163524

Nadry, Z., Sirat, A. W., Hakimi, M., & Quraishi, T. (2025). INTEGRATING BLOCKCHAIN IN EDUCATIONAL MANAGEMENT SYSTEMS: TRANSPARENCY AND ACCOUNTABILITY IN PUBLIC ADMINISTRATION. *Jurnal Ilmiah Dinamika Sosial*, *9*(2), 286-309. https://doi.org/10.38043/jids.v9i2.7079

Olutimehin, A. T. (2025). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms (February 11, 2025)*. https://dx.doi.org/10.2139/ssrn.5138889

Oye, E. (2024). Blockchain-Based Systems For Secure Machine Learning In Cybersecurity. *Available at SSRN 5080340*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5080340

Rathore, S., & Park, J. H. (2020). A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, *17*(8), 5522-5532. https://doi.org/10.1109/TII.2020.3040968

Retno, S., & Hakimi, M. (2025). Analysis of Clustering Results for Crime Incident Data in Indonesia Using Fuzzy C-Means. *Journal of Advanced Computer Knowledge and Algorithms*, *2*(3), 73-79. https://doi.org/10.29103/jacka.v2i3.22565

Selvi, K., & Dilip, G. (2024, July). Enhancing cyber-physical systems security: A review of deep learning and blockchain integration. In *2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN)* (pp. 725-734). IEEE. https://doi.org/10.3390/s21041467

Shahbazi, Z., & Byun, Y. C. (2021). Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors*, *21*(4), 1467. https://doi.org/10.3390/fi15020083

Sirat, A. W., Hakimi, M., Himmat, B., & Enayat, W. (2025). Artificial Intelligence in Educational Leadership: Strategic, Analytical, Interactive, and Decision-Making Applications for the Digital Age. *Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi*, *8*(2), 210-224. https://doi.org/10.38043/telsinas.v8i2.7044

Sirat, A. W., Hakimi, M., Himmat, B., & Enayat, W. (2025). Artificial Intelligence in Educational Leadership: Strategic, Analytical, Interactive, and Decision-Making Applications for the Digital Age. *Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi*, *8*(2), 210-224. https://doi.org/10.38043/telsinas.v8i2.7044

Talukder, M. A., Uddin, M. A., Roy, S., Ghose, P., Sarker, S., Khraisat, A. & Hakimi, M. (2025). A hybrid deep learning model for sentiment analysis of COVID-19 tweets with class

balancing. *Scientific Reports*, *15*(1), 27788. https://doi.org/10.1038/s41598-025-97778-7

Tarashtwal, O., Hakimi, M., & Naderi, Z. (2025). The Role of Artificial Intelligence in Achieving the UN Sustainable Development Goals (SDGs) in Low Income Nations. *Jurnal Ilmiah Akuntansi dan Bisnis*, *10*(2), 163-178. https://doi.org/10.38043/jiab.v10i2.7184

Unal, D., Hammoudeh, M., Khan, M. A., Abuarqoub, A., Epiphaniou, G., & Hamila, R. (2021). Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. *Computers & Security*, *109*, 102393. https://doi.org/10.1016/j.cose.2021.102393

Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports*, *14*(1), 1149. https://doi.org/10.1038/s41598-024-51578-7

Yang, C. M., Su, C. L., & Elsisi, M. (2025). A comprehensive review of blockchain and machine learning integration for cybersecurity in microgrids. *PeerJ Computer Science*, *11*, e3237. https://doi.org/10.7717/peerj-cs.3237