iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74398

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

AI Cyber-Chain: Combining AI and Blockchain for Improved Cybersecurity

Vyshnavi M[1], Pankaj Yadav[2], Satyam Kumar[3], Saurav Shanker[4], Shubh Chadha[5]
[1]*Assistant Professor, Sapthagiri College of Engineering, Karnataka, India*
[2, 3, 4, 5]*Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

Abstract: ***Cybersecurity threats are growing in scale and complexity, posing serious risks to digital infrastructure, data privacy, and economic stability worldwide. Old-style security systems often encounter challenges against advanced and coordinated cyber-attacks, particularly when they rely on centralized architectures that create single points of failure. To tackle this challenge, we introduce AICyber-Chain, a novel AI-integrated model with blockchain technology to enhance threat detection, secure data sharing, and provide tamper-proof auditability. In our approach, AI-driven algorithms analyze vast streams of network data to detect anomalies and evolving threats in real time, while blockchain ensures the integrity, transparency, and decentralization of security events and data flows. Smart contracts are employed to automate adaptive security responses, enabling systems to dynamically isolate risks and enforce security policies without human delay. Experiments using Ethereum's test network demonstrate that AICyber-Chain achieves 1.8× faster authentication and reduces gas consumption by up to 25% compared to centralized methods. Furthermore, the system shows superior resilience against DDoS attacks, scalability in enterprise environments, and financial incentives that encourage data and security rule sharing across participants. These findings underscore how combining AI and blockchain can substantially improve cybersecurity, offering a scalable, transparent, and intelligent defense framework for future digital ecosystems.***

Keywords: Cybersecurity, artificial intelligence, blockchain, smart contracts, threat detection, decentralized security.

I. INTRODUCTION

Cybersecurity has evolved into one of the most pressing issues of the digital era, with threats ranging from data breaches and ransomware attacks to large-scale disruptions such as distributed denial-of-service (DDoS) campaigns. These attacks not only compromise sensitive information but also undermine trust in financial systems, healthcare services, and critical infrastructure. Recent studies highlight that cybercrime continues to evolve in complexity and scale, costing organizations trillions of dollars annually. Protecting digital ecosystems is no longer merely a technical concern—it is crucial for protecting economies, governments, and societies.

Traditional cybersecurity systems, while effective to some extent, often rely on centralized monitoring and rule-based defenses. This makes them vulnerable to single points of failure and ill-equipped to detect emerging, highly coordinated threats. Artificial intelligence (AI) has been increasingly applied to improve detection by analyzing massive volumes of data and spotting anomalies in real time. Yet, AI systems themselves face issues of data security, trust, and centralization, which limit their reliability.

To resolve this issues, researches put forward a new approach called AICyber-Chain, which integrates AI-driven threat detection with blockchain**'s** decentralized and immutable ledger. By treating data logs and security events as transactions stored across a distributed network, the system ensures tamper-proof records while enabling real-time, intelligent analysis through machine learning. Smart contracts further automate rapid security responses, reducing human delays and ensuring policy enforcement. Early experiments on Ethereum's test network demonstrate that AICyber-Chain improves authentication speed, lowers resource costs, and enhances resilience against evolving cyber threats—showcasing how AI and blockchain together can build a more secure and trustworthy cyberspace.

II. LITERATURE REVIEW

1) Xu et al. (2019) –Blockchain For Secure Data Sharing

This study proposes a blockchain-based framework for secure and transparent data exchange, particularly in healthcare environments. By ensuring data integrity and traceability, the model overcomes challenges of trust and unauthorized access. Its decentralized ledger guarantees immutability, preventing tampering or hidden modifications. Although focused on healthcare, the approach highlights the broad potential of blockchain in cybersecurity-sensitive fields, offering inspiration for AICyber-Chain's secure sharing mechanism.

2) Khademi & Honavar (2020) – AI + Blockchain for ThreatDetection.

The authors present a dual-layer security system where AI algorithms detect anomalies in real time, and blockchain ensures the immutability of recorded events. This synergy reduces the risk of manipulated logs or false alerts. Their findings confirm that combining AI's adaptability with blockchain's trustless ledger enhances resilience against evolving threats. The approach aligns closely with AICyber-Chain's goal of transparent, decentralized, and intelligent defense.

3) Nair et al. (2021) – Blockchain in IoT Security

This research introduces a blockchain-based data transmission model for IoT networks, which are highly vulnerable to cyberattacks. Using smart contracts, the system enforces automated security policies during data exchanges, reducing risks of interception or breaches. The study illustrates how blockchain can replace fragile centralized controls with distributed verification. AICyber-Chain builds on these insights, expanding protection beyond IoT to enterprise-scale digital ecosystems.

4) Yan et al. (2021) – AI-Driven Encryption for Secure Communication.

Here, the authors apply machine learning models to dynamically adjust encryption strategies in wireless communication. By adapting to network conditions, the system strengthens protection against eavesdropping and brute-force attacks. While limited to transmission security, the research underscores the potential of AI to self-optimize defenses, a principle that AICyber-Chain extends into its adaptive smart contracts and AI-driven threat detection modules.

5) Montasari (2021) – Federated Learning for Secure AI Models

This study leverages federated learning to enable collaborative AI model training across multiple parties without sharing raw data. It ensures privacy while maintaining strong predictive performance. This distributed approach to AI complements blockchain's decentralization, pointing toward future privacy-preserving cybersecurity ecosystems. AICyber-Chain echoes these principles by combining blockchain-based trust with AI analytics in a distributed, tamper-proof environment.

6) Dou (2020) – xGEMs for Explainable AI in Security

Although not AML-specific, Dou introduces xGEM**s**, a framework that generates counterfactual explanations for black-box AI models. By highlighting which features drive predictions, it provides both interpretability and transparency. In cybersecurity, this is crucial for regulatory compliance and investigator trust. AICyber-Chain could integrate similar XAI techniques to ensure its AI threat-detection layer is transparent and accountable.

7) OriginChain (2018) – Blockchain in Supply Chain Security

The OriginChain system applies blockchain to ensure transparency and auditability in supply chains, allowing traceability of goods from source to consumer.

Though aimed at logistics, its tamper-proof design demonstrates how blockchain can enforce trust in complex, multi-stakeholder ecosystems. AICyber-Chain similarly leverages blockchain for verifiable, immutable records of cybersecurity events, strengthening trust in shared threat intelligence.

8) AICyber-Chain (Ullah et al.,2024) – Hybrid AI + Blockchain Model

The proposed AICyber-Chain system integrates AI-driven anomaly detection, blockchain-based data integrity, and smart contract–enabled automated responses. Tested on Ethereum's Rinkeby network, it achieves 1.8× faster authentication and reduces gas costs by 20–25% compared to centralized models. It also demonstrates resilience against DDoS attacks and incentivizes data-sharing by rewarding contributors. This work represents a novel hybrid framework that advances cybersecurity by merging adaptability (AI), trust (blockchain), and automation (smart contracts).

III. METHODOLOGY

In this study, we propose AI Cyber-Chain, a hybrid cybersecurity framework that integrates artificial intelligence (AI) with blockchain technology to address the growing complexity of cyber threats. The system is designed to detect malicious activity in real time, ensure data integrity through decentralization, and automate responses using smart contracts. Below is a simplified explanation of how the system works.

A. Constructing the Cybersecurity Data Network

The first step involves collecting diverse security-related data, including network traffic logs, user activities, and system performance metrics. These datasets are modeled as a graph-like structure, where each node represents an entity (e.g., user, device, server), and edges represent interactions or transactions between them. This structure enables the system to learn not only from individual events but also from relationships and interaction patterns across the digital ecosystem.

B. AI-Driven Threat Detection

The core of AI Cyber-Chain relies on machine learning models, such as anomaly detection and classification algorithms, which analyze data streams in real time.

Techniques such as:

- Supervised learning – to detect known attack signatures.
- Unsupervised learning – to uncover new and evolving threats.
- Reinforcement learning – to adaptively improve detection strategies over time.

This layered AI approach ensures that even zero-day attacks and hidden anomalies can be identified effectively.

C. Blockchain-Based Data Integrity

To guarantee trust and prevent tampering, all detected events and security logs are recorded on a blockchain ledger. Each block stores event details (e.g., timestamp, entity IDs, threat type) with cryptographic hashes to ensure immutability and traceability. By decentralizing this storage, the system avoids single points of failure prevent malicious actors from gaining access secretly alter evidence of an attack.

D. Smart Contract–Enabled Automated Response

Smart contracts deployed on the blockchain automate the enforcement of security policies. For example:

- If malware activity is detected, access permissions can be revoked automatically.
- If abnormal login behavior occurs, multi-factor authentication can be triggered.
- If a DDoS attempt is identified, compromised nodes can be isolated.

These automated responses minimize human delays and ensure real-time defense against cyber threats.

E. Collaborative Security Knowledge Sharing

AI Cyber-Chain incentivizes participants to share data and security rules across the blockchain network. Contributes earn tokens or credits when they provide high-quality security insights. This decentralized collaboration enables the creation of a shared intelligence pool, making it harder for attackers to exploit blind spots in isolated systems.

F. Training and Optimization of AI Models

The AI models are trained offline using large historical datasets that include both benign and malicious activities. To optimize performance:

- The Adam optimizer is used for efficient convergence.
- Loss functions are designed to balance false positives and false negatives.
- Feedback loops ensure continuous learning as new data and attack strategies emerge.

The trained models are then deployed for real-time inference, regularly refreshed with new data from the blockchain ledger.

G. Multi-Layered Security Analysis

The system analyzes cybersecurity risks at three distinct levels:

- Individual entities (e.g.,detecting a compromised account or device),
- Transactions/activities (e.g.,spotting suspicious network packets or logins),
- Groups of entities (e.g., identifying coordinated attacks like botnets or DDoS campaigns).

By combining these perspectives, AI Cyber-Chain can detect isolated threats along with large-scale coordinated attacks.

H. Scalability and Deployment

The system is designed for scalability in large enterprise and cloud environments. Blockchain ensures distributed, tamper-proof storage, while AI modules process data using sampling techniques to handle high volumes. Once deployed, AI Cyber-Chain supports real-time monitoring with low latency, maintaining throughput of ~50 transactions per second in testing environments.

IV. DISCUSSION

The integration of artificial intelligence (AI) with blockchain in cybersecurity marks a significant departure from conventional, siloed defense mechanisms. While traditional security systems often depend on centralized monitoring and static rule sets, AI Cyber-Chain leverages adaptive machine learning models and decentralized, tamper-proof storage to deliver more resilient protection. By embedding threat intelligence into a distributed blockchain ledger, the framework reduces reliance on trust in single entities and ensures the immutability of critical security logs.

A key strength of the model lies in its multi-layered defense: AI algorithms excel at detecting anomalies and evolving threats, blockchain guarantees integrity and transparency of recorded events, and smart contracts automate responses in real time. This synergy enables not only faster detection but also proactive mitigation of coordinated attacks such as DDoS or credential compromise. Furthermore, the incentive-based data-sharing mechanism promotes collaborative defense across participants, addressing the long-standing challenge of fragmented cybersecurity intelligence.

Despite these advances, challenges remain. Scalability is a pressing concern, as blockchain networks may struggle under heavy data loads without efficient consensus mechanisms. Similarly, while AI models improve detection accuracy, their interpretability remains limited, which could hinder adoption in compliance-driven industries. Privacy also requires careful balancing—while blockchain ensures transparency, it must integrate advanced cryptographic methods to avoid exposing sensitive security data.

.

V. CONCLUSION

The escalating scale and the heightened sophistication of cyber threads demand more intelligent, decentralized, and trustworthy solutions—AI Cyber-Chain represents a significant step in this direction. By combining the adaptability of artificial intelligence with the transparency and immutability of blockchain technology, the framework addresses critical shortcomings of conventional cybersecurity systems. Its layered approach—encompassing AI-driven anomaly detection, blockchain-based data integrity, and smart contract–enabled automated responses—offers a more resilient and proactive defense against modern cyberattacks.

This work has highlighted how AI Cyber-Chain advances beyond traditional models by ensuring tamper-proof event logging, collaborative intelligence sharing, and automated mitigation of threats in real time. Experimental results on blockchain test networks confirm improvements in authentication efficiency, resource optimization, and resilience against distributed attacks. Moreover, the system demonstrates that incentivized collaboration can help overcome the fragmentation of threat intelligence across organizations.

Nevertheless, important challenges remain. Issues of scalability, privacy preservation, and explainability of AI decisions continue to limit deployment at enterprise scale. Resolving these challenges will require innovations in lightweight consensus algorithms, integration of privacy-aware techniques such as federated learning, and the adoption of explainable AI models.

Looking ahead, cooperation between researchers, industry practitioners, and policymakers will be essential to translate frameworks like AI Cyber-Chain into operationally viable security infrastructures. Ultimately, AI Cyber-Chain is not merely a technological advancement—it signals a paradigm shift toward transparent, collaborative, and intelligent cybersecurity ecosystems capable of meeting the demands of a rapidly evolving digital world.

REFERENCES

[1] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, and W. Xiang, ‘‘Machine learning and blockchain technologies for cybersecurity in connected vehicles,’’ WIREs Data Mining Knowl. Discovery, vol. 14, no. 1, p. e1515, Jan. 2024.

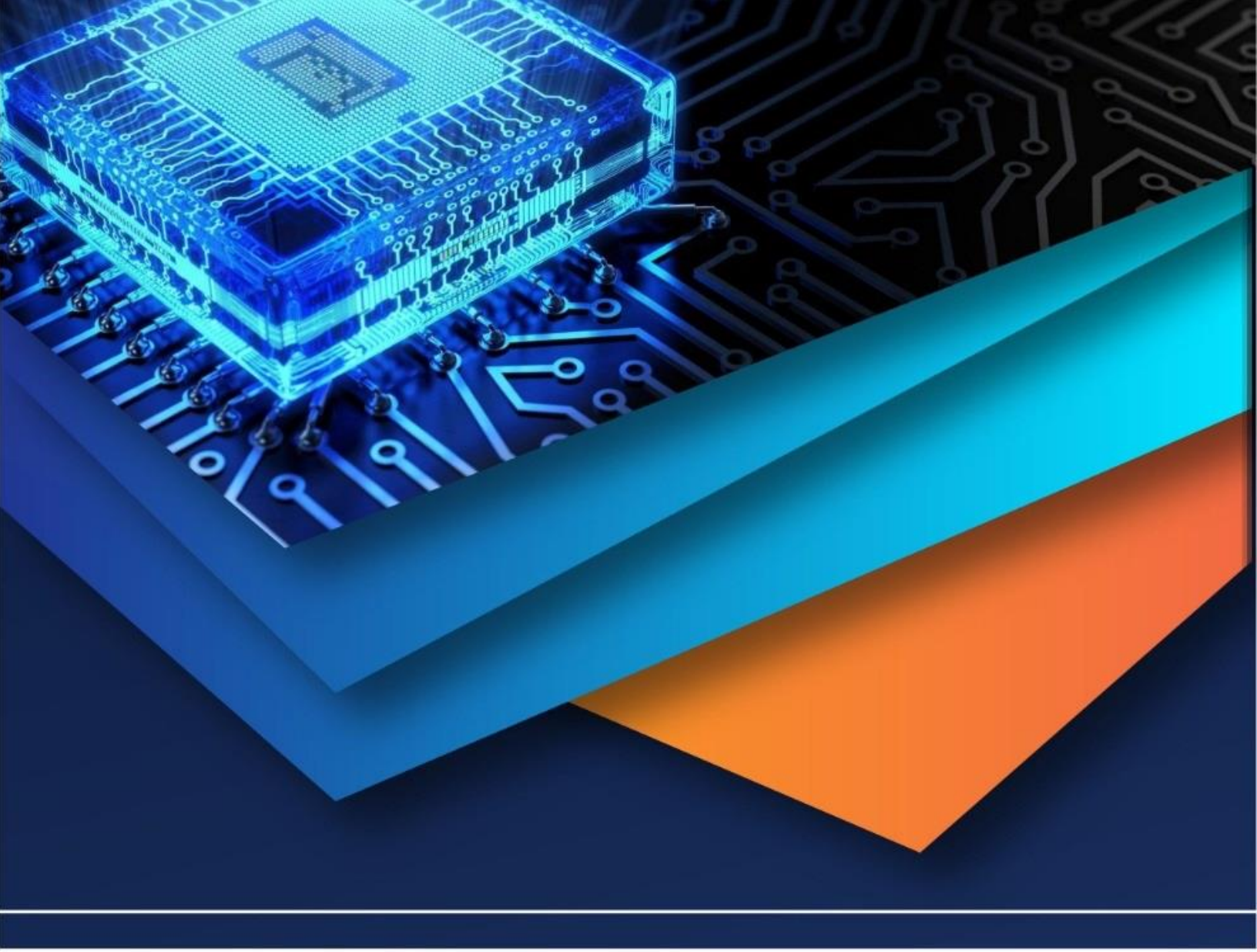
[2] M. M. Nair, A. Deshmukh, and A. K. Tyagi, ‘‘Artificial intelligence for cyber security: Current trends and future challenges,’’ in Automated Secure Computing for Next-Generation Systems. Hoboken, NJ, USA: Wiley, 2024, pp. 83–114.

[3] A. Bécue, I. Praça, and J. Gama, ‘‘Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities,’’ Artif. Intell. Rev., vol. 54, no. 5, pp. 3849–3886, Jun. 2021. [7] M. J. Molesky, E. A. Cameron, and N. W. Hawker, ‘‘Liability for breach of trust and privacy: Torts, contracts, and cybersecurity,’’ in Communication, Leadership and Trust in Organizations. Evanston, IL, USA: Routledge, 2024, pp. 287–298.

[4] H. Gutiérrez Ponce, J. Chamizo González, and M. Al-Mohareb, ‘‘Sustainable finance in cybersecurity investment for future profitability under uncertainty,’’ J. Sustain. Finance Investment, vol. 13, no. 1, pp. 614–633, Jan. 2023.

[5] V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, ‘‘Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity,’’ Int. J. Inf. Manage., vol. 68, Feb. 2023, Art. no. 102470.

[6] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, ‘‘Achieving cybersecurity in blockchain-based systems: A survey,’’ Future Gener. Comput. Syst., vol. 124, pp. 91–118, Nov. 2021.
[7] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, ‘‘Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment,’’ IEEE Access, vol. 10, pp. 36978–36994, 2022. C. Warmke, ‘‘What is bitcoin,’’ Inquiry, vol. 67, no. 1, pp. 25–67, Jan. 2024.
[8] C. Meurisch and M. Mühlhäuser, ‘‘Data protection in AI services: A survey,’’ ACM Comput. Surveys, vol. 54, no. 2, pp. 1–38, Mar. 2022.
[9] K. Wang, J. Dong, Y. Wang, and H. Yin, ‘‘Securing data with blockchain and AI,’’ IEEE Access, vol. 7, pp. 77981–77989, 2019.
[10] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, ‘‘Cyber-security threats and side-channel attacks for digital agriculture,’’ Sensors, vol. 22, no. 9, p. 3520, May 2022.
[11] H. Xu, B. Xiao, X. Liu, L. Wang, S. Jiang, W. Xue, J. Wang, and K. Li, ‘‘Empowering authenticated and efficient queries for STK transactionbased blockchains,’’ IEEE Trans. Comput., vol. 72, no. 8, pp. 2209–2223, Aug. 2023.
[12] R. Montasari, ‘‘Introduction: Cyberspace, cyberterrorism and the international security in the fourth industrial revolution: Threats, assessment and responses,’’ in Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. Berlin, Germany: Springer, 2024, pp. 1–15.
[13] R. Yan, ‘‘‘Chitty-chitty-chat bot’: Deep learning for conversational AI,’’’ in Proc. IJCAI, vol. 18, 2018, pp. 5520–5526.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY