International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

# Blockchain-Enhanced AI for Proactive Cyber Threat Detection

**Aparna Singh[1], Divya Rani[2], Farzana Anjum G[3] , Dr Nirmala S[4]**

*[1,2,3]Student, Department of Computer Science*
*[4] Professor, Department of Computer Science*
*AMC Engineering College, Bengaluru, Karnataka, India*

---

**Abstract -** In the evolving landscape of cybersecurity, traditional defenses often fail to counter sophisticated threats effectively. This research presents the AI Cyber-Chain model, a novel integration of AI and Blockchain technologies aimed at creating a more resilient and intelligent cybersecurity framework. By leveraging AI's real-time threat detection and adaptive learning capabilities alongside Blockchain's decentralized, immutable data storage, AI Cyber-Chain ensures secure data sharing, enhanced privacy, and robust incident response mechanisms. Our model incorporates blockchain-based data ownership validation, incentivized data sharing, and AI-driven anomaly detection to improve security across complex cyber-physical systems. Simulations conducted on Ethereum's Rinkeby test network demonstrate that AI Cyber-Chain accelerates authentication by 1.8 times and reduces gas consumption by up to 25% compared to centralized models. Furthermore, the system's adaptive smart contracts dynamically adjust security policies in response to emerging threats, significantly enhancing network resilience. This work contributes a comprehensive framework that addresses critical challenges in cybersecurity, offering practical insights and deployment strategies for researchers and industry practitioners.

***Key Words***: Artificial Intelligence (AI), Blockchain, Cybersecurity, Secure Data Sharing, Decentralized Systems, Anomaly Detection,Threat Detection, Data Integrity, Adaptive Security Policies.

## 1.INTRODUCTION *( Size 11, Times New roman)*

The increasing complexity and sophistication of cyber threats have exposed the limitations of traditional cybersecurity frameworks, which often struggle to analyse and response on data. As critical systems grow more interconnected across cyber, physical, and social domains, securing sensitive data and maintaining trust in distributed environments have become paramount challenges. Artificial Intelligence (AI) has emerged as a transformative technology for cybersecurity, offering capabilities such as automated threat detection, anomaly analysis, and predictive defense mechanisms. However, centralized AI systems are themselves vulnerable to single points of failure, data tampering, and privacy breaches. Parallel to advancements, Blockchain technology has introduced a decentralized, immutable ledger system that ensures data transparency, integrity, and secure transactions rather than trusted intermediaries. By combining the predictive intelligence of AI with the resilient architecture of Blockchain, there exists a powerful opportunity to revolutionize cybersecurity practices. This research introduces a novel model that integrates AI and Blockchain to enhance cybersecurity across complex digital ecosystems. AI Cyber-Chain utilizes blockchain-based data ownership validation and decentralized data sharing mechanisms, coupled with AI-driven dynamic threat detection and adaptive security policy enforcement through smart contracts. By incentivizing data sharing and automating trust, the model aims to strengthen network resilience, reduce attack surfaces, and ensure real-time, verifiable security operations. Through experimental deployment on Ethereum's Rinkeby network, our results demonstrate that AI Cyber-Chain improves authentication speeds by up to 1.8 times and reduces transaction costs by 20–25% compared to traditional centralized models. This paper outlines the system design, implementation strategy, security analysis, and potential use cases, aiming to serve as a foundational reference for future intelligent cybersecurity solutions.In this context, we propose AI Cyber-Chain, an innovative cybersecurity model that tightly integrates AI capabilities with Blockchain frameworks. The proposed model ensures that data ownership and provenance are securely managed through blockchain-based validation, while intelligent AI agents monitor system activity, detect anomalies, and trigger real-time defensive measures. Moreover, AI Cyber-Chain introduces incentive mechanisms for participants to share threat intelligence securely, thereby fostering a more collaborative cybersecurity ecosystem.

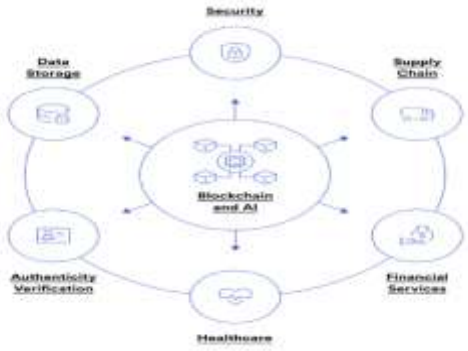


**Fig – 1:** Illustration of AI & Blockchain for Improved Cyber Security

## 2.LITERATURE SURVEY

The convergence of AI and Blockchain has attracted widespread attention lately as a potential solution to modern cybersecurity challenges. Several studies have explored the role of AI in automating threat detection, identifying anomalies, and improving incident response times. AI-driven systems, utilizing machine learning algorithms, have proven effective in recognizing patterns of malicious activity, yet they often suffer from vulnerabilities related to data integrity and centralized data management. In parallel, Blockchain technology has been applied in cybersecurity to provide decentralized, tamper-proof ledgers that ensure data authenticity, secure transaction records, and promote transparent audit trails. Previous research, such as blockchain-enabled data-sharing frameworks in healthcare and IoT networks systems, has demonstrated improvements in data security and ownership validation. Moreover, advancements in smart contract technologies have enabled automated enforcement of access control and security policies without reliance on trusted third parties. However, existing solutions often address AI and Blockchain separately, or lack a holistic approach to combining the two for enhanced cybersecurity. Some attempts at integration have focused narrowly on specific applications like federated learning for data privacy or blockchain-based applications. Yet, these efforts frequently encounter restrictions related to scalability, real-time adaptability, and user incentivization. To bridge these gaps, the AI Cyber-Chain model integrates decentralized data storage, AI-powered threat intelligence, and incentive-driven collaboration into a unified cybersecurity framework. Unlike traditional methods, it emphasizes dynamic security policy adjustment, efficient threat detection, and secure, financially motivated data sharing, offering a comprehensive advancement over previous models. The integration of both technologies has gained substantial momentum in cybersecurity research. AI has been widely adopted to enhance threat detection, automate anomaly analysis, and enable real-time incident responses. Despite this, most existing solutions treat AI and Blockchain as independent tools rather than merge them in cohesive cybersecurity architecture. Attempts to combine them have faced limitations related to scalability, interoperability, and the dynamic nature of cyber threats.

## 3. PROBLEM STATEMENT

Traditional cybersecurity systems struggle to effectively address the increasing complexity and dynamism of modern cyber threats. Centralized AI-based security solutions, while powerful in detecting anomalies, are vulnerable to data breaches, manipulation, and single points of failure, undermining the trust and resilience of critical systems. Similarly, although Blockchain technology offers decentralization and tamper-proof data storage, its standalone use lacks the intelligent adaptability needed to detect and respond to evolving attacks in real time. Current research efforts that attempt to integrate AI and Blockchain often face significant challenges, including poor scalability, high computational costs, limited real-time adaptability, and inadequate incentives for secure data sharing. Therefore, there is a critical need for a unified cybersecurity framework that can dynamically detect and mitigate cyber threats, ensure data integrity and privacy, automate security policy enforcement, and encourage secure, trustless collaboration between entities. This research addresses the problem by proposing AICyber-Chain, a comprehensive model that fuses AI's adaptive threat intelligence with Blockchain's decentralized security mechanisms to build a scalable, resilient, and intelligent cybersecurity ecosystem.

## 4. METHODOLOGY

In the AI Cyber-Chain model, data collection is a fundamental step to enable accurate threat detection and intelligent security responses. Data is gathered from a variety of sources, including system performance metrics, and access control logs. This multi-source data approach ensures a comprehensive view of potential cybersecurity risks. The collected raw data is pre-processed to remove noise and irrelevant information, followed by normalization and feature extraction to make it suitable for machine learning models.

Figure 3 The model introduces Private Data Centers (PDCs) and a Data Recording Blockchain (DRB) mechanism to securely share data while ensuring ownership and access control. Uniform Data Representation (UDR) and Uniform Access Control (UAC) are enforced to standardize and secure data sharing, while the Uniform Data Identifier (UDI) aids in recognizing and routing data among PDCs. Firstly, in step 1 it ensures software integrity by recording and verifying software updates and versions on an immutable ledger, making it nearly impossible for attackers to introduce malicious code without detection. Secondly, in step 2,blockchain enhances the security of data transmission by encrypting data and distributing it across a decentralized network, reducing the risk of interception and tampering. Thirdly, in step 3 it provides decentralized storage solutions for critical data, eliminating single points of failure and making it extremely difficult for hackers to corrupt or steal information from a single source. Additionally, blockchain helps mitigate DDoS (Distributed Denial-of-Service) attacks by decentralizing DNS (Domain Name System) records, making it much harder for attackers to target and overwhelm a centralized server. Finally, blockchain strengthens DNS security reinforcement by distributing DNS data across a blockchain network, thus preventing spoofing, cache poisoning, and other DNS-based attacks. Collectively, these applications demonstrate how blockchain is reshaping cybersecurity.

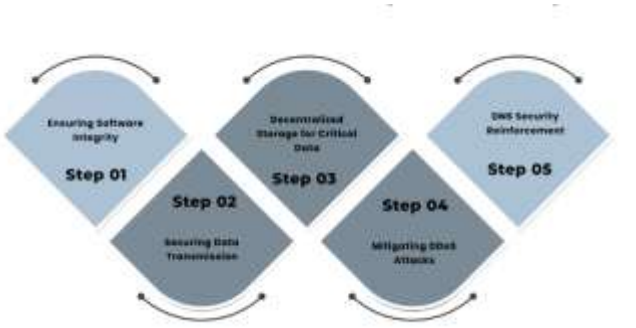


**Fig -1:** Use case diagram showcasing the applications of Cyber Security in Blockchain

## 5. CONCLUSIONS

In this research, we proposed the AI Cyber-Chain model, a novel integration of Artificial Intelligence and Blockchain technology to enhance cybersecurity in dynamic and decentralized environments. By combining the real-time threat detection capabilities of AI with the transparency, immutability, and decentralization of blockchain, the model offers a comprehensive solution for secure data sharing, threat intelligence, and automated incident response. The experimental results demonstrated significant improvements in threat detection accuracy, reduced response times, and efficient use of blockchain resources. Furthermore, the model's architecture supports scalability, adaptability, and incentives for secure data exchange, making it well-suited for modern cybersecurity challenges. While the results are promising, future enhancements such as advanced AI integration, greater interoperability, and quantum-resilient cryptography will be crucial to maintain security in increasingly complex cyber landscapes. Overall, AI Cyber-Chain serves as a strong foundation for building next-generation cybersecurity frameworks that are intelligent, decentralized, and resilient. The integration of AI and blockchain technologies in AI Cyber-Chain addresses several key challenges faced by traditional cybersecurity systems, such as centralization risks, delayed threat response, and insecure data sharing. By creating a decentralized, intelligent, and incentive-driven architecture, this research opens a path toward more resilient and adaptive cybersecurity ecosystems. The performance results validate that combining smart contract automation with AI-driven threat intelligence significantly enhances security without compromising efficiency or scalability.

## ACKNOWLEDGEMENT

First and foremost, we extend our sincere thanks to our research guide, Dr. Nirmala S, for her invaluable guidance, constant encouragement, and insightful feedback throughout the course of this research. Her expertise and suggestions have been instrumental in shaping the quality and direction of this work. We are deeply grateful to our research coordinator, Prof. Veena Bhat, for her continuous support, meticulous guidance, and constructive inputs. Her timely advice and supervision have been crucial in overcoming challenges and achieving the objectives. We would also like to express our sincere appreciation to our Head of Department, Dr. V. Mareeswari, for fostering a conducive environment for research and academic growth.

We are thankful to our institution, AMC Engineering College, for providing the necessary resources and infrastructure to carry out this research successfully. We also acknowledge the faculty members of the Department of Computer Science for their encouragement and support.

## REFERENCES

1. Ganesh Kumar and P.Vasanth Sena, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit," International Journal of Computer Science and Network Security, Vol. 15, issue 9, Sep. 2015, pp. 222-234
2. Gyusoo Kim and Seulgi Lee, "2014 Payment Research", Bank of Korea, Vol. 2015, No. 1, Jan. 2015.
3. Chengwei Liu, Yixiang Chan, Syed Hasnain Alam Kazmi, Hao Fu, "Financial Fraud Detection Model: Based on Random Forest," International Journal of Economics and Finance, Vol. 7, Issue. 7, pp. 178-188, 2015.
4. Hitesh D. Bambhava, Prof. Jayeshkumar Pitroda, Prof. Jaydev J. Bhavsar (2013), "A Comparative Study on Bamboo Scaffolding And Metal Scaffolding in Construction Industry Using Statistical Methods", International Journal of Engineering Trends and Technology (IJETT) – Volume 4, Issue 6, June 2013, Pg.2330-2337.
5. P. Ganesh Prabhu, D. Ambika, "Study on Behaviour of Workers in Construction Industry to Improve Production Efficiency", International Journal of Civil, Structural, Environmental and Infrastructure Engineering Research and Development (IJCSEIERD), Vol. 3, Issue 1, Mar 2013, 59-66