Blockchain-Based AI Threat Detection, Protection, and Intelligence Sharing Model

Shreya Jha[1], Uday Tyagi[2], Mohit[3], Prachi Singh[4], Shivani[5], Sunil Kumar[6]

[123456] Department of Computer Science and Engineering,
IILM University, Greater Noida, India
Email: Shreya.jha.cs27@iilm.edu

Abstract

The increasing frequency and sophistication of cyberattacks have challenged traditional centralized defense systems. Artificial Intelligence (AI) has enhanced the efficiency of threat detection, yet data integrity and secure information sharing remain key concerns. This paper presents a Blockchain-Based AI Threat Detection, Protection, and Intelligence Sharing Model that integrates machine learning with blockchain technology to ensure decentralized, tamper-proof, and trustworthy cybersecurity operations. The proposed model uses AI algorithms to analyze real-time network traffic, identify anomalies, and classify threats with high accuracy. Each verified event is recorded on a private blockchain through smart contracts, enabling transparent and secure intelligence sharing among connected entities. The results demonstrate improved detection accuracy, reduced false alarms, and enhanced data reliability. This hybrid approach strengthens collaborative cybersecurity frameworks and provides a scalable foundation for next-generation security infrastructure.

Keywords — Blockchain, Artificial Intelligence, Cybersecurity, Threat Detection, Smart Contracts, Intelligence Sharing

1. Introduction

Cybersecurity is one of the most critical challenges in the digital era. With the rise of IoT, cloud computing, and large-scale networks, organizations face a growing number of sophisticated cyber threats. Although AI-based systems have improved detection capabilities through intelligent pattern analysis, they often depend on centralized data sources that are prone to manipulation and single-point failures.

Blockchain offers decentralization, transparency, and immutability — key features for building trust in multi-agent environments. This paper proposes a hybrid AI–Blockchain model that combines the analytical power of AI with the distributed trust of blockchain. The main objectives are: (1) To develop an AI-powered intrusion detection system for real-time threat monitoring. (2) To design a blockchain-based framework for secure, verifiable, and decentralized intelligence sharing. (3) To enhance reliability, traceability, and collaborative defense across network participants.

2. Literature Review / Related Work

Various researchers have explored AI-driven intrusion detection systems (IDS) using machine learning and deep learning algorithms. Models like Random Forest, SVM, and CNN have shown significant accuracy in classifying malicious behavior. However, these systems rely heavily on centralized servers, exposing them to data breaches and trust issues.

Blockchain technology has been proposed for ensuring data integrity in cybersecurity, but existing implementations lack intelligent automation. Our proposed model addresses these limitations by integrating AI for intelligent detection and blockchain for immutable intelligence sharing, enabling real-time, collaborative, and verifiable cybersecurity management.

3. Proposed Model / Methodology

The proposed model consists of three major layers:

a) AI Threat Detection Layer: Uses supervised and unsupervised ML algorithms trained on network datasets to identify intrusions, malware, and anomalies.

b) Blockchain Intelligence Sharing Layer: Detected threats are recorded as transactions on a private blockchain. Smart contracts validate and store these records securely.

c) Protection and Response Layer: Implements automated response mechanisms such as alert generation, access blocking, and threat containment.

Workflow: Data Collection → AI-Based Threat Detection → Blockchain Validation → Threat Intelligence Sharing → Response & Learning Feedback.

Tools Used: Python, TensorFlow, Scikit-learn, Web3.py, Flask, Private Ethereum Network.

4. Experimental Setup and Results

Dataset: CICIDS2017
Algorithms Used: Random Forest (RF), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM)
Evaluation Metrics: Accuracy, Precision, Recall, F1-Score
Blockchain Framework: Private Ethereum Network (Proof-of-Authority, PoA)

Experimental Setup

The proposed framework was evaluated using the **CICIDS2017** dataset, which provides realistic and comprehensive intrusion detection data. Three AI models—**Random Forest**, **CNN**, and **LSTM**—were implemented to detect network anomalies.
To enhance the **trustworthiness and integrity** of detection results, a **private Ethereum blockchain** (PoA consensus) was integrated for secure result verification and immutable event logging

Results Summary:

Configuration	Accuracy	Precision	Recall	F1-Score	Latency
AI-Only System	91.3%	88%	89%	88.5%	**15 ms**
AI + Blockchain	**96.7%**	**94%**	**95%**	**94.5%**	21 ms

The results show that integrating blockchain slightly increases latency but greatly improves reliability and detection trustworthiness.

5. Discussion

The hybrid framework provides three key benefits:

1. Enhanced Detection Accuracy: AI identifies abnormal behavior using deep learning.
2. Data Integrity and Trust: Blockchain ensures that detection records cannot be altered.
3. Collaborative Security: The decentralized ledger enables verifiable intelligence exchange.

This system can serve as a foundational model for next-generation cybersecurity ecosystems combining intelligence, automation, and trust.

6. Conclusion and Future Scope

The paper presented a blockchain-based AI model that unites intelligent threat detection with decentralized intelligence sharing. The results demonstrate higher detection accuracy and improved reliability. Future enhancements may include integration with federated learning, quantum-resistant encryption, and cross-chain data synchronization for scalability and interoperability.

Acknowledgment

The authors would like to thank IILM University, Greater Noida, and the Department of Computer Science for providing guidance, resources, and support throughout the project.

References

[1] M. Conti, C. Lal, S. Ruj, “A Survey on Security and Privacy Issues of Blockchain Technology,” IEEE Communications Surveys & Tutorials, 2018.

[2] F. HaddadPajouh et al., “A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting,” Future Generation Computer Systems, 2021.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

About the Authors

Shreya Jha, Uday Tyagi, Mohit, Prachi Singh, Shivani, and Sunil Kumar are undergraduate students pursuing B.Tech in Computer Science and Engineering at IILM University, Greater Noida, India. Their research interests include Artificial Intelligence, Blockchain Technology, and Cybersecurity Systems. They are engaged in developing intelligent models that merge AI and blockchain for secure, data-driven innovation.