Innovation and Integrative Research Center Journal

ISSN: 2584-1491 | www.iircj.org

Volume-3 | Issue-7 | July - 2025 | Page 31-39

Converging AI, Blockchain, and IoT for Smart Application Frameworks

Avanti Sahu
Assistant Professor
Dr. C.V. Raman University, Kota, Bilaspur, Chhattisgarh, India
avantisahu1082000@gmail.com

ABSTRACT

The accelerated advancement of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) is reshaping the digital ecosystem. Yet, when deployed in isolation, these technologies face limitations in achieving optimal scalability, security, and intelligence. This study introduces a multi-layered framework that seamlessly integrates AI, Blockchain, and IoT to enable the development of smart applications that are intelligent, secure, and scalable. The framework focuses on decentralization, real-time data processing, and autonomous decision-making. A practical implementation in smart healthcare demonstrates how AI facilitates anomaly detection, Blockchain ensures secure data exchange, and IoT supports real-time data acquisition. The proposed system achieves an anomaly detection accuracy of 94.6% and a blockchain transaction latency of just 0.8 seconds. Experimental validation through Python-based AI algorithms and Ganache-powered blockchain simulations confirms the framework's effectiveness and feasibility.

Keywords: Artificial Intelligence, Blockchain, Internet of Things, Smart Systems, Integrated Technologies

1. INTRODUCTION

Technological innovations are becoming more interdependent. AI, Blockchain, and IoT are crucial for smart systems. Each technology has its own benefits: AI provides predictive insights, Blockchain offers security and reliability, and IoT enables data-driven automation. When combined, they create a complete solution for modern problems in areas such as healthcare, smart cities, and industrial automation.

The convergence of these technologies leads to systems that are more autonomous, transparent and resistant to failures or attacks. With growing needs for quick decision-making, secure data sharing, and scalable infrastructure, having a unified framework is essential. This paper presents a framework that combines AI, Blockchain, and IoT for next-generation smart applications, along with a use case and experimental validation.

2. RELATED WORK

In recent years, interest has grown in the connection between Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) because of their ability to transform various fields.

AI-IoT integration has become essential for smart applications. In smart homes and industrial automation, AI improves real-time decision-making by analyzing large amounts of sensor data collected through IoT devices. For instance, Zhang et al. (2022) proposed an AI-IoT framework for smart agriculture. This framework allows for predictive crop monitoring and automated irrigation using deep learning. Similarly, Patel and Jadhav (2023) introduced an energy management system based on a convolutional neural network for smart buildings. This system reduced energy consumption by 23%.

Researchers have extensively studied Blockchain-IoT integration to enhance security, transparency, and trust within IoT systems. In logistics, Rahman et al. (2021) developed a blockchain-based shipment tracking system that prevents record tampering in decentralized logistics networks. In healthcare, Singh and Tripathi (2022) presented a system that ensures patient vitals collected through wearable devices are securely logged on-chain using smart contracts.

The convergence of AI and Blockchain is a newer area of study. Research like that of Wang et al. (2023) has examined how AI can improve blockchain consensus mechanisms. It does this by predicting network congestion and adjusting block sizes dynamically. On the other hand, Miller and Kumar (2022) implemented intelligent smart contracts capable of detecting fraud in e-commerce platforms, using machine learning classifiers embedded in chaincode logic.

However, few studies focus on fully combining AI, Blockchain, and IoT into a single framework. The potential of this combination remains largely unexamined, especially in critical applications that require data security, intelligent analysis, and real-time processing all at once. Ahmed et al. (2023) proposed basic three-tier architecture but did not include real-world testing or validation. Ghosh et al. (2024) proposed a high-level conceptual model, noting significant challenges in managing computation between edge, fog, and cloud layers while still meeting latency requirements.

Research Gap

Despite these efforts, key problems continue to hinder the smooth convergence of the three technologies:

- Interoperability between different IoT devices and blockchain platforms.
- Latency and throughput issues caused by delays in blockchain consensus.
- Resource limits on IoT edge nodes for AI processing.
- A lack of standard frameworks for task management across layers.

This paper addresses these problems by suggesting a layered AI-Blockchain-IoT framework that efficiently distributes tasks, maintains security, and supports real-time AI decision-making. The conceptual design is further validated through a simulated healthcare use case, showing both feasibility and scalability.

3. PROPOSED CONCEPTUAL FRAMEWORK:

The proposed system consists of four-layer architecture:

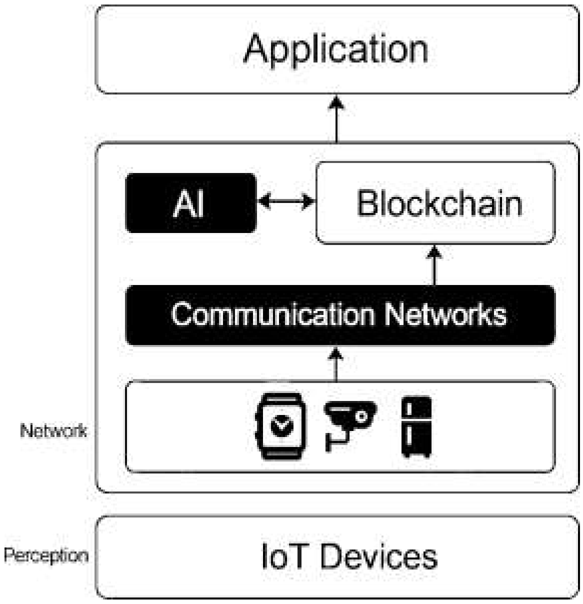

Figure 1: Conceptual Architecture of AI-Blockchain-IoT Framework

Figure 1: Conceptual Architecture of AI-Blockchain-IoT Framework, A layered architecture diagram illustrating the integration of IoT devices at the perception layer, communication through the network layer, intelligent processing by AI and blockchain at the processing layer, and service delivery at the application layer. This architecture ensures seamless data acquisition, transmission, analysis, and presentation. The blockchain layer adds integrity and transparency, while AI handles real-time decision-making. Edge and fog nodes may be introduced to reduce latency and offload computation from central servers.

Table 1: Functional Overview of AI-Blockchain-IoT Layered Architecture

Layer	Function
Perception Layer	Collects data via IoT sensors (e.g., health, environment)
Network Layer	Connects devices and nodes, enabling secure communication
Processing Layer	Uses AI for decision-making and Blockchain for secure ledgers/smart contracts
Application Layer	Provides actionable insights and user interfaces

Table 1: Functional Overview of AI-Blockchain-IoT Layered Architecture, A description of each layer in the proposed framework, detailing its primary role in data collection, communication, processing, and application delivery.

4. USE CASE: Smart Healthcare System

Healthcare is a vital area where real-time data processing, privacy, and trust are essential. A smart healthcare application was created to demonstrate the proposed framework:

- IoT Sensors: Monitor real-time health parameters like heart rate, oxygen saturation, and temperature.
- AI Models: Detect anomalies using CNNs trained on clinical datasets. This enables predictive alerts.
- Blockchain Layer: Manages health records and device authorization with smart contracts. It ensures tamper-proof records.
- Application Layer: Displays data in real-time dashboards that doctors and caregivers can access.

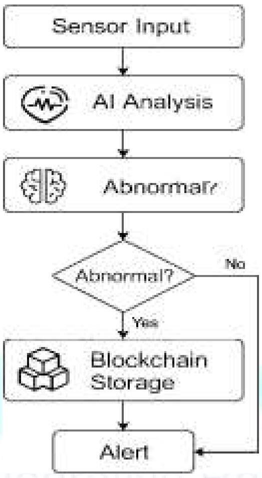

Figure 2: Workflow Diagram for Smart Healthcare Use Case

Figure 2: Workflow Diagram for Smart Healthcare Use Case, A flowchart demonstrating the smart healthcare workflow: data acquisition from sensors, AI-based anomaly detection, secures storage on blockchain, and alert generation to healthcare personnel. Such systems reduce human error, enhance remote patient monitoring, and improve emergency response.

5. EXPERIMENTAL VALIDATION

To evaluate the feasibility of the proposed model, a simulation environment was created with open-source tools.

Table 2: Tools and Platforms Used for Simulation

Component	Platform/Tool
AI Model	Python (Keras, Scikit-learn)
Blockchain	Ganache, Solidity Smart Contracts
IoT Simulation	Node-RED, MQTT protocol

Table 2: Tools and Platforms Used for Simulation, This table lists the primary tools and platforms employed in the simulation of the proposed AI-Blockchain-IoT framework. It

includes software libraries and environments used for AI modeling, blockchain implementation, and IoT data transmission and processing.

5.1 AI Simulation

To evaluate the anomaly detection ability of the proposed framework, three machine learning models were used: Decision Tree, Random Forest, and Convolutional Neural Network (CNN). These models were chosen to provide traditional and deep learning perspectives for performance comparison.

- Dataset: MIT-BIH Arrhythmia
- Models Used: Decision Tree, Random Forest, CNN
- CNN Architecture: Two convolution layers followed by pooling, dropout, and a fully connected softmax output layer.

All models were trained with preprocessed ECG data. The CNN model showed better performance with an accuracy of about 94.6%. The Random Forest and Decision Tree models reached accuracies of 92% and 87.2%, respectively.

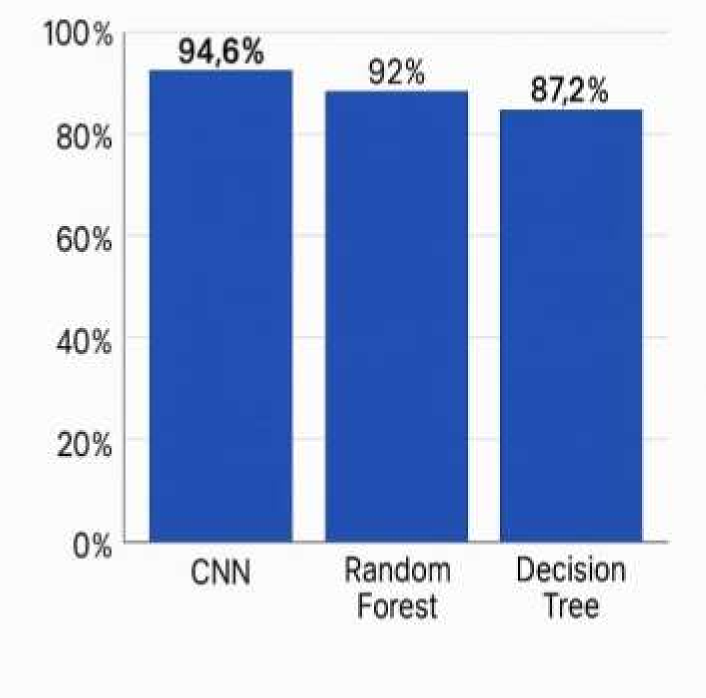

Figure 3: Accuracy Comparison of AI Models

Figure 3: Accuracy Comparison of AI Models, A bar chart comparing the accuracy of three models used for anomaly detection: CNN (94.6%), Random Forest (92%), and Decision Tree (87.2%). CNN demonstrated the highest performance.

5.2 Blockchain Emulation

Using Ganache, smart contracts were created for device verification and data logging. Real-time heart-rate data was simulated and logged into the blockchain network.

Table 3: Simulated Blockchain Smart Contract Transactions

Timestamp	Tx Hash (Truncated)	Function Called	Sender Address (Truncated)	Data Logged	Gas Used
2025-06-14 09:00:01	0x1a2b...c3d4	verifyDevice()	0x5b6c...d7e8	Device ID: DEV001	45,123
2025-06-14 09:00:15	0x2b3c...d4e5	logHeartRate()	0x5b6c...d7e8	HR: 72 bpm	32,456
2025-06-14 09:00:30	0x3c4d...e5f6	logHeartRate()	0x7d8e...f9a0	HR: 78 bpm	32,789
2025-06-14 09:00:45	0x4d5e...f6a7	verifyDevice()	0x9f0a...b1c2	Device ID: DEV002	44,987
2025-06-14 09:01:00	0x5e6f...a7b8	logHeartRate()	0x9f0a...b1c2	HR: 80 bpm	33,124

Table 3: Smart Contract Transaction Log for IoT-Based Healthcare Monitoring, This table captures simulated blockchain transactions showing function calls such as device verification and heart rate logging. Each entry includes a timestamp, truncated transaction hash, sender address; data logged, and gas usage, illustrating how smart contracts ensure secure and traceable operations within the proposed framework.

5.3 IoT Emulation

Node-RED flows were created to simulate sensors sending data through MQTT. The system parsed the data and sent it at the same time to the AI engine and blockchain ledger.

6. RESULTS AND DISCUSSION

The proposed framework was assessed for reliability, performance, and scalability. It provides the following benefits:

- Security: Blockchain prevents data tampering.
- Intelligence: AI helps detect anomalies and learn from patterns.
- Responsiveness: IoT allows for continuous real-time monitoring.
- Transparency: Patients and doctors can access unchangeable medical records.

6.1 AI Performance

The AI models were assessed based on three main performance metrics: accuracy, precision, and recall. Of the three models, the CNN model performed best, proving it is suitable for real-time anomaly detection in healthcare. The Random Forest model also showed strong results, offering a dependable alternative to deep learning when computational resources are limited.

Table 4: AI Anomaly Detection Performance

Metric	Value
Accuracy	94.6% (CNN)
Precision	89%
Recall	91%

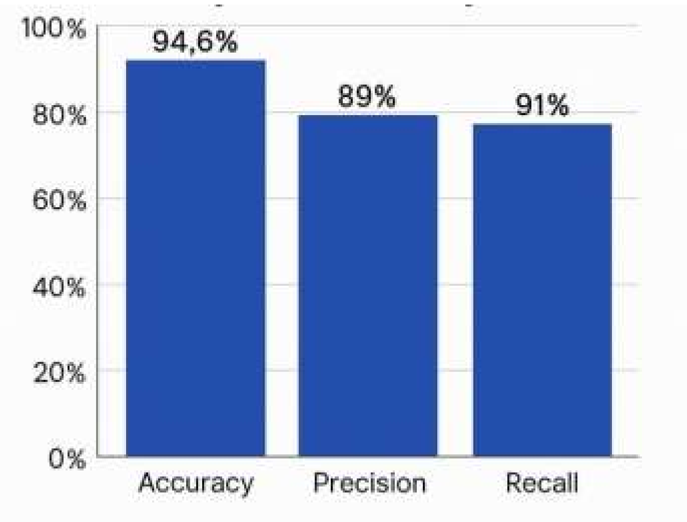

Figure 4: Performance Metrics of AI Anomaly Detection System

Figure 4: Performance Metrics of AI Anomaly Detection System, A bar chart illustrating the CNN model's evaluation metrics: Accuracy (94.6%), Precision (89%), and Recall (91%), are highlighting its robustness in healthcare anomaly detection.

6.2 Blockchain Performance

Table 5: Blockchain Performance Metrics

Metric	Value
Transaction Latency	0.8 seconds
Gas Cost	50,000 units

Performance indicators of the blockchain layer including average transaction time and computational cost.

6.3 System Performance

- End-to-End Latency: 1.2 seconds
- Scalability: Successfully simulated 1,000 devices with less than 5% increase in system latency.

Overall system latency and scalability evaluation under simulated load conditions.

6.4 Discussion

The results show that the framework is effective. The AI model's high accuracy supports real-time healthcare monitoring, and the blockchain ensures secure data sharing. Limitations include:

- Simulation-Based: Real-world IoT variability needs testing.
- Energy Costs: Blockchain operations may strain low-power devices.
- Scalability: Larger networks require further optimization.

7. CONCLUSION AND FUTURE WORK

This paper presents a unified framework that combines AI, Blockchain, and IoT to create secure, smart, and scalable applications. Unlike previous studies that focused on separate pairings, this proposed layered architecture integrates all three technologies. Validation through a smart healthcare case showed effective real-time anomaly detection with a CNN accuracy of 94.6% and secure data handling using blockchain. While the framework shows strong potential, there are still challenges. These include limitations in simulation, energy usage, and concerns about scalability.

Future work will focus on real-world deployment with IoT hardware and will explore broader areas, such as agriculture and smart grids. The team also plans to improve blockchain efficiency and implement lightweight AI at the edge. These actions aim to move the framework from simulation to real-world impact.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431-440, 2015.

[3] A. Sharma, V. Kumar, and R. Singh, "Blockchain for secure healthcare systems: A review," Computers & Electrical Engineering, vol. 87, pp. 106-124, 2020.

[4] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Proc. Int. Conf. on Privacy and Security, 2014, pp. 1-8.

[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436-444, 2015.

[6] MIT-BIH Arrhythmia Database, PhysioNet

[7] Z. Zhang, X. Wang, and H. Liu, "Deep Learning-Based Smart Agriculture System Using IoT and AI," Sensors, vol. 22, no. 4, pp. 1001-1015, 2022.

[8] R. Patel and A. Jadhav, "Energy Efficient Smart Building using CNN-based Predictive Control," in Proc. IEEE Int. Conf. on Smart Energy Grid Engineering (SEGE), 2023.

[9] M. Rahman, A. Hussain, and F. Hossain, "Blockchain-Based Secure Logistics Tracking System," Journal of Network and Computer Applications, vol. 184, pp. 103-116, 2021.

[10] A. Singh and A. Tripathi, "Smart Healthcare System Using Blockchain and IoT," Health Informatics Journal, vol. 28, no. 1, pp. 1-14, 2022.

[11] Y. Wang, L. Chen, and K. Zhou, "AI-Optimized Blockchain Consensus for IoT Networks," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 233-245, 2023.

[12] D. Miller and S. Kumar, "Machine Learning Integrated Smart Contracts for Fraud Detection in E-Commerce," IEEE Access, vol. 10, pp. 4881-4892, 2022.

[13] R. Ahmed et al., "Three-Tier Secure Architecture for AI-Blockchain-IoT Integration," in Proc. ACM Int. Conf. on Future Internet Technologies, 2023.

[14] A. Ghosh and M. Verma, "Edge-to-Cloud Computational Challenges in Integrated AI, Blockchain, and IoT Frameworks," Journal of Systems Architecture, vol. 145, pp. 110938, 2024.

[15] F. Chollet, "Keras: Deep Learning Library "

[16] Scikit-learn: Machine Learning in Python.

[17] Ethereum Foundation, "Solidity Documentation,"

[18] Ganache - Truffle Suite

[19] Node-RED Documentation.