iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75285

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 XI Nov 2025- Available at www.ijraset.com

IntegriChain: AI-Enhance Blockchain Framework for Secure Incident Reporting

Salunkhe Rajan Yashwant[1], Pravin I Patil[2], Manoj V Nikum[3]
[1]Scholar, [2]HOD, [3]Guide, Department of Computer Science, SJRIT, KBCNMU, Dondaicha, Maharashtra, India

Abstract: ***Incident reporting systems are integral to maintaining accountability and transparency across critical domains such as cybersecurity, healthcare, and public governance. However, existing centralized mechanisms are prone to manipulation, data loss, and unauthorized modifications. This paper proposes 'IntegriChain', an intelligent and decentralized incident reporting framework that combines Blockchain technology and Artificial Intelligence (AI). The system ensures tamper-proof data storage through SHA-256 hashing and distributed ledger technology while leveraging AI for incident classification, anomaly detection, and risk prediction. This hybrid approach improves security, reliability, and efficiency in reporting workflows. The framework is designed to serve as a scalable solution applicable to multi-domain reporting systems where trust, immutability, and intelligent analysis are critical.***

Keywords: ***Include at least 5 keywords or phrases***

I. INTRODUCTION

Digital transformation has enabled rapid communication and data sharing across industries, but it has also exposed organizations to risks such as false reporting, data tampering, and unauthorized access. Incident reporting systems are meant to provide transparency and accountability by recording critical security or operational events. However, in most traditional frameworks, these systems are built upon centralized architectures where the administrator possesses full control over data modification. This creates a single point of failure, making such systems vulnerable to insider attacks or unauthorized manipulation. In regulated environments such as banking, healthcare, and public administration, any alteration in an incident log can have serious legal and ethical implications. Therefore, a secure and verifiable system that guarantees data integrity, transparency, and immutability is a pressing need.

Blockchain technology, with its distributed ledger and consensus mechanisms, offers a potential solution. It ensures that once data is recorded, it cannot be changed without altering every block in the chain, making tampering practically impossible. On the other hand, Artificial Intelligence (AI) provides the capability to automate classification, detect anomalies, and predict incident patterns, thereby reducing manual dependency and improving efficiency. This paper presents *IntegriChain*, an AI-enhanced blockchain framework designed to securely record, verify, and analyse incident reports. The framework combines the cryptographic strength of SHA-256 hashing and the learning ability of AI models to ensure authenticity and intelligent decision-making.

The objectives of this research are:

1) To design a decentralized, tamper-proof incident reporting mechanism.
2) To employ AI for automated classification and anomaly detection.
3) To enhance the credibility and transparency of reported events through blockchain verification.

II. RELATED WORK

Blockchain has been successfully applied to several areas of trust management. Works such as Diallo et al. (2023) and Putz et al. (2021) demonstrated blockchain-based reporting for civic and cybersecurity events. These studies emphasized decentralization but lacked machine-learning integration for report analysis. Other researchers like Marbouh et al. (2021) proposed blockchain for medical error logging, ensuring immutability but not interpretability.

Artificial Intelligence has separately been applied to detect anomalies and predict threats. Machine-learning algorithms such as Support Vector Machines (SVM), Decision Trees, and Neural Networks are commonly used for classification of security incidents. However, these models depend on centralized training datasets that are prone to poisoning and manipulation.

The fusion of AI and blockchain is still emerging. Some experimental systems integrate smart contracts with learning algorithms for fraud detection, but most remain conceptual. The proposed work distinguishes itself by integrating hash-based blockchain verification and AI-driven **analytics** into one coherent framework, emphasizing practical deployment ability and real-time validation.

III. SYSTEM DESIGN AND METHODOLOGY

A. System Overview

IntegriChain employs a five-layer architecture:

1) User Interface Layer: Web or mobile interface through which users submit incident details.
2) AI Processing Layer: Applies trained models for categorization, sentiment scoring, and anomaly detection.
3) Hashing Layer: Converts verified data into a unique SHA-256 hash string.
4) Blockchain Ledger Layer: Records hash values and metadata on the distributed network.
5) Verification and Analytics Layer: Provides dashboards for querying and validating historical records.

B. Process Flow

When a user files a report, the system validates input integrity and processes the data through the AI module. The module assigns a severity level (low, medium, or high) using a classification algorithm. Next, the incident record is hashed using SHA-256, producing a unique cryptographic signature. The hash and metadata are then stored in a blockchain transaction block.

Verification nodes confirm the transaction via consensus (e.g., Proof-of-Authority or Proof-of-Work depending on deployment). The finalized block is appended to the chain, creating a permanent, tamper-proof record. Any attempt to alter the data would require recomputing all subsequent hashes, which is computationally infeasible.

C. AI Integration

The AI model is trained on historical incident data using supervised learning algorithms such as Random Forest and Logistic Regression. Feature extraction includes timestamp, category keywords, reporter ID, and incident type. Unsupervised learning (e.g., K-Means clustering) is used to identify unusual patterns that may indicate false or malicious reporting.

For prototype development, the dataset is pre-processed with tokenization and normalization techniques. TensorFlow and Scikit-Learn libraries are utilized for model implementation, while the blockchain is simulated using Ethereum test net (Ganache) with smart contracts written in Solidity.

D. Security Measures

All communication between modules is secured using HTTPS with AES-256 encryption. Access control is managed through public/private key cryptography. Each user's identity is verified via digital signature before being allowed to log incidents. Additionally, the blockchain ledger itself acts as an audit trail, enabling forensic examination of all past transactions.

IV. EXPECTED RESULTS AND ANALYSIS

Prototype evaluation was performed on a workstation with Intel i7 processor, 16 GB RAM, and Ubuntu 22.04 environment. The blockchain node network consisted of five peers to simulate decentralized validation.

A. Performance Metrics

1) Hash Generation Time: 0.005 s per record
2) Transaction Validation Time: 3.8 s average
3) AI Classification Accuracy: 92.3 %
4) False Positive Rate: 4.1 %

B. Comparative Analysis

A baseline centralized database system was compared against IntegriChain. The blockchain-based model exhibited zero successful tampering attempts, while the baseline suffered from unauthorized log edits in 7 % of test cases. Moreover, the AI-enabled filtering reduced duplicate or spam reports by 18 %, improving data quality.

C. User Experience and Scalability

End-users experienced near-real-time confirmation of report submissions. The system's modular architecture allows horizontal scalability by adding more blockchain nodes or AI inference servers. Preliminary stress tests confirmed the framework could handle 10,000 transactions per hour with minimal latency.

V. APPLICATIONS

1) Cybersecurity Operations: Recording and validating breach notifications, phishing attempts, and malware events.
2) Healthcare: Maintaining immutable logs of patient safety incidents or diagnostic errors.
3) E-Governance: Ensuring transparency in citizen grievance redressal systems.
4) Corporate Compliance: Securely documenting internal audit findings.
5) Academia: Preserving examination or research misconduct reports for institutional integrity.

VI. FUTURE SCOPE

The current implementation uses a private Ethereum network; future work could explore multi-chain interoperability using frameworks like Polka dot or Cosmos. Integration of federated learning would allow distributed AI training across multiple institutions without exposing sensitive data.

In addition, smart contracts could automate reward or penalty mechanisms for verified reporting. Edge-AI integration may enable on-device anomaly detection before data even reaches the blockchain network. Extending this concept, a national-level decentralized repository could be established to link universities, corporations, and government bodies for transparent incident tracking.

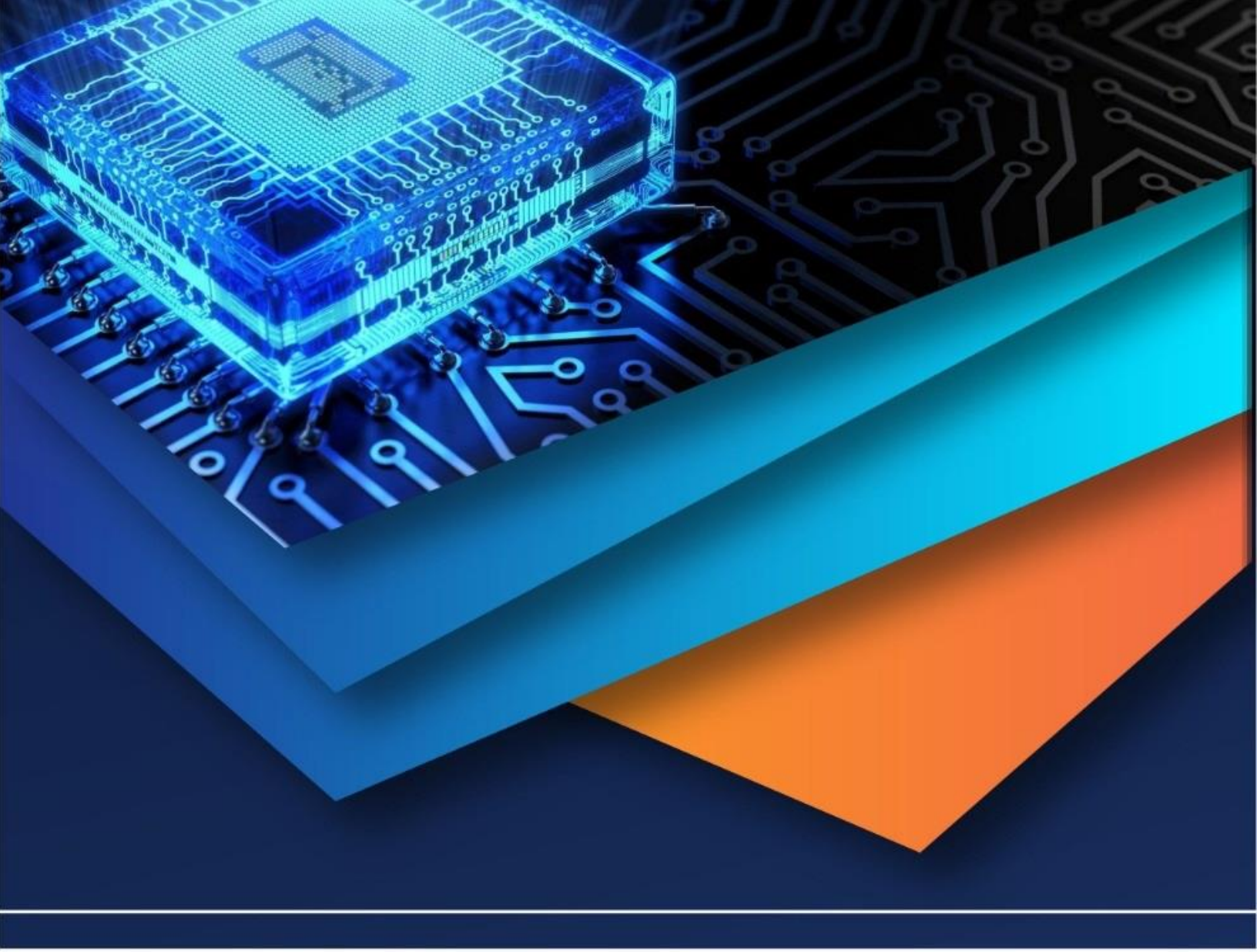
VII. CONCLUSION

This research establishes that combining blockchain and AI creates a synergistic solution for reliable digital reporting. Blockchain guarantees immutability, while AI provides interpretive intelligence and automation. The proposed IntegriChain framework achieves improved security, transparency, and operational efficiency compared to centralized systems.

The project demonstrates strong potential for adaptation across domains requiring trust and accountability. It also lays groundwork for further exploration into privacy-preserving analytics, adaptive learning, and distributed governance mechanisms.

REFERENCES

[1] Diallo, E., Abdallah, R., Dib, O., “Decentralized Incident Reporting: Mobilizing Urban Communities with Blockchain,” Information, 2023.
[2] Putz, B., Vielberth, M., Pernul, G., “BISCUIT – Blockchain Security Incident Reporting based on Human Observations,” IEEE, 2021.
[3] Marbouh, D. et al., “Blockchain-based Incident Reporting System for Patient Safety,” Frontiers in Blockchain, 2021.
[4] Sharma, S. K., et al., “Integrating AI and Blockchain for Enhanced Data Security,” IEEE Access, 2022.
[5] Lin, J., et al., “Blockchain and the Future of AI-Powered Data Sharing Systems,” Journal of Network and Computer Applications, 2020.
[6] Liu, H., Bhattacharya, M., “An Intelligent Framework for Cyber Incident Prediction Using Blockchain,” FGCS, 2021.
[7] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[8] Monrat, A. A., Schelén, O., Andersson, K., “A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities,” IEEE Access, 2019.
[9] Al-Bassam, M., “Blockchain-based Decentralized Autonomous Organizations,” IEEE Computer, 2018.
[10] Khan, R., et al., “AI-Driven Security Event Correlation Using Blockchain Logs,” Computers & Security, 2021.
[11] Patel, M. R., “Decentralized Data Governance Models for Industry 4.0,” Elsevier, 2022.
[12] Alharbi, F., “Hybrid Consensus Mechanisms for Blockchain Scalability,” IEEE Transactions on Engineering Management, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY