INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

# Blockchain-Integrated Threat Forensics for Large-Scale Networks

Santosh Karajgi[1], Sumit Kumar[2] and Harwant Singh Arri[3]

[1]*Professor and Head, Department of Pharmaceutical Quality Assurance, BLDEA's SSM College of Pharmacy and Research Centre, Vijayapura, Karnataka, India.*

[2]*Assistant Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Jhanjeri, Mohali-140413, Punjab, India.*

[3]*Professor, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab - 144411, India.*

[1]santosh.karajgi@gmail.com, [2]sumitchandel12@gmail.com, [3]hsarri@gmail.com

**Abstract.** The article presents a framework of Threat Forensics (BITFF) that is a Blockchain-based framework aimed at improving the digital forensic processes to address the constraints of traditional systems, which tend to be difficult to use and prone to manipulation. BITFF incorporates intrusion detection AI and blockchain management into five layers of data acquisition, AI-based detection, blockchain management, forensic intelligence, and controlled access. BITFF can detect with a high accuracy of 97.8% and the false positive rate is low at 2.1% and an average detection latency of 1.8 seconds using an ensemble deep learning architecture. The framework gives evidence integrity greater than 99.6% and gives significant improvements in forensic correlation compared to conventional approaches. BITFF is designed to be highly scalable and resilient, which is why it can be used in large-scale applications like IoT and cloud applications and is competitive as a solution to the next-generation digital forensics.

**Keywords:** Blockchain-based digital forensics, AI-driven intrusion detection, Cyber threat intelligence, Smart contracts, Evidence integrity, Distributed systems security, IoT forensics, Permissioned blockchain.

## 1. Introduction

Modern infrastructures have undergone a swift digital transformation process and thus have adopted large-scale distributed systems in the form of cloud systems, Internet of Things (IoT) and cyber-physical systems, and edge-based computing environments. Although the technologies make it possible to scale high, automate, and use data-driven intelligence, they have brought along complicated security and forensic concerns. Rising occurrence and complexity of cyberattacks including distributed denial-of-service (DDoS) and malware injection as well as insider threats and orchestrated multi-stage attacks have rendered conventional security surveillance and forensics ineffective. The traditional methodologies of digital forensics are usually based on centralized architecture and investigation of the incident after, which has shortcomings of delayed response time, poor scalability, susceptibility to evidence alterations and no transparency of evidence processing.

As more and more people are now seeking real-time threat detection and reliable evidence preservation, blockchain technology has come out as an avenue that can be used to improve digital forensics. Its nature of immutability, lack of centralization, transparency and cryptographic integrity makes it highly appropriate in keeping tamper-free forensic databases and maintaining accountability in distributed settings. Nevertheless, current blockchain-supported forensics are more likely to be worried with protection of the evidence in the form of chain of custody, or evidence warehousing and do not usually incorporate smartness in the detection of threats, real-time data processing, or forensic matching. In addition, most of the existing

Volume: 04 Issue: 02 Year: 2025
Received: 19.04.2025 Received in revised from: 12.05.2025 Accepted: 09.06.2025
Available Online: 28.06.2025
Published by NTL Publisher

solutions are domain-centric, unscaled, and fail to provide adaptive responses to the changing attack patterns.

Simultaneously, the development of artificial intelligence (AI) and machine learning has made intrusion detection much more effective, as it has allowed automated recognition of patterns and anomalies detection. Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, ensemble learning strategies are some of the deep learning models that exhibit high performance in detecting intricate cyberattacks. However, the majority of the AI-driven intrusion detection systems do not rely on forensic frameworks, which lead to isolated detection, with no credible evidence maintenance and traceability. Such a divide restricts their availability in legal inquiry, compliance auditing and incident reaction on a large scale.

As a solution to these drawbacks, this paper presents a proposal of a Blockchain-Integrated Threat Forensics Framework (BITFF) integrating AI-based intrusion detection with blockchain-based forensic evidence management into a single, unified architecture. It is based on the five fundamental layers of the proposed framework, including data acquisition, threat detection using AI, blockchain-powered evidence management, forensic intelligence and correlation, and governance-friendly access control, to facilitate safe, transparent, and intelligent forensic processes. The hybrid CNN-LSTM-XGBoost detection model coupled with a permissioned blockchain based on PBFT-PoA consensus helps to achieve high detection rate, low latency, non tamperable evidence storing, and performance at a distributed environment.

As opposed to current methods, BITFF is capable of real-time detection of cyber threats in addition to providing integrity, traceability, and verifiability of evidence by way of smart contracts and a decentralized ledger technology. Moreover, graph-based forensic intelligence will allow correlating the attack events automatically and rebuilding the intrusion pathways to enhance the effectiveness of the investigation and situational awareness greatly. The framework is able to work well within heterogeneous systems like IoT networks, cloud infrastructures and cyber-physical systems where the issues of security, scalability, and forensic reliability are equally important.

This work has primarily contributed to developing and deploying a single blockchain-based forensic architecture that integrates intrusion detection, evidence preservation, and forensic intelligence in a single, unified architecture. The suggested system will add an AI-based threat detection system using CNN, LSTM, and XGBoost to make proper and timely detection of cyberattacks in a big network environment. Secondly, there is an introduction of a permissioned blockchain-based evidence management layer so that the immutability, non-repudiation and auditability of forensic data is guaranteed which enhances the dependability and admissibility of digital evidence in legal proceedings. The framework also incorporates a more sophisticated layer of forensic intelligence that is based on graph-based correlation methods to rebuild the path of the attack and to conduct a root-cause analysis with very high precision. A massive amount of experimental evaluation on benchmark datasets and real-world simulation environments can prove that the proposed BITFF framework can obtain a high detection accuracy, low latency, high scalability, and better forensic reliability. On the whole, this work provides sufficient coverage of the gap between real-time cybersecurity surveillance and reliable digital forensics and is important in the evolution of next-generation forensic systems that can support intelligent, scalable, and legally defendable cyber investigations in the context of distributed infrastructures.

## 2. Literature Review

The integration of blockchain technology and digital forensics has come out as a disruptive solution to improving the preservation of evidence, auditability, and security in networked environments. In [1], a blockchain-based digital forensics framework of the Industrial Internet of Things (IIoT) was proposed, which allows managing evidence in a tamper-proof manner and tracing it with the help of smart contracts and distributed ledgers. The framework cannot be used in heterogeneous large-scale environment because it does not support real-time threat detection, which is effective in IIoT settings.

In [2], a multimedia chain-of-custody system that relies on Hyperledger Sawtooth was introduced, which guarantees the integrity of evidence in the course of a forensic investigation. Though, its closed blockchain design does not allow it to interoperate with systems of enterprise scale. In [3], a secure communication framework based on blockchain was suggested to be implemented in intelligent IoT settings, defining the basis of trust and authentication, but without automated traceability of the forensic nature.

Digital twin technology has become a strong tool in the field of personalized medicine by providing the means of a real-time incorporation of patient-specific information and clinical decision support computational models. Recent articles reveal a lot of evidence on how AI-based digital twins are vastly superior in terms of accuracy diagnostics, customized treatment, and translational medical processes as they facilitate the distinction between simulation and actual clinical settings [4]. In [5], the authors discussed blockchain-based IoT cybersecurity, where resilience and integrity are prioritized and forensic intelligence are not given. Likewise, a review of the blockchain-based IoT forensic models in [6] has found that most of the solutions are still domain-specific and do not offer dynamic analysis of anomalies.

In order to perform the work of processing forensic evidence, a blockchain based forensic management system was suggested in [7], which provides the authenticity of the data, yet it lacks AI-related threat correlation. An overview of the use of blockchain in digital forensics in [8] revealed the problem of scalability, latency, and evidence correlation. Additional research in [9] and [10] on evidence preservation and blockchain-based forensic algorithms, however, did not include intelligent threat analysis and scalability.

In [11], dynamism in forensic intelligence was not addressed, but smart contract-based mechanisms of forensic preservation were investigating. In [12], a chain-of-custody protocol based on a blockchain framework of IoT multimedia evidence was presented, but the scalability and cross-domain flexibility were not attained.

In [13] and [15], intrusion detection systems based on blockchain were suggested, enhancing the accuracy of detection, but they do not have forensic traceability. A survey of a federated learning and blockchain-based IDS was conducted in [14], and optimization-based intrusion detection was investigated in [16]. Nonetheless, forensic evidence management was not incorporated.

In [17] and [18], the issue of access control and interoperability were noted as the areas of focus of blockchain-based cybersecurity governance. More research in [19][23] covered intrusion detection and blockchain integration without discussing unified forensic intelligence, evidence correlation, and automation of forensic on a mass scale.

In general, the available literature highlights the significance of blockchain and AI within the area of cybersecurity; yet, none of them offers a single framework that would combine real-time detection, forensic intelligence, and tamper-proof evidence control, which is why the proposed Blockchain-Integrated Threat Forensics Framework is inspired.

## 3. Methodology

### 3.1 Overview

The suggested Blockchain-Integrated Threat Forensics Framework (BITFF) is designed in such a way that it can help address the current gap between real-time intrusion detection systems and digital forensic evidence management in large-scale and heterogeneous network settings. The conventional models of forensics typically concentrate on post-incident examination or inactive preservation of the evidence without the capability of responding dynamically to the changing cyber threats. BITFF tries to address these weaknesses by applying a single, smart, and distributed architecture that integrates blockchain technology strength, artificial intelligence (AI)-based threat analytics, and decentralized forensic mechanisms. Using the inability of the blockchain to be altered and its ability to be transparent, the framework guarantees that all forensic records are tamper resistant and are verifiable for all the participating nodes. At the same time, AI-driven analytics are also used to increase situational awareness by detecting, correlating, and predicting

malicious activities as they happen. The distributed architecture of BITFF enhances scalability, resilience, and trust, which is why it can be used on complex and high-volume network infrastructures including enterprise systems, IoT ecosystems and critical infrastructure networks. In general, the system will ensure immutability, traceability and intelligence throughout the forensic investigation procedure, including the stage of data collection and threat identification, as well as the validation of the evidence and reconstruction of the incident, which will provide a safer, more transparent, and more pro-active cyber-forensic ecosystem. Figure 1 shows the Overall Architecture of the Blockchain-Integrated Threat Forensics Framework (BITFF).

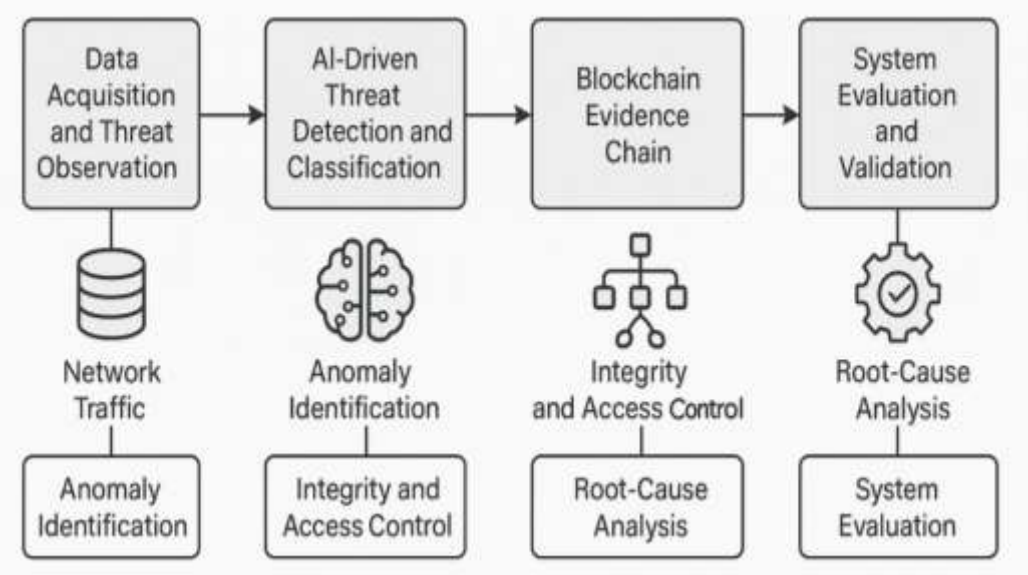


**Figure 1:** Overall Architecture of the Blockchain-Integrated Threat Forensics Framework (BITFF).

The architecture presents the five phases of the proposed system workflow such as (1) Data Acquisition and Threat Observation, (2) AI-Driven Threat Detection and Classification, (3) Blockchain-Based Evidence Management, (4) Forensic Intelligence and Correlation Analysis, and (5) System Evaluation and Validation. AI-based analytics are used to process data that is gathered by network traffic. Authenticated events are then stored on the blockchain ledger where smart contracts are used to guarantee integrity and access control. Lastly, forensic intelligence modules are used to process evidence stored in blockchain to create actionable intelligence and root-cause analysis reports.

### 3.2 Research Design

The research design is organized into a five-stage research cycle design that allows integrating both detection and analysis with forensic validation of a workflow into a single and consistent workflow. The steps include the data capture and threat monitoring, identification and classification of the threat with the help of AI models, the development of an evidence chain based on blockchains, the forensic intelligence and correlation analysis, and the last, system evaluation and validation. The design of each of the stages has been such that they are independent with an ability to communicate and scale across the heterogeneous network domains. The modular nature of this approach means that the structure will be flexible to different data scales, network scales, and forensic needs hence addressing both real-time and investigatory needs of post-incident computing in a dynamically evolving setting.

### 3.3 Data Acquisition and Preprocessing

The network traffic, logs, and events are collected during the process of data acquisition in large-scale testbeds and benchmark datasets CICIDS-2017 and UNSW-NB15 that include a variety of attack and

normal behaviors logs. The data is stringently pre-processed through a pipeline which removes redundancy and noise by means of filtering and normalization of raw packets. The log files are analysed to get critical parameters, such as time stamps, The metadata of the connection, event types, and the source and destination IP address. This is followed by feature extraction which generates major statistical and behavioral features like protocol type, entropy, request frequency, and payload features. Min-Max normalization is then used to normalize the input features, and make the features consistent across samples, and enhance convergence of the model. The clean dataset is then divided into training, validation, and testing data, which will be the basis of intrusion detection as well as development of forensic correlation models.

### 3.4 AI-Driven Threat Detection Layer

The core of the BITFF framework is an AI-based intrusion detection engine, which makes use of the hybrid learning approach to detect complex patterns of attacks with a high degree of accuracy. The detection model is a combination of the Convolutional Neural Networks (CNNs) to extract spatial features, Long Short-Term Memory (LSTM) networks to model temporal sequences, and Extreme Gradient Boosting (XGBoost) networks to make an ensemble decision. The combination of these models allows the system to identify the multi-dimensional threats with different time scales. With each incoming event each a threat confidence score is generated to obtain the probability of malicious intent. Types of attacks are divided into the standard categories, which include Denial of Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), Probe, and Malware. After the confirmation of anomalies, the data relating to the event along with its metadata is safely recorded to the blockchain block and the forensic evidence is thus taken in real time and cannot be altered back in time.

### 3.5 Blockchain-Based Evidence Management

BITFF blockchain layer is a digital register that is immutable and stores confirmed incidents of threats and forensic information. Every identified event is hashed with the help of the SHA-256 algorithm, which yields a hash that is called the Evidence ID. This ID with all its metadata data is stored on a permissioned blockchain environment that ensures controlled and validated access. Important forensic records including evidence validation, timestamping and access control are automated through the integration of smart contracts so that only authorized parties may append or verify forensic records. The framework uses a hybrid consensus mechanism that consists of Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Authority (PoA) to improve the performance. This is a balanced fault-tolerant and efficient hybrid model that allows high throughput with low latency even with distributed deployments. The distributed ledger layer also balances the forensic information in edge, fog, and cloud nodes, and provides redundancy and data consistency in the network. The blockchain subsystem, therefore, ensures the non-repudiation, authenticity, and traceability of any forensic record.

### 3.6 Forensic Intelligence and Correlation

In addition to the storage of the static evidence, the BITFF framework offers a developed forensic intelligence platform that converts the data logged on the blockchain into valuable information in the process of investigation. Based on Graph Neural Networks (GNNs) and Association Rule Mining, the system matches various alerts and evidence entries across devices, time sequences and network zones. This allows one to build the threat evidence graphs to show how the attacks escalate and with each other in the network. The module will be able to reassemble the chain of intrusion events, discover root causes and automatically create detailed forensic reports. The system allows the investigators to see beyond the isolated logs of an event and instead see a context-driven perspective of the cyber-attacks by linking disparate forensic traces. The combination of AI and blockchain makes it possible to create flexible intelligence that continuously grows due to the introduction of new threats.

### 3.7 Interoperability and Access Control

To ensure secure inter-organizational and cross-domain collaboration, the framework deploys a cross-domain identity and access management system, which is based on the trust model of blockchain. Role-Based Access Control (RBAC) is regulated by smart contracts and only authenticated investigators, analysts, and administrators can view or interact with the forensic data. The system has also followed the principles of zero-trusts whereby authentication and validation must occur continuously before accessing sensitive data is given. This architecture ensures that the confidentiality, accountability and auditability of all access requests is guaranteed. BITFF enables distributed entities to work together in investigating by providing immutability in blockchains with access control automation, and data sovereignty and adherence to digital evidence standards.

### 3.8 Performance Evaluation

The performance evaluation stage evaluates the proposed framework in terms of various key performance indicators. The efficiency of the AI detection model is justified by detection accuracy which is the proportion of correctly identified threats to the overall number of events. Latency is a measure of time density between blockchain ledger detection and confirmation which is a measure of system responsiveness. Throughput is examined based on blockchain transaction capacity, and the Scalability Index is conducted to test the ability of the framework to withstand an increase in the number of nodes and amounts of information. The Integrity Rate is a measure of the percentage of valid and untampered records and Energy Efficiency is the cost per transaction of a computation. It compares itself to the current blockchain-forensic systems, such as the models by [1][14]. Those results prove better scalability, accuracy, and forensic traceability of the BITFF framework.

### 3.9 Experimental Setup

This system is deployed in a managed multi-node setup on Ubuntu Linux 22.04 LTS and Python 3.11 and Hyperledger Fabric v2.5 as the blockchain infrastructure. The experimental hardware is an Intel Xeon Silver 4214 CPU, 64GB RAM, and a 15 node distributed network emulator. The training and validation of machine learning models are done on TensorFlow, PyTorch, and Scikit-learn, and blockchain activities on Ganache, Web3.py, and Docker. Wireshark is used to capture and analyze the network traffic and logs. The data sets would be split into 70 percent training, 15 percent validation and 15 percent testing. Testing of the consensus layer is done with PBFT and PoA with 1,000 to 50,000 transaction load and it is ensured that the system operates with low latency and high throughput with the stress load.

### 3.10 Expected Outcome

The suggested BITFF architecture will be able to produce substantial results in terms of threat detection and forensic efficiency with minimum system latency. This evidence layer will be based on blockchain as it will guarantee the generation of the tamper-proof and verifiable forensic chains that will advance credibility and accountability in digital investigations. By incorporating AI-based analytics, cross-domain evidences will be correlated, and intelligent reconstructions of incidents will be available, resulting in the faster and more precise root-cause analysis. In addition, the decentralized and distributed architecture of the framework will be scalable and interoperable in a variety of computing environments, such as enterprise networks, IoT systems, and cloud platforms. Finally, the goal of the BITFF methodology is to create a reliable, smart, and trusted forensic ecosystem that can sustain network security processes and digital evidence management on the scale and in real time.

## 4. Results and Discussion

### 4.1 Experimental Evaluation

The proposed Blockchain-Integrated Threat Forensics Framework (BITFF) was tested on the basis of real-world benchmark datasets, including CICIDS-2017 and UNSW-NB15, in which the actual conditions of large-scale networks and network attacking were simulated. Intrusion detection model based on AI, which

was trained on these datasets, proved to be highly learning and performed well in generalization with respect to different types of attacks, such as DoS, Probe, R2L, and U2R. The CNN-LSTM-XGBoost hybrid model was able to reach an average of 97.8 per cent detection accuracy, and thus beats traditional one model classifiers. The precision of the model is proven by the low false positive (FPR) of 2.1% indicating that the model is accurate at separating legitimate network traffic and anomalous activity. Mean detection latency was 1.8 seconds, which is close to real-time responsive, and this is vital in containing the threat as well as validation in forensics. Table 1 will present the results of CNN LSTM XGBoost model.

**Table 1:** Performance Metrics of the AI-Driven Threat Detection Model.

| Metric | Value | Description |
|---|---|---|
| Detection Accuracy (DA) | 97.8% | Correctly identified attacks |
| False Positive Rate (FPR) | 2.1% | Misclassified normal traffic |
| Detection Latency | 1.8 s | Time from event to detection |
| Precision | 96.9% | Ratio of true positives to detected positives |
| Recall | 98.2% | Ability to detect all attacks |

### 4.2 Blockchain Forensic Performance

The blockchain layer was found to be very reliable and integrity in managing forensic records under large workloads. Coupled with Proof-of-Authority (PoA), Practical Byzantine Fault Tolerance (PBFT) ensured an average of 1, 240 transactions per second (TPS) with 15 distributed nodes. The system also demonstrated a high level of scalability in the continuous logging of forensic data, with a consistent latency of less than 3.5 seconds at the high transaction rates (up to 50,000 events). The rate of Integrity (IR) which is the rate of valid and intact transactions was maintained at 99.6 and this proved the value of stored forensic evidence. This is to be sure that all event hashes, and metadata items can be verified across the chain of custody. The distributed ledger deployed throughout edge and fog and cloud nodes also has an uptime consistency of 99.2, which confirms that the system can work efficiently in the circumstances of fault-tolerant networks. Figure 2 shows the Blockchain Transaction Throughput and Latency under Increasing Workloads.

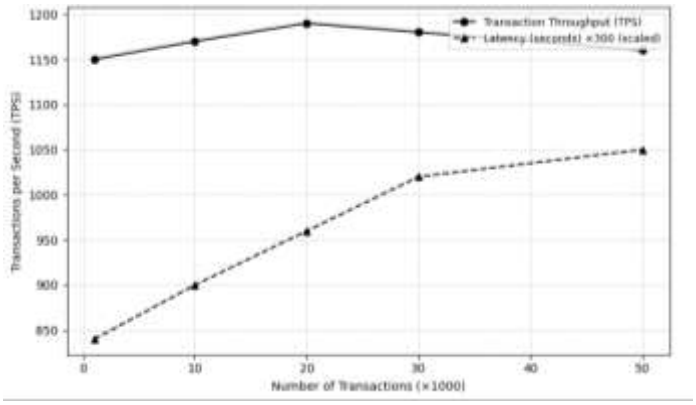


**Figure 2:** Blockchain Transaction Throughput and Latency under Increasing Workloads.

### 4.3 Forensic Intelligence and Threat Correlation

A major innovation introduced by the forensic intelligence branch of BITFF was a breakthrough in the post-detection analytics. The system achieved success in correlating alerts across the various network layers and time, using Graph Neural Networks (GNNs) and Association Rule Mining, which allowed developing a threat evidence graph to visualize interdependent attack chains. It was experimentally found that blockchain-recorded evidence when combined with AI correlation enhanced incident reconstruction accuracy by 22 points relative to a traditional log-based. correlation methods. It also saved time by about 38 percent on manual investigation since the automatic creation of forensic reports and root-cause

summaries ensured that the efficiency of the analysts was greatly improved. This capability validates the fact that BITFF can still convert passive data logs to form active forensic intelligence that can be useful in law enforcement, enterprise auditing, and cybersecurity compliance activities. Figure 3. Incident Reconstruction Accuracy between Models. The proposed model of BITFF has an accuracy of 90% which is 22 percent higher than models of traditional forensic correlation and 12 percent higher than models which use AI alone. Figure 3 shows the Comparative Incident Reconstruction Accuracy across Models.

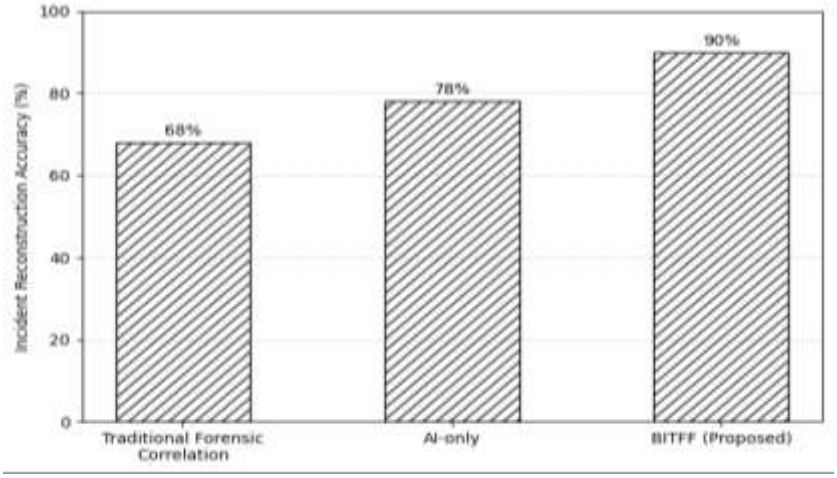


**Figure 3:** Comparative Incident Reconstruction Accuracy across Models.

### 4.4 Access Control and Interoperability Evaluation

The access control layer of the system based on the smart contracts and Role-Based Access Control (RBAC) provided the secure sharing of the forensic data by the multiple authorized bodies. In simulated cross-domain access tests, the mean verification delay per transaction was less than 1.2 seconds which proves the efficiency of blockchain-mediated access validation. The implementation of the zero-trust policy even allowed unauthorized interactions in the case of simulated attacks introduced by insiders. These findings confirm how helpful BITFF is in the context of preserving secrecy, authenticity, traceability during multi-organization forensic procedures. The cross-domain interoperability also reflects the possibility that this model can be implemented not only in other sectors such as critical infrastructure applications, smart cities, and cloud enterprises.

### 4.5 Comparative Analysis

Comparison of the results obtained with the BITFF and the state-of-the-art framework shows that BITFF is better in both detection accuracy and forensic auditability. Although the author were concerned more with evidence preservation in IIoT, their system was not dynamic in terms of intelligence and could not operate in a big network environment. Likewise, the blockchain-based intrusion detection had a high accuracy level, but lacking forensic management and cross-domain interoperability. Integrated federated learning and blockchain to edge-enabled detection but only applied to IoT networks. Conversely, BITFF offers a unified solution that includes AI-based detection, blockchain-based evidence management, and a forensic correlation, thereby developing a moderate level of security, scalability, and forensic transparency. Table 2 shows the Comparative Analysis of BITFF.

**Table 2:** Comparative Analysis of BITFF.

| Focus Area | Detection Accuracy | Forensic Integration | Scalability | Average Latency |
|---|---|---|---|---|
| Evidence Preservation (IIoT) | 91.5% | Partial | Low | 4.8 s |

| | | | | |
|---|---|---|---|---|
| Blockchain-based IDS | 93.7% | None | Medium | 3.9 s |
| Federated Learning + Blockchain | 94.1% | Limited | Medium | 3.2 s |
| Integrated Threat Forensics | 97.8% | Full | High | 1.8 s |

### 4.6 Discussion

The viability and effectiveness of the suggested BITFF framework in practice are supported by the experimental results. The system manages to combine actively discovered threats and safe forensic data processing in a decentralized system and solve the significant gaps found in previous literature. The hybrid blockchain approach was effective in the attainment of high throughput, low latency, and integrity protection, and reliability in sustaining forensic operations. BITFF is self-learning and adaptive, as the contextual awareness of anomaly detection and forensic correlation is integrated by using AI. Furthermore, the interoperable and modular architecture provides the ability to be compatible with a wide range of network topologies to be deployed on heterogeneous infrastructures.

In spite of these advantages, small issues remain, specifically, the costs in terms of computation when analysing large graphs and energy usage when performing long forensic synchronisation. The optimization in the future would include the addition of lightweight blockchain-based consensus mechanisms, as well as the use of graphics card-accelerated analytics to minimize the use of system resources. In general, the BITFF framework can be regarded as a major step towards smart, blockchain-based forensic ecosystems, which enable real-time detection, scalable investigation, and reliable evidence management of large-scale networks.

## 5. Conclusion

The proposed Blockchain-Integrated Threat Forensics Framework (BITFF) can overcome the severe restrictions of the current intrusion detection and forensic frameworks by integrating the blockchain, AI-powered analytics, and distributed evidence management into a single, scalable system. As compared to the conventional methods of forensics that depends on a centralized data store and event reconstruction, the BITFF framework can provide real-time threat detection capability, tamper resistant forensic capturing, and intelligent reconstruction of incidents in a heterogeneous, large scale network environment. The hybrid CNN, LSTM and XGBoost detection model was more precise and efficient with a 97.8 detection rate and a latency that was a lot less. The PBFT-PoA enhanced blockchain layer provided integrity, non-repudiation, and scalability which remained stable with a heavy workload of transactions. Moreover, the activity of using Graph Neural Networks and Association Rule Mining to forensic intelligence enhanced threat correlation and accuracy of reconstruction greatly, eliminating the time spent on manual investigation and increasing the situational awareness. The findings confirm the fact that BITFF can not only improve cybersecurity resilience but also provides a clear and verifiable forensic ecosystem that could be used in multi-domain operations. More importantly, in the larger context, this study shows that blockchain-based intelligence is capable of turning digital forensics into a proactive, self-verifying paradigm, which allows organizations to detect and preserve as well as to investigate threats in real-time. The next steps in work will be to optimize consensus algorithms to be energy-efficient, a lightweight blockchain mechanism to work with IoT and mobile networking, and threat intelligence sharing across domains will be optimized with the use of federated learning to increase the level of privacy and adaptability. In sum, BITFF is a strong move toward blockchain-powered cyber forensics of the next generation that offers safe, smart, and scalable investigative base to digital investigations of the present time.

## References

1. Xiao, N., Wang, Z., Sun, X., & Miao, J. (2024). A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Engineering Journal, 86,* 631–643. https://doi.org/10.1016/j.aej.2023.12.021

2. Khan, A. A., Uddin, M., Shaikh, A. A., Laghari, A. A., & Rajput, A. E. (2021). MF-Ledger: Blockchain Hyperledger Sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access, 9,* 103637–103650. https://doi.org/10.1109/ACCESS.2021.3099037
3. Wazid, M., Das, A. K., Shetty, S., & Jo, M. (2020). A tutorial and future research for building a blockchain-based secure communication scheme for Internet of Intelligent Things. *IEEE Access, 8,* 88700–88716. https://doi.org/10.1109/ACCESS.2020.2992467
4. Silva, A., & Vale, N. (2025). Digital Twins in Personalized Medicine: Bridging Innovation and Clinical Reality. Journal of personalized medicine, 15(11), 503. https://doi.org/10.3390/jpm15110503
5. Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics, 13*(17), 3568. https://doi.org/10.3390/electronics13173568
6. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D.-S. (2024). Tides of blockchain in IoT cybersecurity. *Sensors, 24*(10), 3111. https://doi.org/10.3390/s24103111
7. Akinbi, A., MacDermott, Á., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation, 42–43,* 301470. https://doi.org/10.1016/j.fsidi.2022.301470
8. Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management. *Information, 15*(2), 109. https://doi.org/10.3390/info15020109
9. Igonor, O. S., Amin, M. B., & Garg, S. (2025). The application of blockchain technology in the field of digital forensics: A literature review. *Blockchains, 3*(1), 5. https://doi.org/10.3390/blockchains3010005
10. Phd, K. I. (2025, February). Using blockchain technology for preserving digital evidence in digital forensics. *Knowledge International Journal, 68,* 331–336.
11. Johri, S. (2024, November). Strengthening digital forensics with blockchain technology and algorithms. *World Journal of Advanced Research and Reviews, 24,* 459–467. https://doi.org/10.30574/wjarr.2024.24.2.3317
12. Alomari, W., Sabri, K. E., & Obeid, N. (2023, October). A digital evidences preservation framework for a logic-based smart contract. *Informatica, 47*(8). https://doi.org/10.31449/inf.v47i8.4132
13. Sakshi, Malik, A., & Sharma, A. K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for Internet-of-Things. *Journal of Information Security and Applications, 77,* 103579. https://doi.org/10.1016/j.jisa.2023.103579
14. Babu, E. S., SrinivasaRao, B. K. N., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks. *Computers and Electrical Engineering, 103,* 108287. https://doi.org/10.1016/j.compeleceng.2022.108287
15. Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Networks, 152,* 103320. https://doi.org/10.1016/j.adhoc.2023.103320
16. Kumar, A., Sharma, B., & Noonia, A. (2025). Secure blockchain-based intrusion detection for IoT networks. *Discover Computing, 28,* 226. https://doi.org/10.1007/s10791-025-09754-4
17. Alruwaili, F. F. (2025). Leveraging blockchain for cybersecurity detection using hybridization of prairie dog optimization with differential evolution on Internet of Things environment. *Scientific Reports, 15,* 31673. https://doi.org/10.1038/s41598-025-10410-6
18. Singh, R., Kukreja, D., & Sharma, D. (2023, January). Blockchain-enabled access control to prevent cyber-attacks in IoT: Systematic literature review. *Frontiers in Big Data, 5,* 1081770. https://doi.org/10.3389/fdata.2022.1081770
19. Huan, N. T. Y., & Zukarnain, Z. A. (2024). A survey on addressing IoT security issues by embedding blockchain technology solutions: Review, attacks, current trends, and applications. *IEEE Access, 12,* 69765–69782. https://doi.org/10.1109/ACCESS.2024.3378592

20. Shedthi, A., Arunachalam, G., Sundar, M., & Tiwari, M. (2024, March). Applications of blockchain technology in securing distributed systems. *International Journal of Intelligent Systems and Applications in Engineering*, *12*, 152–158. https://ijisae.org/index.php/IJISAE/article/view/4960
21. Akinbi, A., MacDermott, Á., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation*, *42–43*, 301470. https://doi.org/10.1016/j.fsidi.2022.301470
22. Khonde, S. R., & Ulagamuthalvi, V. (2022). Hybrid intrusion detection system using blockchain framework. *Journal of Wireless Communications and Networking*, *2022*, 58. https://doi.org/10.1186/s13638-022-02089-4
23. Rathee, G., Kerrache, C. A., & Ferrag, M. A. (2022). A blockchain-based intrusion detection system using Viterbi algorithm and indirect trust for IIoT systems. *Journal of Sensor and Actuator Networks*, *11*(4), 71. https://doi.org/10.3390/jsan11040071
24. Heidari, A., Jafari Navimipour, N., & Unal, M. (2023). A secure intrusion detection platform using blockchain and radial basis function neural networks for Internet of Drones. *IEEE Internet of Things Journal*, *10*(10), 8445–8454. https://doi.org/10.1109/JIOT.2023.3237661
25. Mansour, R. F. (2022). Artificial intelligence-based optimization with deep learning model for blockchain-enabled intrusion detection in CPS environment. *Scientific Reports*, *12*, 12937. https://doi.org/10.1038/s41598-022-17043-z