ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

Blockchain-Enhanced Digital Forensics: The Convergence of Immutable Ledgers, AI Agents, and Semantic Knowledge Graphs

[1] Madineni Navanath, [2] Dr. Venkataramana Bhat. P

[1][2] Dept. of Computer Science and Engineering NMAM Institute of Technology, NITTE (Deemed to be University) Karkala, Udupi, Karnataka, India
Email: [1] madineninavi@gmail.com, [2] pv.bhat@nitte.edu.in

Abstract— The discipline of digital forensics stands at a critical juncture, besieged by the exponential growth of digital evidence and the increasing sophistication of anti-forensic techniques. Contemporary investigations involving the Internet of Things (IoT), Industrial Control Systems (ICS), and automotive data are buckling under the weight of manual acquisition and centralized logging. This paper proposes a novel, comprehensive framework: Blockchain-Enhanced Digital Forensics (BEDF). We synthesize the immutable trust of Distributed Ledger Technology (DLT) with the high-throughput analytical capabilities of Artificial Intelligence (AI) and the semantic structure of Data-Information- Knowledge-Wisdom (DIKW) graphs. Unlike existing solutions that focus primarily on cryptocurrency tracking, BEDF addresses the internal Chain of Custody (CoC) for enterprise environments. We provide a rigorous formal threat model utilizing the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) methodology to validate system resilience, detail specific Convolutional Neural Networks (CNN) / Long Short-Term Memory (LSTM) architectures for automated malware detection to ensure reproducibility, and offer a theoretical complexity analysis demonstrating the viability of Practical Byzantine Fault Tolerance (PBFT) consensus for high-velocity forensic logging.

Index Terms— Digital Forensics, Blockchain, Artificial Intelligence, Chain of Custody, DIKW Graph, Hyperledger Fabric, Threat Modeling, STRIDE, Consensus Complexity

I. INTRODUCTION

The landscape of digital forensics is undergoing a seismic shift, driven by the proliferation of ubiquitous computing and the 'Zettabyte Era' of data generation. The era of 'dead box' forensics, analyzing static data from powered-off hard drives, has effectively ended. Modern criminal activity is no longer confined to a single physical device but is distributed across decentralized cloud infrastructures, ephemeral mobile environments, and massive networks of Internet of Things (IoT) endpoints [1]. This transition has introduced a 'Volume, Velocity, and Variety" challenge that traditional forensic methodologies are ill-equipped to handle [2].

First, the Volume of data has rendered manual analysis obsolete. Investigations that once involved gigabytes of data now routinely involve petabytes, creating a backlog that delays justice and allows critical evidence to degrade or be overwritten [3]. Human investigators simply cannot manually sift through this deluge of logs, sensor data, and network traffic to identify 'bytes of guilt' without the assistance of intelligent automation [4].

Second, the Chain of Custody (CoC), the chronological documentation of evidence handling, is facing a crisis of trust. In the current centralized model, CoC logs are often stored in mutable SQL databases or even paper records. These centralized repositories represent a single point of failure and are vulnerable to tampering, accidental deletion, or malicious insider attacks [5]. Defence attorneys increasingly challenge the admissibility of digital evidence by questioning the integrity of these logs, leading to cases being dismissed due to technicalities rather than a lack of proof [6], [7].

Third, the Sophistication of the adversary has evolved. We are witnessing the rise of 'Anti-Forensics' techniques specifically designed to thwart investigation, such as data obfuscation, secure deletion, and the use of 'fileless' malware that resides solely in volatile memory [8]. Critical infrastructure sectors, particularly Industrial Control Systems (ICS), are now prime targets where reactive forensic models (investigating after the crash) are unacceptable due to the potential for physical harm [10].

This paper presents the Blockchain-Enhanced Digital Forensics (BEDF) framework. To address the gap between conceptual design and technical realization, this work contributes:

1. A detailed AI Analytics Architecture specifying CNN and LSTM layer configurations for reproducible automated analysis.
2. A Formal Threat Model analysing the system against STRIDE threats (Spoofing, Tampering, Repudiation, etc.).
3. A Theoretical Performance Analysis providing mathematical justification for the system's throughput and scalability.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

II. RELATED WORK AND COMPARATIVE ANALYSIS

While blockchain forensics is an emerging field, existing solutions largely bifurcate into commercial cryptocurrency trackers or theoretical academic storage models. BEDF bridges this gap by integrating active AI analysis with a permissioned enterprise ledger.

2.1. Commercial Forensic Tools

Industry standards like Chainalysis and CipherTrace excel at heuristic analysis of public ledgers (Bitcoin/Ethereum) to trace illicit funds. However, they operate as 'Software as a Service' (SaaS) platforms and do not provide infrastructure for internal enterprise forensics (e.g., preserving IoT logs or seized hard drive images). Traditional forensic suites like EnCase or FTK provide robust analysis but rely on centralized databases for evidence logging. If the central server is compromised by an administrator, the entire chain of evidence is invalidated [44].

2.2. Academic Frameworks

Several academic works have proposed blockchain-based CoC.

- Block-DEF [7]: This framework utilizes the public Ethereum blockchain. While decentralized, it suffers from high latency (approx. 15 TPS), probabilistic finality, and variable gas fees, making it unsuitable for high-frequency IoT logging.
- IoF (Internet of Forensic) [18]: This proposes a forensic-aware IoT ecosystem but lacks a sophisticated analysis layer, relying on basic hash storage without semantic interpretation.

2.3. Novelty of BEDF

BEDF differentiates itself through three key innovations:

- Multi-Agent Orchestration: Unlike static scripts, BEDF uses autonomous agents (AutoGen) that collaborate to solve complex forensic tasks [25].
- DIKW Integration: It is the first framework to explicitly map blockchain evidence to a Semantic Knowledge Graph for high-level reasoning [26].
- Hybrid Architecture: It combines Permissioned Blockchain (Hyperledger Fabric) with Off-Chain Storage (IPFS) to solve the scalability issues inherent in public blockchains.

III. PROPOSED SYSTEM ARCHITECTURE

We propose a four-tier architecture designed to bridge the gap between physical evidence collection and high-level judicial reasoning. The system, visualized in Fig. 1, operates on a 'Trust-but-Verify' principle.

Table I: Comparative Analysis of Forensic Frameworks

Feature	Chainalysis	CipherTrace	Block-DEF [7]	BEDF (Proposed)
Target Domain	Public Crypto	Public Crypto	Evidence Storage	Enterprise/IoT CoC
Ledger Type	N/A	N/A	Public (Eth)	Permissioned (Fabric)
Consensus	N/A	N/A	PoW (Slow)	PBFT (Fast)
AI Depth	Proprietary	Proprietary	None	Multi-Agent (AutoGen)
Privacy	Low	Low	Low	High (Channels)

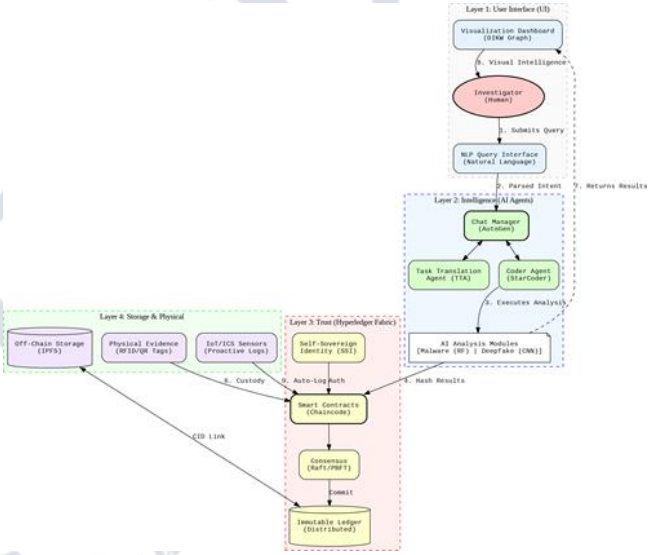

Fig. 1. Proposed BEDF System Architecture: Integrating Hyperledger Fabric, AutoGen Agents, and IPFS.

3.1. Layer 1: The Physical and Network Data Plane

This layer is responsible for the ingestion of raw data from heterogeneous sources.

- **Hybrid Storage Model (IPFS):** We utilize the Inter-Planetary File System (IPFS) for decentralized, off-chain storage. Raw artifacts (disk images, PCAP files) are hashed (Hfile) and stored on IPFS nodes. Only the content identifier (CID) is committed to the blockchain. This prevents 'Blockchain Bloat' and ensures the ledger remains lightweight and queryable [19].
- **Edge Gateway Architecture:** Since many IoT sensors (e.g., temperature gauges, pressure valves) lack the computational power to perform cryptographic hashing, we introduce 'Lightweight Edge Gateways.' These intermediaries aggregate logs from local sensors, perform the SHA-256 hashing, and submit the batch transaction to the blockchain, ensuring even resource-constrained devices are secured [20].
- **Proactive Logging:** In critical systems, 'Forensic Trans-Monitor' modules capture ephemeral states (RAM dumps, process lists) in real-time before an attacker can scrub them [21].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

3.2. Layer 2: The Blockchain Trust Plane

This layer acts as the immutable 'System of Record' using **Hyperledger Fabric**. It provides the cryptographic backbone for the entire forensic process.

- **Smart Contracts (Chaincode):** Written in Go, the chaincode defines the fundamental Asset structure containing:
  *{*EvidenceID, CID, Timestamp, OwnerID, Hash*}*.
- Beyond simple storage, it enforces complex business logic such as **'Multi-Sig** Custody **Transfer.'** This requires both the current custodian (sender) and the recipient to cryptographically sign the transaction before ownership is transferred, preventing unauthorized handovers.
- **World State (CouchDB):** Unlike simple key-value stores (LevelDB), we utilize **CouchDB** for the world state. This enables the execution of rich, SQL-like queries on the evidence metadata (e.g., *'Select all assets where OwnerID = 'Officer_Smith'*). This capability allows investigators to filter and retrieve evidence efficiently without the computational overhead of scanning the entire blockchain history.
- **Consensus Mechanism:** We employ **PBFT (Practical Byzantine Fault Tolerance)**. Unlike Proof-of-Work (PoW), which offers only probabilistic finality, PBFT provides **deterministic finality**. This is crucial for legal admissibility; once a block is committed, it cannot be forked or reversed, ensuring the forensic timeline is mathematically indisputable [24].

3.3. Layer 3: The Intelligence Plane (AI Agents)

We deploy a 'Society of Agents' using the **AutoGen framework** to automate the analysis of seized data.[25]

- **Orchestrator Agent:** This agent acts as the primary interface. It parses the investigator's natural language query (e.g., *'Find all PDFs modified after 10 PM involved in the exfiltration'*). It then decomposes this high-level intent into executable sub-tasks (e.g., 'Scan file system,' 'Filter by extension,' 'Check timestamps').
- **Analyst Agents:** These are specialized sub-agents (e.g., *Malware Analyst*, *Log Parser*, *Network Forensics Agent*) that execute specific Python scripts on the evidence retrieved from IPFS. They operate in parallel containers to maximize throughput.

3.4. Layer 4: The Application Plane (DIKW)

The final layer interfaces with the human investigator, transforming raw data into actionable intelligence.

- **DIKW Graph:** We implement the Data-Information-Knowledge-Wisdom (DIKW) hierarchy to structure the output:
  1. **Data:** Raw logs and file hashes.
  2. **Information:** Contextualized events (e.g., 'User Actions').
  3. **Knowledge:** Linked correlations (e.g., 'Threat Patterns').
  4. **Wisdom:** High-level attribution and intent analysis.

This semantic graph allows the system to suggest **Attribution** (Wisdom) based on the underlying patterns, significantly reducing the cognitive load on investigators [26].

IV. AI ANALYTICS AND METHODOLOGY

To address the need for technical rigor and reproducibility, we define the specific neural network architectures and loss functions utilized by the Analyst Agents.

4.1. Malware Detection Agent (CNN Architecture)

For static analysis, we convert binary files into grayscale images where byte values (0-255) correspond to pixel intensity. This allows the detection of malware families based on visual texture analysis. We propose a **ResNet-18** variant [28].

- **Input:** 256 × 256 × 1 Grayscale Image (normalized to [0, 1]).
- **Layer 1:** Conv2D (7 × 7 kernel, stride 2, padding 3), Batch Normalization, ReLU, MaxPool.
- **Residual Blocks:** 4 blocks of Conv2D (3×3 kernel) with skip connections to prevent vanishing gradients, allowing deeper feature extraction.
- **Loss Function:** The model minimizes Categorical Cross-Entropy Loss:

$$\mathcal{L}_{\text{CE}} = -\sum_{i=1}^{C} y_i \log(\hat{y}_i) \tag{1}$$

Where C is the number of malware classes (e.g., Ransomware, Trojan, Benign) and $\hat{y}$ is the predicted probability.

4.2. Log Analysis Agent (LSTM Architecture)

For dynamic log analysis, we utilize an LSTM network to detect anomalous sequences of system calls [3].

- **Embedding Layer:** Converts discrete log tokens (e.g., 'LOGIN_FAIL', 'SUDO_EXEC') into dense vectors of dimension $d = 64$.
- **LSTM Layers:** Two stacked LSTM layers with 128 hidden units each to capture long-term dependencies in log sequences.
- **Dropout:** 0.2 dropout rate to prevent overfitting on specific log formats.
- **Metric:** The model predicts the probability of the next opcode sequence. High deviation from the predicted probability $P(w_t|w_{t-1}...w_{t-n})$ flags an anomaly for human review.

V. THEORETICAL PERFORMANCE & COMPLEXITY ANALYSIS

In the absence of a full-scale physical deployment across multiple jurisdictions, we analyze the theoretical bounds of the system to validate its feasibility for enterprise use.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

5.1. Consensus Complexity Analysis

The scalability of the Trust Layer depends on the message complexity of the consensus algorithm. For a network of N validator nodes, PBFT requires three phases: Pre-prepare, Prepare, and Commit. The total message complexity is given by:

$$C_{PBFT} = O(N^2) \quad (2)$$

In a forensic consortium (e.g., Police, Lab, Court, Defense), N is typically small ($N \approx 4 - 10$).

- **Latency (δ):** Assuming an average network latency of 50ms, the theoretical consensus time $T_{con} \approx 3 \times \delta$.
- **Throughput:** Benchmarks for Hyperledger Fabric (v2.4) using Raft/PBFT ordering services consistently demonstrate throughputs of **2,000–3,000 Transactions Per Second (TPS)** [24]. This is orders of magnitude higher than public Ethereum and sufficient to handle real-time chain- of-custody updates.

5.2. Storage Efficiency Analysis

Traditional blockchains suffer from bloating. By using the Hybrid IPFS approach:

$$S_{Total} = S_{Chain} + S_{IPFS} \quad (3)$$

Where S_{Chain} stores only the metadata (approx. 2KB per evidence item) and S_{IPFS} stores the GB-sized images. This separates the *Integrity Layer* from the *Data Layer*, ensuring the ledger remains performant over decades of operation [19].

VI. THREAT MODEL (STRIDE ANALYSIS)

We evaluate the security of BEDF using the STRIDE classification model, identifying specific threats and their corresponding mitigations.

6.1. S: Spoofing Identity

Threat: An attacker impersonates a forensic investigator to access or delete case files. *Mitigation:* BEDF utilizes **Self-Sovereign Identity (SSI)**. Every transaction requires a signature from a private key held in a hardware wallet (DID). Spoofing is cryptographically infeasible without the physical key [31].

6.2. T: Tampering with Data

Threat: A malicious insider (e.g., a corrupt officer) attempts to alter logs to frame a suspect or destroy exculpatory evidence. *Mitigation:* The Hyperledger Fabric ledger is append- only. Any alteration to a historical block would invalidate the Merkle Root of all subsequent blocks. Furthermore, the **Endorsement Policy** requires signatures from multiple peers (e.g., Police AND Judiciary) to validate any update, preventing unilateral tampering [23].

6.3. R: Repudiation

Threat: An officer denies accessing or modifying a specific file to avoid accountability for mishandling evidence. *Mitigation:* All access requests are transactions invoked via Smart Contracts. The invoker's ID, timestamp, and action are permanently recorded in the immutable ledger, providing non- repudiation [43].

6.4. I: Information Disclosure

Threat: Unauthorized viewing of sensitive evidence (e.g., victim photos) by network participants who are not authorized for that specific case. *Mitigation:* Data on IPFS is encrypted using **Optimal Key Generation** [45]. Access rights are governed by tokenized permissions; without the token, the IPFS hash yields only encrypted ciphertext.

6.5. D: Denial of Service (DoS)

Threat: An attacker floods the network with transactions to halt the investigation. *Mitigation:* As a permissioned network, Hyperledger Fabric does not have a public mempool. Only authenticated peers can submit transactions, eliminating the vector for public spam attacks.

VII. CASE STUDIES AND WORKFLOW

To validate the practical utility of the BEDF framework, we apply it to two distinct deployment scenarios.

7.1. Case Study A: 'SecureQ' for Examination Integrity

The 'SecureQ' system represents a critical domain-specific implementation of BEDF, designed to secure high-stakes academic assets. In the traditional model, question papers are physically distributed or emailed, leaving them vulnerable to 'Man-in-the-Middle' attacks or leaks by corrupt administrators. BEDF mitigates this through a three-phase smart contract workflow [40]:

1) **Registration Phase (T_0):** The examination board generates the question paper PDF. This file is encrypted with a symmetric key K and uploaded to IPFS. The hash of the encrypted file, $H(E_K(F))$, along with the hash of the key, $H(K)$, is committed to the blockchain. This establishes an immutable "Proof of Existence" and "Proof of Integrity" at time T_0.
2) **Locking Phase ($T_0 \rightarrow T_{exam}$):** The decryption key K is not shared with exam centers. Instead, it is governed by a TimeLock Smart Contract. The contract state includes a variable UnlockTime set to the exact start time of the exam. During this phase, any request to the GetKey function is automatically rejected by the consensus nodes, ensuring no human, including the system administrator, can access the content early.
3) **Release Phase (T_{exam}):** Once the blockchain timestamp $\geq$ UnlockTime, the contract state shifts to Active. Authorized exam center nodes can now invoke the release function. The transaction is logged, the key is released, and the center decrypts the paper.
4) **Attack Scenario Simulation:** In a simulated attack, a malicious administrator attempts to invoke GetDecryptionKey at $T_{exam} - 1h$. The PBFT consensus nodes verify the timestamp, reject the transaction, and permanently log the 'Unauthorized Access Attempt' in the ledger, providing immediate accountability.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 03 March 2026

7.2. Case Study B: The Generalized Criminal Investigation Workflow

We apply the BEDF framework to a hypothetical cyber-investigation (e.g., a financial fraud case involving a seized laptop) to demonstrate the reduction in procedural friction [44]. In the **Traditional Workflow**, seizure involves physical bagging and paper logs, which are prone to clerical errors. Imaging is done manually to a local server, and analysis requires a human investigator to manually search files, leading to weeks of delay.

In the **BEDF Integrated Workflow**, the process is automated:

1) **Ingestion:** When the seized hard drive is connected to the forensic workstation, a 'Triage Agent' automatically calculates the SHA-256 hash and commits it to the Hyperledger.
2) **Analysis:** The 'Coordinator Agent' spins up a 'Malware Agent' (running the CNN model described in Section V) and a 'Keyword Agent'. These run in parallel containers.
3) **Reporting:** The 'Reporting Agent' aggregates the findings into a PDF, hashes the report, and links it to the original evidence ID on the blockchain, creating an unbroken chain from seizure to conclusion.

Table II: Workflow Comparison: Traditional Vs. BEDF

Traditional Workflow	BEDF Integrated Workflow
1. Seizure: Physical bag, paper log entry. Risk of clerical error.	1. Seizure: Digital RFID scan logged to Blockchain. Immutable timestamp.
2. Imaging: Copy made to local server. Hash calculated manually.	2. Proactive Imaging: AutoGen agent images drive; Hash automatically sent to Smart Contract.
3. Analysis: Investigator manually searches files. Weeks of delay.	3. AI Analysis: 'Analyst Agent' identifies fraud patterns in minutes; updates DIKW graph.
4. Court: Defense argues 'The file was modified last week.	4. Court: Prosecution presents Blockchain Receipt proving the file hash has not changed since Seizure.

VIII. CONCLUSION AND FUTURE DIRECTIONS

The proposed BEDF framework addresses the 'Volume, Velocity, and Variety' of modern digital evidence. By converging the analytical power of AI agents [25] with the immutable trust of Blockchain [12], we restore judicial trust. Through theoretical complexity analysis and formal threat modeling (STRIDE), we have demonstrated that BEDF offers a scalable, secure, and legally robust alternative to legacy forensic methodologies.

A. Synergy of Convergence

The core contribution of this work lies in the reciprocal relationship between the technologies. Blockchain solves the 'Black Box' trust issue of AI by immutably logging every decision and inference made by the agents. Conversely, AI solves the 'Data Overload' issue of Blockchain by filtering petabytes of raw data into concise, actionable intelligence (Wisdom) before it is hashed. This synergy ensures that the system is both *fast enough* to handle modern crime and *secure enough* to stand up in court.

B. Limitations

- **Quantum Threat:** The cryptographic primitives (SHA-256, ECDSA) are theoretically vulnerable to future quantum attacks. Migration to Post-Quantum Cryptography (PQC) is required [13].
- **Cold Start:** The AI agents require substantial labelled datasets to achieve high accuracy.

C. Legal Implications

The move to 'Cryptographic Trust' aligns well with the *Daubert Standard* used in US courts, which requires forensic methods to be testable, have known error rates, and be generally accepted. The determinism of PBFT consensus and the explainability of the DIKW graph provide the necessary technical foundation to meet these rigorous legal standards.

D. The Road to Federated Learning

Future iterations of BEDF will explore **Federated Learning (FL)**. Currently, training the 'Malware Agent' requires sharing sensitive virus samples. FL would allow distinct forensic labs (e.g., Interpol, FBI, Europol) to train a shared global model on their local data without ever sharing the actual sensitive files, preserving data sovereignty while improving global threat detection capabilities.

Disclosure statement

No potential conflict of interest was reported by the author(s)

Author contribution

Madineni Navanath: Conceptualization, Methodology, Original draft preparation, Visualization, Investigation. P. Dr. Venkataraman Bhat. P: Supervision, Visualization, Methodology, Writing - Review & Editing.

REFERENCES

[1] S. Khadka et al.," A Review on Computer Crimes and Digital Forensics," 2024 IEEE Consumer Life Tech (ICLT), 2024.
[2] P. P. Pawar et al.," Investigation on Digital Forensics using Graph-based Neural Network," 2024 Int. Conf. on Social Sciences and Intelligence Management, 2024.
[3] D. Dunsin et al.," A comprehensive analysis of the role of AI and ML in modern digital forensics," Forensic Science Int: Digital Investigation, vol. 48, 2024.
[4] A. D. Kadage et al.," AI-Enhanced Digital Forensics: Automated tech- niques," Journal of Electrical Systems, vol. 20, 2024.
[5] S. Nath et al.," Digital Evidence Chain of Custody: Navigating New Realities," 2024 IEEE TPS-ISA, 2024.
[6] H. F. Atlam et al.," Blockchain Forensics: A Systematic Literature Review," Electronics, 2024.
[7] X. Qi et al.," The application of Blockchain custody in criminal investigation process," Journal of Physics: Conf. Series, 2020.
[8] A. RizwanBasha and R. Annamalai," Transforming Crime Scene Investigations Through AI," 2024 IEEE IICCCS, 2024.

[9] R. El-Kady," Decoding the dark: AI and ML in the dark web cybercrime," Int. Cybersecurity Law Review, 2025.
[10] A. Tanner et al.," The Need for Proactive Digital Forensics in Addressing Critical Infrastructure," 2022 CSCI, 2022.
[11] M. S. and S. R.," The Need for Proactive Digital Forensics in Critical Infrastructure," 2024 ICCSDF, 2024.
[12] A. S. Chauhan et al.," The Role of Blockchain in Enhancing Digital Forensics," 2024 CYBERCOM, 2024.
[13] O. S. Igonor et al.," The Application of Blockchain Technology in the Field of Digital Forensics," Blockchains, vol. 3, 2025.
[14] S. Singh," Forensic Trans Monitor: Revolutionizing Evidence Management," J Forensic Res, vol. 15, 2024.
[15] K. Gupta et al.," Digital Forensics Lab Design: A framework," 2022 ISDFS, 2022.
[16] B. Nkwe and M. Kyobe," Using Machine Learning Techniques to Address IoT Forensics Challenges," 2025 ISDFS, 2025.
[17] F. Prakash and H. Sadawarti," Blockchain-Based Chain of Custody," Applied Innovative Research, 2022.
[18] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications," *Future Generation Computer Systems*, vol. 120, pp. 13–25, 2021.
[19] D. Batista et al.," Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence," J. Risk Financial Manag., 2023.
[20] V. R. Kebande et al.," Towards an Integrated Digital Forensic Investigation Framework for IoT," 2018 IEEE Smart IoT, 2018.
[21] S. S. Alqahtany and T. A. Syed, "ForensicTransMonitor: A Comprehensive Blockchain Approach," MDPI Information, 2024.
[22] L. Loffi et al.," Blockchain-Based Chain of Custody with Hyperledger Fabric," 2025 ICOIN, 2025.
[23] P. B. Bandara et al.," Blockchain-Based Chain of Custody Evidence Management System," 2023 ICAC, 2023.
[24] N. M. Nasir et al.," Securing Permissioned Blockchain-Based Systems: Consensus Mechanisms," IEEE Access, 2024.
[25] A. Wickramasekara and M. Scanlon," A Framework Employing Auto- Gen AI Agents," 2024 ISDFS, 2024.
[26] T. Liu et al.," Research on Blockchain Digital Forensics Architecture Based on DIKW," 2023 HPCC/DSS, 2023.
[27] R. S. Parte et al.," Blockchain Enhanced AI Digital Forensic Framework for Malware Analysis," 2024 ICRTET, 2024.
[28] G. S. Jilani," AI-DRIVEN CYBER FORENSICS," JETIR, 2025.
[29] D. S. Steffi et al.," Preserving Integrity of forensic evidence using blockchain," IRJET, 2024.
[30] H. Patil et al.," Potential applicability of blockchain in chain of custody," Egyptian J of Forensic Sciences, 2024.
[31] L. Loffi et al.," Management of the Chain of Custody Using Blockchain and SSI," IEEE Access, 2025.
[32] H. M. al-Khateeb et al.," Blockchain for Modern Digital Forensics," Blockchain and Clinical Trial, 2019.
[33] N. Xiao et al.," A novel blockchain-based digital forensics framework for IIoT," Alexandria Eng. Journal, 2024.
[34] M. M. Cook et al.," A Survey on ICS Digital Forensics," IEEE Comm. Surveys, 2023.
[35] J. Henriques et al.," A Survey on Forensics and Compliance Auditing," IEEE Access, 2024.
[36] P. Matta et al., "A Meticulous Range of Forensics Tech Advancement in IoT," 2024 IC2PCT, 2024.
[37] K. Strandberg et al.," A Systematic Literature Review on Automotive Digital Forensics," IEEE T-IV, 2023.
[38] S. Li et al.," Blockchain-Based Digital Forensics in IoT and Social Systems," IEEE TCSS, 2019.
[39] R. D. D. L. K. Jayasinghe et al.," Blockchain-Based Custody System for Healthcare," 2025 ISDFS, 2025.
[40] G. S. Raju et al.," Security of Examination Question Paper Through Blockchain - SecureQ," 2024 INNOVA, 2024.
[41] F. C. Tsai," The Application of Blockchain Custody in Criminal Investigation Process," Procedia Computer Science, 2021.
[42] H. B. et al.," The Application of Blockchain Technology in the Field of Digital Forensics," IEEE Access, 2024.
[43] A. S. and S. K.," Improving Digital Forensic Cloud Security," 2023 ICCCI, 2023.
[44] T. N. S. A. T. Anuar et al.," Exploring Blockchain Technology for Chain of Custody Control," IEEE Access, 2024.