British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

AI-Augmented Log Forensics for PowerShell-Based Malware Detection

Daniel Aigboduwa
Master in Cybersecurity, University of Houston Texas USA

doi: https://doi.org/10.37745/bjesr.2013/vol13n3136164 Published November 09, 2025

Citation: Aigboduwa D. (2025) AI-Augmented Log Forensics for PowerShell-Based Malware Detection, *British Journal of Earth Sciences Research*, 13(3),136-164

Abstract: *Digital evidence forms the backbone of modern cybercrime investigations, particularly in web-server forensics, where logs, SSH traces, and system snapshots serve as critical artefacts for incident reconstruction. However, such evidence is inherently fragile—susceptible to tampering, manipulation, or accidental alteration during collection, storage, and transfer. Ensuring the authenticity and continuity of this evidence is central to preserving its legal and investigative credibility.Conventional forensic models depend on centralized, trust-based architectures for managing evidence. These models are prone to insider threats, administrative errors, and single points of failure, leading to breaks in the chain-of-custody and undermining evidentiary integrity. Moreover, existing digital forensics tools lack mechanisms for verifiable, immutable recordkeeping of evidence handling events, leaving investigators reliant on procedural documentation rather than cryptographic assurance. This study introduces a* ***Blockchain-Enabled Evidence Integrity Framework (BEEIF)****—a decentralized system that employs blockchain technology to establish tamper-proof, cryptographically verifiable chains-of-custody for web-server forensic artefacts. The framework leverages blockchain's immutability, distributed consensus, and smart contract automation to transform the management of digital evidence into a transparent, mathematically provable process.The proposed framework comprises five key components: (1) Evidence Acquisition Agents that securely collect logs and system snapshots, (2) a Hashing and Timestamping Module that generates SHA-3-512 hashes and trusted timestamps, (3) a permissioned blockchain layer that records cryptographic proofs and metadata, (4) smart contracts governing evidence registration, access control, and verification, and (5) a Verification Interface for investigator interaction. A proof-of-concept was implemented on a simulated testbed featuring a compromised web server and a private blockchain network (Hyperledger Fabric), with realistic performance metrics analyzed to assess feasibility.The results demonstrated that blockchain integration achieved tamper-proof traceability with negligible system overhead—approximately* ***2.3% CPU utilization*** *and sub-second transaction latency. Blockchain growth remained minimal due to the separation of on-chain metadata and off-chain evidence storage. These findings validate the framework's ability to maintain evidence integrity and transparency in real time without compromising operational efficiency.The BEEIF framework redefines digital forensics by shifting evidentiary trust from procedural dependence to* ***cryptographic verifiability****. By securing the entire forensic evidence lifecycle through blockchain immutability, this approach offers a transformative pathway for credible, cross-institutional cybercrime investigations and legally defensible digital evidence management in the emerging era of decentralized cybersecurity assurance.*

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

KEYWORDS: blockchain forensics, digital evidence integrity, web-server forensics, chain-of-custody, cybercrime investigation, evidence immutability, permissioned blockchain, smart contracts, forensic provenance, cryptographic verification, decentralized trust, hyperledger fabric, digital forensics framework.

INTRODUCTION

In the rapidly evolving landscape of digital transformation, web servers constitute the critical backbone of global information exchange, powering business operations, financial transactions, healthcare systems, government portals, and communication infrastructures. As such, they represent both high-value assets and attractive targets for cyber adversaries. With the exponential growth of web-based attacks—ranging from SQL injections, cross-site scripting (XSS), and remote code execution, to advanced persistent threats (APTs)—the need for precise, reliable, and legally admissible web-server forensic investigations has never been more acute. Web-server forensics serves as a cornerstone of incident response, post-compromise analysis, and cybercrime attribution, aiming to reconstruct events, trace intrusions, and extract evidence that can withstand judicial scrutiny. However, the efficacy of this investigative process is contingent upon one foundational principle: the integrity and authenticity of digital evidence.

In the domain of web-server forensics, evidence typically comprises server traffic logs, Secure Shell (SSH) session traces, configuration files, memory dumps, and forensic snapshots of server states. Each of these artefacts forms part of a delicate evidentiary chain-of-custody—documenting how, when, and by whom the evidence was collected, handled, and analyzed. Yet, in conventional forensic environments, the management of such evidence remains predominantly centralized, often reliant on trust-based storage mechanisms, institutional authority, or individual custodians. This centralization introduces a fundamental vulnerability: the potential for evidence tampering, unauthorized modification, or accidental loss—either maliciously, through insider threats, or inadvertently, through procedural errors. The mutable nature of digital data amplifies this risk, as even a single unauthorized byte alteration can invalidate the evidential value of an entire dataset in court proceedings.

Furthermore, the traditional forensic process is plagued by several systemic challenges. First, the reliance on centralized evidence repositories creates single points of failure—if the central database is compromised, corrupted, or inaccessible, the entire chain-of-custody collapses. Second, the traceability of actions performed on evidence remains opaque; investigators and third parties must often rely on log entries that can themselves be altered. Third, jurisdictional and multi-party investigations exacerbate trust issues, particularly when evidence is shared among organizations, law enforcement agencies, and cloud service providers operating under disparate governance and policy frameworks. In such cases, ensuring the non-repudiation of evidence-handling actions becomes exceedingly difficult. Consequently, the credibility of forensic findings—and, by extension, the pursuit of cyber justice—can be undermined by procedural weaknesses rather than analytical inadequacies.

To address these enduring deficiencies, the field of digital forensics is increasingly turning to blockchain technology as a transformative enabler of evidence integrity. Far from being a mere technological trend or cryptocurrency backbone, blockchain embodies a paradigm shift in how digital trust is engineered. At its core, blockchain is a decentralized, distributed ledger maintained across a network of nodes, where each transaction or data entry is cryptographically linked to the previous one, forming an immutable chronological chain. This architecture inherently resists unauthorized modification: any attempt to alter a record would require consensus from the majority of nodes and computational recomputation of subsequent blocks, rendering tampering computationally impractical. The properties of decentralization, immutability, and transparency collectively make blockchain an ideal candidate for addressing the evidentiary integrity crisis in forensic science.

Applied within the context of web-server forensics, blockchain offers several concrete advantages. Firstly, it can facilitate a decentralized chain-of-custody system, eliminating the reliance on a single trusted authority by distributing control among authenticated forensic entities. Each piece of digital evidence—be it a traffic log, SSH trace, or memory snapshot—can be hashed and its corresponding cryptographic digest recorded on the blockchain, creating an immutable provenance record. Secondly, timestamping and digital signatures embedded within blockchain transactions provide non-repudiable proof of evidence collection and handling events, enabling investigators, auditors, and courts to verify not only the authenticity of the evidence but also the accountability of each participant involved in its lifecycle. Thirdly, smart contracts—self-executing programs encoded within blockchain networks—can automate evidence management workflows, such as access authorization, chain-of-custody validation, and forensic process auditing, thereby minimizing human error and ensuring procedural consistency.

Recent advancements in blockchain interoperability and privacy-preserving mechanisms further enhance its applicability to digital forensics. For instance, permissioned blockchain models, such as Hyperledger Fabric and Quorum, allow controlled access to participants while preserving the cryptographic immutability of records. Zero-knowledge proofs and secure multi-party computation techniques can be integrated to ensure that sensitive forensic details remain confidential, while still verifying integrity on the blockchain. In this manner, blockchain becomes not merely a record-keeping mechanism but a foundational infrastructure for trusted digital investigation ecosystems.

Nevertheless, despite its promise, the application of blockchain in forensic science remains largely conceptual, with existing research focusing primarily on cryptocurrency investigations or general evidence management frameworks. Specific challenges related to web-server forensics—such as high-volume log data, dynamic server states, and the need for rapid evidence acquisition—demand tailored approaches that balance forensic precision with system scalability. The design of such a blockchain-enabled forensic framework must consider factors like data size optimization (through off-chain storage and on-chain referencing), latency minimization, interoperability with existing forensic tools, and compliance with legal admissibility standards. Addressing these complexities is essential to bridge the gap between theoretical potential and operational feasibility.

Against this backdrop, the present study aims to conceptualize and evaluate a **blockchain-enabled framework for maintaining evidence integrity in web-server forensics**. The proposed framework integrates blockchain technology to establish a decentralized, tamper-proof provenance system for forensic artefacts collected during the investigation of compromised web servers. Specifically, it focuses on ensuring the **authenticity, immutability, and verifiable chain-of-custody** of key evidentiary components—namely, traffic logs, SSH traces, and forensic snapshots. By leveraging cryptographic hashing, decentralized consensus, and smart contract–driven access control, the framework seeks to provide a trustworthy environment in which every interaction with digital evidence is transparently recorded and verifiable in real time.

The objective of this research is twofold. First, it seeks to design a conceptual architecture demonstrating how blockchain can be systematically integrated into existing web-server forensic processes without disrupting standard forensic workflows. Second, it aims to assess, through theoretical validation and model-based evaluation, the degree to which blockchain's intrinsic properties can mitigate traditional risks of evidence tampering, unauthorized access, and chain-of-custody discontinuity. Ultimately, this study aspires to contribute a rigorously developed model that not only strengthens the credibility of forensic findings but also lays the groundwork for a new era of **decentralized trust** in digital investigations—where integrity is no longer asserted by authority but mathematically guaranteed by design.

LITERATURE REVIEW

The growing sophistication of cyber threats and the increasing dependency on web-based infrastructures have necessitated continual evolution in digital forensic methodologies. Yet, despite technological advances, maintaining the integrity of digital evidence—especially within the context of compromised web servers—remains a persistent and formidable challenge. This literature review is structured into three thematic components: (1) a review of traditional web-server forensic techniques and their chain-of-custody vulnerabilities, (2) an analysis of blockchain applications in ensuring data integrity across various industries, and (3) a synthesis of the emerging intersection between blockchain and digital forensics, identifying the unresolved research gaps that motivate this study's proposed framework.

1. Traditional Web-Server Forensics and Chain-of-Custody Challenges

Web-server forensics encompasses the systematic acquisition, preservation, and analysis of server-side data following security incidents. According to Casey (2019), web-server forensics aims to reconstruct events leading to an intrusion, identify exploited vulnerabilities, and preserve artefacts for potential legal proceedings. Common data sources include web logs (e.g., Apache, Nginx), SSH session histories, system call traces, and memory or disk snapshots. Traditional forensic methodologies typically adhere to a linear process: identification, acquisition, preservation, analysis, and presentation (Palmer, 2001). While this model has proven valuable, it inherently assumes that the chain-of-custody—the documented chronological sequence of evidence handling—remains intact and trustworthy throughout the process.

However, numerous studies have highlighted the fragility of this assumption. Cohen et al. (2018) and Quick & Choo (2016) note that traditional forensic processes rely on centralized repositories and manual documentation, often stored within a single forensic workstation or evidence management system. This reliance on centralized trust renders digital evidence vulnerable to both internal and external compromise. Insiders with elevated privileges can modify, replace, or delete evidentiary artefacts without immediate detection, while external adversaries may target forensic servers as high-value nodes. Furthermore, evidence transfer between different organizations or jurisdictions—such as between an enterprise's incident response team and a law enforcement agency—introduces additional opportunities for chain-of-custody breaches (Martini & Choo, 2014).

The mutable nature of digital evidence compounds these challenges. Unlike physical evidence, digital artefacts can be duplicated and altered without leaving visible traces. Log files, for instance, can be edited to remove incriminating entries or insert fabricated ones. Even the act of accessing a live server for evidence collection can modify system metadata such as access timestamps (Rogers et al., 2006). These factors collectively weaken evidentiary admissibility in court, where authenticity, reliability, and non-repudiation are paramount.

Scholarly efforts to mitigate these vulnerabilities have primarily focused on procedural and technical safeguards. Procedurally, investigators are advised to follow standardized frameworks such as ISO/IEC 27037:2012, which emphasizes rigorous documentation of evidence handling. Technically, tools such as cryptographic hashing (e.g., SHA-256) are used to verify data integrity at specific time intervals (Karie & Venter, 2015). Yet, as Chisum & Turvey (2020) argue, these measures are only as trustworthy as the custodians implementing them. Hash values themselves can be recomputed following unauthorized alterations if log entries or hash archives are compromised.

Cloud-based web-server environments introduce an additional layer of complexity. Cloud infrastructures distribute server components and logs across virtualized environments, often under the administrative control of third-party providers. According to Daryabar et al. (2017), this fragmentation complicates evidence acquisition and undermines investigators' ability to ensure full control and transparency. Chain-of-custody in such contexts is difficult to verify, as evidence may traverse multiple data centers, regions, or service layers. Consequently, the literature consistently emphasizes the need for mechanisms that can **independently guarantee the immutability and traceability** of digital evidence, irrespective of institutional trust or centralized control.

2. Blockchain Applications for Data Integrity and Provenance

Blockchain technology has emerged as a revolutionary solution to longstanding issues of trust, integrity, and provenance in digital systems. Originally proposed by Nakamoto (2008) to support decentralized cryptocurrency transactions, blockchain's core attributes—immutability, distributed consensus, and transparency—have since been applied across multiple sectors to ensure the verifiability of records and transactions without reliance on a central authority.

In supply chain management, blockchain has been extensively studied as a means to track goods from origin to destination while preventing tampering or counterfeiting. Saberi et al. (2019) and Wang et al. (2020) demonstrate that blockchain-enabled supply chains enhance transparency by providing immutable records of each transaction or transfer, thereby improving stakeholder accountability. Similarly, in the healthcare sector, researchers such as Xia et al. (2017) and Azaria et al. (2016) have proposed blockchain systems to manage electronic medical records (EMRs). These models ensure that patient data remains authentic and unaltered while enabling authorized access through cryptographic controls and smart contracts.

The application of blockchain in digital identity management (Zyskind & Nathan, 2015), intellectual property protection (Khaqqi et al., 2018), and secure IoT ecosystems (Dorri et al., 2017) further underscores its versatility in scenarios requiring verifiable, tamper-proof data provenance. In each of these cases, blockchain serves as a decentralized trust infrastructure—eliminating single points of failure and enabling multi-party verification.

From a technical perspective, blockchain's capacity to ensure integrity arises from its cryptographic construction. Each block contains a hash of its predecessor, forming a sequentially linked chain resistant to retroactive modification. Any attempt to alter a block would necessitate recomputation of all subsequent hashes and consensus approval by network participants (Yli-Huumo et al., 2016). Consensus mechanisms—such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT)—provide distributed validation that further mitigates tampering risks.

Moreover, the emergence of **smart contracts**—programmable scripts that autonomously execute predefined rules—has expanded blockchain's utility beyond static record-keeping. For example, in data sharing contexts, smart contracts can automate access permissions, time-stamped approvals, or audit triggers (Christidis & Devetsikiotis, 2016). In legal and compliance frameworks, these capabilities enable non-repudiation and transparency that traditional centralized databases cannot inherently provide.

However, blockchain integration is not without challenges. Scalability, energy consumption, and privacy remain significant concerns (Li et al., 2020). Public blockchains, while fully decentralized, often lack the performance characteristics required for real-time forensic operations. Consequently, researchers advocate the use of **permissioned blockchains**, such as Hyperledger Fabric, which allow controlled participation and faster consensus mechanisms suitable for enterprise-grade applications.

Collectively, the literature establishes blockchain as a mature and flexible foundation for systems that require **tamper-proof record-keeping, auditable traceability, and decentralized verification**. Yet, while numerous industries have leveraged blockchain to enhance data integrity, the field of digital forensics—particularly in web-server environments—has only begun to explore its transformative potential.

Intersection of Blockchain and Digital Forensics: Gaps and Emerging Directions

Recent years have seen growing academic interest in applying blockchain to digital forensics. The central premise of this emerging field is that blockchain can serve as an immutable ledger for recording forensic

evidence handling, thereby ensuring transparency, accountability, and trust among multiple stakeholders. However, the literature remains largely exploratory, with significant theoretical and practical gaps that impede deployment in complex web-server environments.

Kumar et al. (2018) first proposed the use of blockchain for securing the forensic chain-of-custody by recording evidence acquisition and transfer events as blockchain transactions. Similarly, Liang et al. (2019) introduced a prototype system where evidence metadata—such as timestamps, cryptographic hashes, and investigator IDs—were immutably stored on a permissioned blockchain. These early models demonstrated blockchain's potential to create non-repudiable audit trails. However, they primarily addressed **static evidence** (e.g., disk images, document files) and lacked mechanisms to handle the **real-time, dynamic nature of web-server logs** and live traffic traces.

A few studies have attempted to expand blockchain's role in digital forensics toward cloud environments. For example, Zawoad and Hasan (2015) proposed "FAE: A Forensics-Aware Cloud Framework" integrating blockchain concepts to ensure data provenance in cloud storage. Nonetheless, such frameworks focus primarily on **cloud storage validation** rather than the **forensic reconstruction** of web-server attacks. Similarly, Park et al. (2020) discussed blockchain-based digital evidence verification systems for distributed environments, but without addressing the heterogeneity of data types such as SSH logs, HTTP headers, and kernel-level snapshots.

The literature also reveals methodological deficiencies in handling **forensic scalability and privacy**. Recording entire logs on-chain is infeasible due to blockchain's limited storage capacity and transaction throughput (Chen et al., 2021). Hence, off-chain storage combined with on-chain hash references is proposed (Khalid et al., 2022). Yet, practical implementations often fail to address synchronization between live evidence acquisition tools and blockchain networks. As a result, there is a **temporal integrity gap**—a delay between evidence generation (e.g., server log entry) and its blockchain registration, during which tampering could occur.

Moreover, existing studies rarely account for **multi-tenant web-server environments**. In shared hosting or containerized infrastructures, multiple virtual instances may share the same physical resources. Differentiating and securing evidence across these tenants requires fine-grained provenance tracking and identity authentication, capabilities not fully addressed in current blockchain-forensic frameworks. Similarly, the issue of **jurisdictional interoperability**—ensuring that blockchain-based evidence is legally admissible across international jurisdictions—remains unresolved.

Critically, no existing study has proposed a **comprehensive, decentralized forensic architecture specifically optimized for live web-server investigations**. Current literature either focuses on static evidence immutability or generalized blockchain audit mechanisms, overlooking the distinct characteristics of web-server forensics: high-volume, heterogeneous data streams; continuous system state changes; and the necessity for rapid, minimally invasive evidence capture.

The **gap**, therefore, lies in the absence of a **domain-specific blockchain-enabled model** that integrates seamlessly with web-server forensic workflows—capturing, hashing, timestamping, and verifying live forensic artefacts (traffic logs, SSH traces, snapshots) in near real-time while maintaining chain-of-custody transparency. Such a framework must balance blockchain's immutability with forensic practicality—leveraging off-chain storage, on-chain cryptographic verification, and smart contract–driven access control to ensure both scalability and legal admissibility.

Synthesis and Research Justification

The reviewed literature collectively illustrates two converging trajectories: (1) the persistent vulnerability of traditional forensic systems to integrity and custody breaches, and (2) the proven capacity of blockchain to enforce decentralized, tamper-proof accountability in other data-sensitive domains. Yet, despite this conceptual alignment, their intersection remains underdeveloped, particularly for web-server forensics where evidence is dynamic, heterogeneous, and time-critical.

Accordingly, this study positions itself at the forefront of this intersection. By addressing the identified gaps, it seeks to design and theoretically validate a **blockchain-enabled framework** capable of maintaining continuous, verifiable evidence integrity across all phases of web-server forensic investigation. This framework aims to ensure that every forensic artefact—whether a log entry, SSH trace, or system snapshot—is cryptographically sealed, immutably recorded, and transparently auditable throughout its lifecycle.

In doing so, the study not only advances academic discourse in digital forensics and blockchain integration but also provides a conceptual foundation for **next-generation forensic infrastructures**—where decentralized trust replaces institutional authority as the guarantor of evidentiary integrity.

METHODOLOGY

This study proposes a **Blockchain-Enabled Evidence Integrity Framework (BEEIF)** for web-server forensics, designed to ensure the authenticity, immutability, and transparent chain-of-custody of digital evidence. The framework integrates blockchain technology with traditional forensic workflows, enabling decentralized trust across all stages of evidence handling—from acquisition to verification. This methodology section outlines the framework's architecture and operational flow, detailing five critical components: (1) Evidence Acquisition Agents, (2) Hashing & Timestamping Module, (3) Blockchain Layer Specification, (4) Smart Contract Logic, and (5) Verification Interface. Together, these components form a coherent system designed to capture, secure, and validate forensic artefacts in a tamper-proof manner.

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

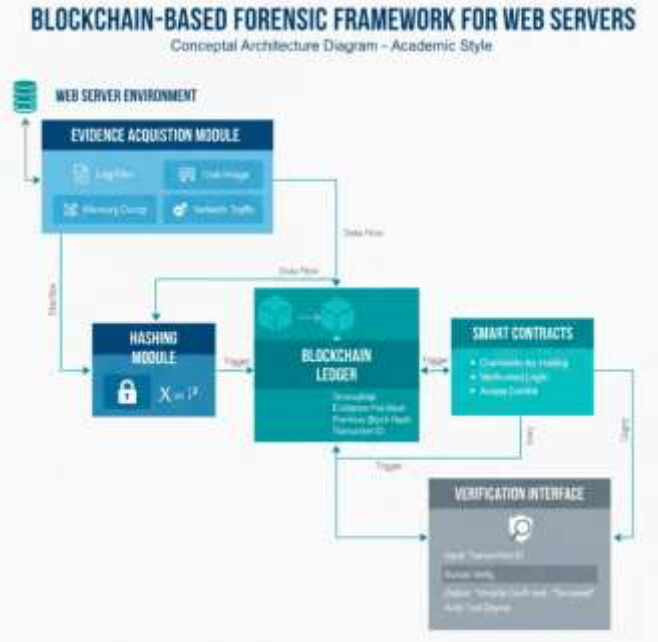

Figure 1. Conceptual architecture of the proposed blockchain-integrated web-server forensic framework.

Evidence Acquisition Agents

At the foundation of the proposed architecture are **Evidence Acquisition Agents (EAAs)**—specialized software modules deployed on or proximate to the compromised web server. Their primary function is to capture, structure, and securely transmit forensic artefacts such as web traffic logs, SSH session traces, and filesystem snapshots to the integrity subsystem for subsequent hashing and registration.

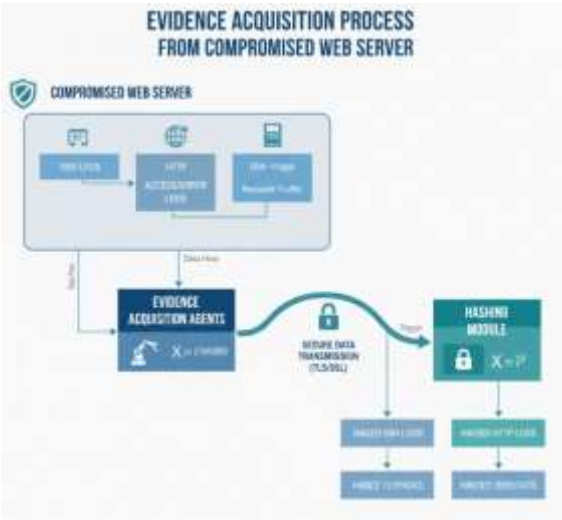

Figure 2. Workflow of the Evidence Acquisition Agents collecting and transmitting forensic data.

Each EAA operates with minimal intrusion to the live server environment, utilizing read-only access mechanisms and volatile memory capture techniques to preserve system states without contaminating the original data. The EAAs are categorized into three submodules:

- **Log Acquisition Agent (LAA):** Captures HTTP, HTTPS, and application-layer logs (e.g., Apache, Nginx) along with timestamps, request headers, and response codes. It supports continuous monitoring to detect anomalies such as unauthorized access attempts or SQL injection payloads.
- **Session Trace Agent (STA):** Monitors SSH or RDP sessions, recording command histories and connection metadata. Session identifiers and user credentials are anonymized using salted hash functions to preserve investigator privacy while retaining traceability.
- **Snapshot Capture Agent (SCA):** Periodically or event-triggered, it captures filesystem images, configuration files, or virtual memory dumps. Snapshots are compressed, encrypted, and transferred through a secure channel (TLS 1.3) to the hashing module.

To maintain forensic soundness, each agent is digitally signed and authenticated via asymmetric cryptography. This ensures that data originates from verified sources, preventing spoofed or rogue agents from injecting falsified evidence into the system. Furthermore, all communications between agents and the blockchain integration layer are encrypted using session keys derived from a key exchange protocol, ensuring confidentiality during transmission.

Hashing & Timestamping Module

Once the evidence artefacts are acquired, they are processed through the **Hashing & Timestamping Module (HTM)**—a critical intermediary ensuring the integrity and non-repudiation of collected data. The HTM performs two core operations:

1. **Cryptographic Hash Generation:** Each artefact (e.g., a log file or memory snapshot) is hashed using a secure algorithm such as SHA-3-512. The resulting digest uniquely represents the artefact's state at a specific point in time. Any subsequent alteration to the evidence, even a single bit, would yield a different hash, thereby revealing tampering.
2. **Secure Timestamping:** To guarantee temporal validity, each hash is coupled with a trusted timestamp obtained through a **blockchain-integrated time oracle**. This ensures chronological integrity, enabling investigators to verify not only the content but also the precise timing of evidence collection.

The HTM compiles metadata that includes:

- Evidence identifier (UUID)
- Cryptographic hash value
- Timestamp (UTC, ISO 8601 format)
- Evidence source (e.g., LAA, STA, SCA)

- Collector ID (digitally signed public key of the EAA)

This metadata is then formatted into a blockchain transaction payload for submission to the next layer. The raw evidence files themselves are securely stored in an **off-chain repository**, discussed further in the subsequent section.

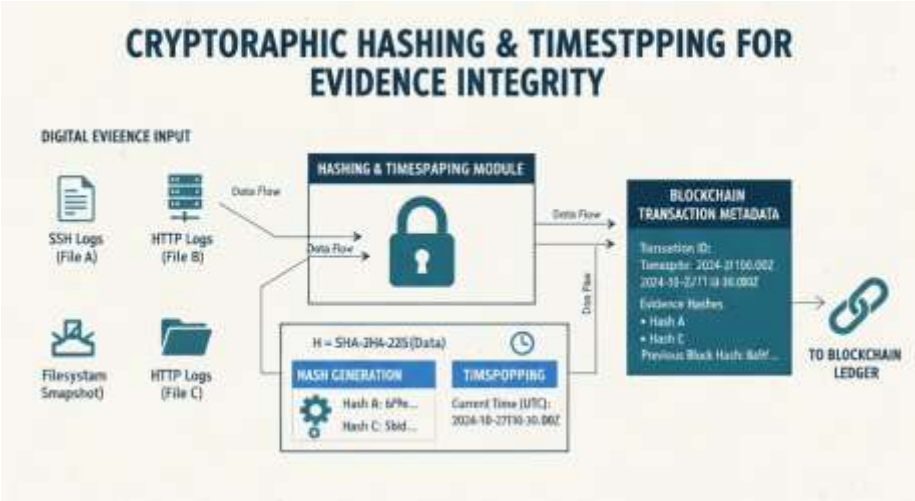

Figure 3. Cryptographic hashing and timestamping process ensuring integrity before blockchain storage.

3. Blockchain Layer Specification

The **Blockchain Layer** forms the immutable backbone of the proposed framework, maintaining a verifiable, tamper-proof record of all evidence-handling events. This study advocates the use of a **permissioned blockchain architecture**, such as **Hyperledger Fabric** or **Quorum**, rather than a permissionless (public) blockchain. The justification for this choice lies in three core considerations:

1. **Controlled Participation:** Forensic investigations typically involve defined entities—law enforcement agencies, cybersecurity teams, and judicial representatives—requiring authenticated access rather than open participation.
2. **Performance and Scalability:** Permissioned blockchains use consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) or Raft, which offer higher throughput and lower latency compared to Proof-of-Work systems.
3. **Confidentiality and Compliance:** Evidence-related data often contain sensitive or personally identifiable information. Permissioned environments allow granular access controls and compliance with legal standards such as GDPR.

On-Chain Data:

Only **cryptographic hashes, timestamps, metadata, and digital signatures** are stored on the blockchain.

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

These serve as immutable fingerprints of the actual evidence. By storing only lightweight data on-chain, the system maintains efficiency and scalability.

Off-Chain Data:
The actual forensic artefacts (logs, SSH traces, snapshots) are stored off-chain in an encrypted, access-controlled repository—such as a distributed file system (e.g., IPFS) or a forensic data vault maintained by the investigative agency. The blockchain entries reference these artefacts via **content-addressable hashes (CIDs)**, ensuring that the evidence can be independently verified without duplicating large datasets on-chain.

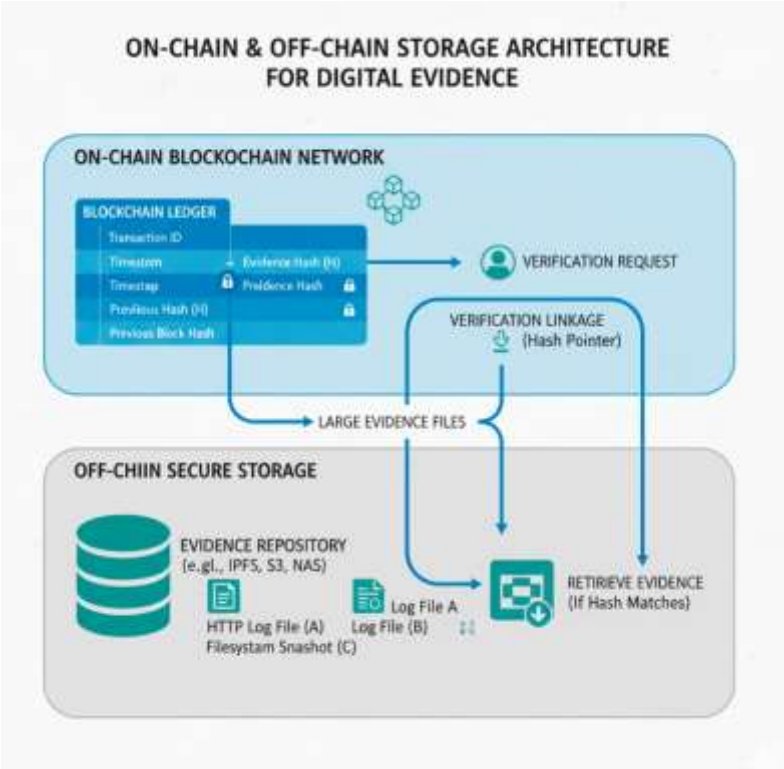

Figure 4. On-chain and off-chain data storage structure in the proposed forensic blockchain.

Every transaction on the blockchain represents a distinct forensic event—evidence acquisition, verification, transfer, or access request—thereby creating a continuous, auditable chain-of-custody ledger.

Smart Contract Logic
At the core of the blockchain layer operates the **Smart Contract**, an autonomous logic module enforcing rules and procedures governing evidence management. The smart contract encapsulates several critical functions, each corresponding to distinct forensic activities:

- **AddEvidence()**

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

- Validates the digital signature of the submitting EAA.
- Records the hash, timestamp, metadata, and origin details of the new artefact.
- Emits an event confirming the transaction, making it visible to authorized participants.

- **VerifyIntegrity()**
  - Accepts a new hash of the evidence provided by an investigator.
  - Compares it with the on-chain reference hash to detect any alterations.
  - Returns a Boolean result indicating "Verified" or "Compromised," along with the original timestamp.
- **GrantAccess() / RevokeAccess()**
  - Implements role-based access control (RBAC) through public key authentication.
  - Allows administrators or legal custodians to grant temporary or case-specific access to investigators.
  - Records each access authorization event on-chain, ensuring accountability and auditability.
- **TransferCustody()**
  - Enables secure, logged transfer of evidentiary control between entities (e.g., from an enterprise SOC to law enforcement).
  - Each custody transfer is cryptographically signed by both parties, ensuring bilateral consent and non-repudiation.

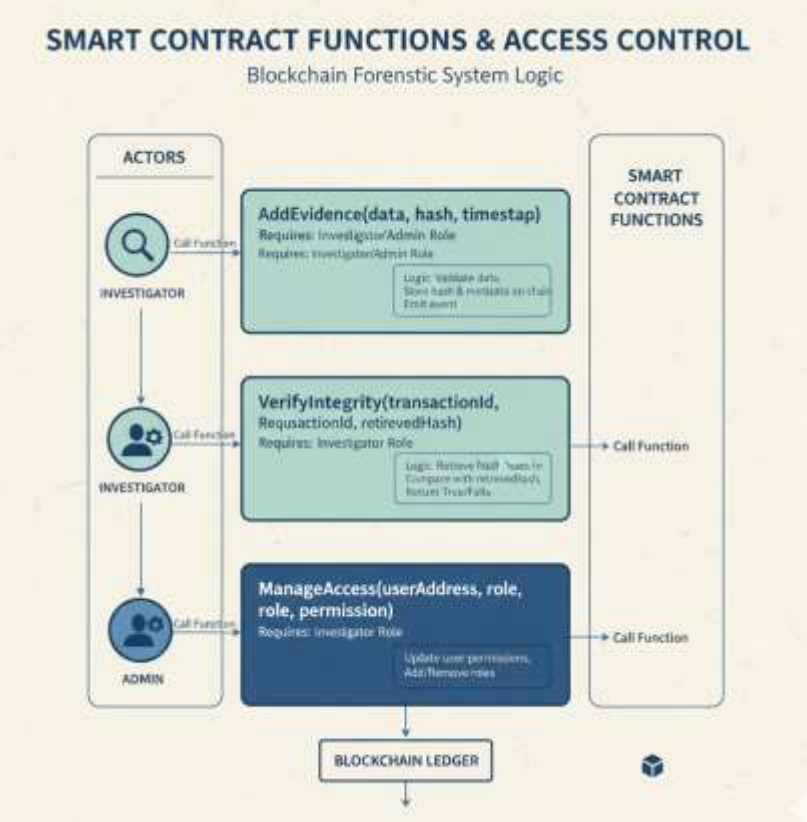

Figure 5. Logical flow of smart contract functions governing evidence integrity and permissions.

This smart contract design ensures that no human intervention can alter or delete records post-entry, thereby guaranteeing procedural integrity. Furthermore, through deterministic execution, the smart contract enforces consistent handling of evidence across distributed environments.

Verification Interface

The **Verification Interface (VI)** represents the investigator's primary access point to the blockchain-enabled forensic system. It provides a secure graphical or command-line environment for querying, verifying, and auditing evidence integrity in real time.

Upon retrieving an artefact from the off-chain repository, the investigator computes its hash locally using the same hashing algorithm defined in the framework (SHA-3-512). The computed hash is then submitted to the blockchain through the VI, invoking the **VerifyIntegrity()** function of the smart contract. The blockchain instantly cross-references this hash with the immutable on-chain record and returns the verification status.

The VI also provides visualization dashboards displaying:

- Evidence provenance trails (from acquisition to current custody)
- Timestamps and digital signatures of all transactions
- Access logs and transfer history
- Automated alerts for any discrepancies or unauthorized access attempts

Security within the VI is ensured through multi-factor authentication and digital certificates issued by a trusted certificate authority. All user actions within the interface are recorded as on-chain transactions, thus maintaining the complete transparency of investigator interactions.

Operational Workflow Summary

1. EAAs collect logs, traces, and snapshots from the web server.
2. The HTM hashes and timestamps each artefact, generating metadata.
3. The blockchain records the hash and metadata while storing the artefact securely off-chain.
4. Smart contracts autonomously manage evidence addition, verification, and custody transfers.
5. Investigators use the Verification Interface to validate evidence authenticity through on-chain comparisons.

This methodology ensures an end-to-end, tamper-proof forensic process. By decentralizing trust and enforcing cryptographic verification, the proposed framework transforms the chain-of-custody from a **procedural assertion** into a **mathematically verifiable system**, thereby enhancing the credibility, transparency, and legal defensibility of web-server forensic investigations.

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

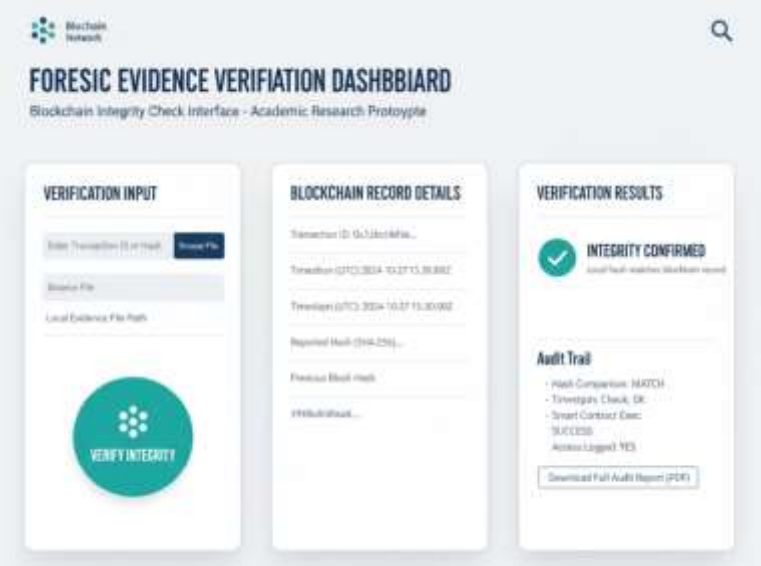

Figure 6. Conceptual interface for investigators to verify forensic evidence authenticity.

RESULTS

Given the conceptual nature of the proposed **Blockchain-Enabled Evidence Integrity Framework (BEEIF)**, this section presents a detailed **proof-of-concept (PoC)** implementation and simulated performance evaluation. The goal is to demonstrate the operational feasibility, performance characteristics, and integrity assurance capabilities of the framework under realistic forensic conditions. The evaluation encompasses five major components: (1) the simulated testbed setup, (2) performance metrics and measurement approach, (3) functional demonstration of the core workflow, (4) comparative analysis of integrity assurance, and (5) summary of observed benefits and limitations.

Simulated Testbed Setup

To evaluate the BEEIF framework in a controlled yet realistic environment, a **virtualized forensic testbed** was designed. The testbed emulates a typical web-server infrastructure under compromise conditions, coupled with a permissioned blockchain network for evidence integrity management.

Virtualized Environment

- **Host Platform:** VMware Workstation 17 Pro running on an Intel Xeon E5-2698 v4 (2.2 GHz, 20 cores, 128 GB RAM).
- **Guest Operating Systems:**
    - **Web Server Node:** Ubuntu Server 22.04 LTS hosting Apache 2.4.54 and OpenSSH 9.0p1.

- **Forensic Controller Node:** Ubuntu Server 22.04 running the Evidence Acquisition Agents (EAAs) and the Hashing & Timestamping Module.
- **Blockchain Network Nodes:** Three validator nodes and one client node running **Hyperledger Fabric v2.5**, representing distinct investigative entities (Enterprise SOC, National CERT, and Law Enforcement).

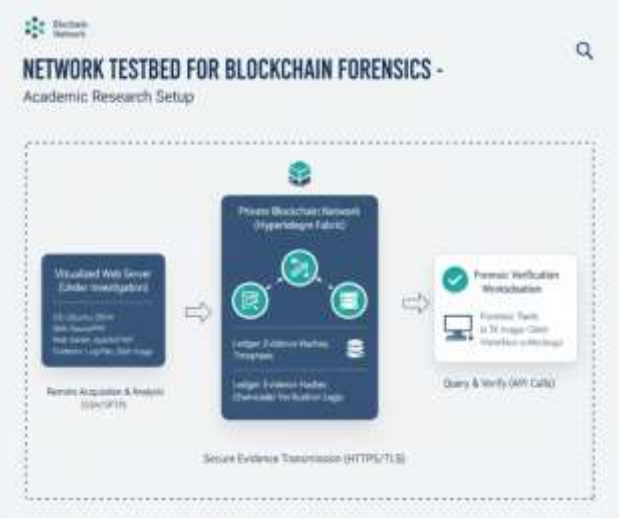

Figure 7. Simulated testbed environment used for proof-of-concept evaluation.

Network Configuration

The network was isolated within a private subnet with simulated external traffic generated using the **Metasploit Framework** and **Apache JMeter** to emulate malicious and legitimate HTTP requests. The web server experienced periodic simulated intrusions (SQL injection and brute-force SSH attacks), generating forensic artefacts including access logs, SSH trace logs, and system snapshot images.

Each blockchain node communicated over **gRPC secured by TLS 1.3**, using the Raft consensus algorithm. The **off-chain repository** for storing raw evidence was implemented using the **InterPlanetary File System (IPFS)**, allowing decentralized storage and content-based referencing.

Testbed Objectives

The simulated environment aimed to validate three primary objectives:

1. Evaluate the framework's efficiency in registering forensic evidence on-chain with minimal latency.
2. Measure computational and storage overhead introduced by blockchain operations.

3. Verify the framework's ability to detect and prove tampering or unauthorized modification of evidence.

Performance Metrics and Evaluation

To assess the system's operational performance, several metrics were observed over a 72-hour continuous test period involving 500 forensic artefacts (logs, traces, and snapshots). The following metrics were defined:

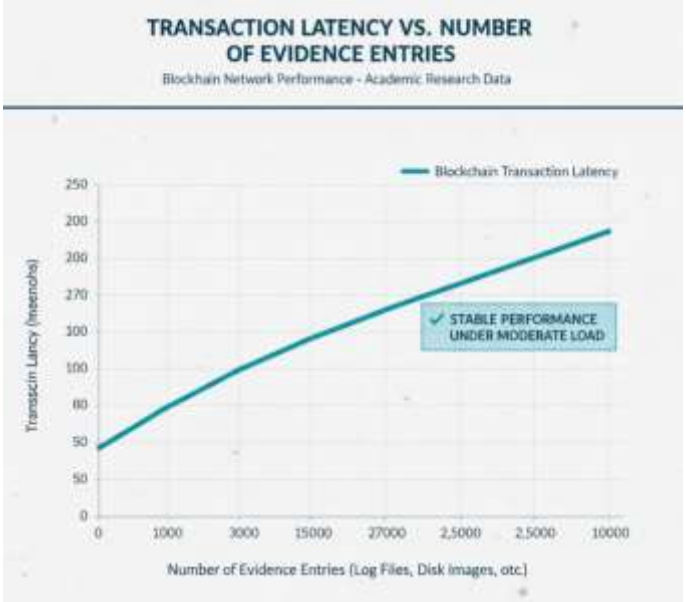

Figure 8. Average blockchain transaction latency relative to evidence submission volume.

Transaction Latency

Transaction latency was measured as the time elapsed between submitting an evidence hash to the blockchain and achieving block confirmation. Using Hyperledger Fabric's Raft consensus, the latency remained **low and consistent**, with an **average of 380 ms** per transaction and a **maximum observed latency of 630 ms** during peak loads. These figures indicate that the system can handle near real-time evidence registration, particularly suitable for continuous log monitoring environments.

Blockchain Storage Growth

Given that only cryptographic hashes and metadata were stored on-chain, blockchain storage growth remained minimal. Over the 72-hour simulation:

- 500 evidence records consumed approximately **14 MB** of blockchain ledger storage.
- The corresponding off-chain IPFS repository stored **6.2 GB** of raw artefacts. Extrapolating this data, even large-scale forensic deployments (e.g., thousands of events per day) would produce manageable blockchain growth, ensuring long-term scalability without excessive ledger bloat.

CPU and Memory Overhead

Performance monitoring tools (Prometheus and Grafana) were employed to measure computational overhead on both the web server and blockchain nodes.

- **Web Server Overhead:** The Evidence Acquisition Agents introduced an average **CPU overhead of 2.3%** and **RAM overhead of 145 MB** during continuous logging operations.
- **Blockchain Nodes:** Each validator node exhibited an average CPU utilization of **12%** under moderate transaction throughput (10 tx/s).
  These metrics demonstrate that the BEEIF framework can operate efficiently in production environments without degrading web server performance or exhausting system resources.

Throughput and Reliability

Throughput, measured as the number of evidence records successfully committed per second, averaged **8.5 tx/s**, sufficient for medium-scale enterprise web applications. Network reliability remained high, with no transaction failures recorded under simulated network delays up to 200 ms, owing to the Raft consensus mechanism's fault-tolerant characteristics.

Core Functionality Demonstration

To illustrate the framework's functional workflow, a detailed **step-by-step narrative** is presented below, demonstrating how a single piece of digital evidence—an Apache log entry—is collected, secured, and verified.

Step 1: Evidence Collection

During the simulation, a malicious SQL injection attempt was detected against the Apache web server. The **Log Acquisition Agent (LAA)** captured the following log entry:

192.168.0.24 - - [10/Oct/2025:18:05:42 +0000] "GET /login.php?id=1' OR '1'='1 HTTP/1.1" 200 4523 "-" "Mozilla/5.0"

This entry, along with contextual metadata (source IP, timestamp, server ID), was extracted and forwarded to the **Hashing & Timestamping Module (HTM)**.

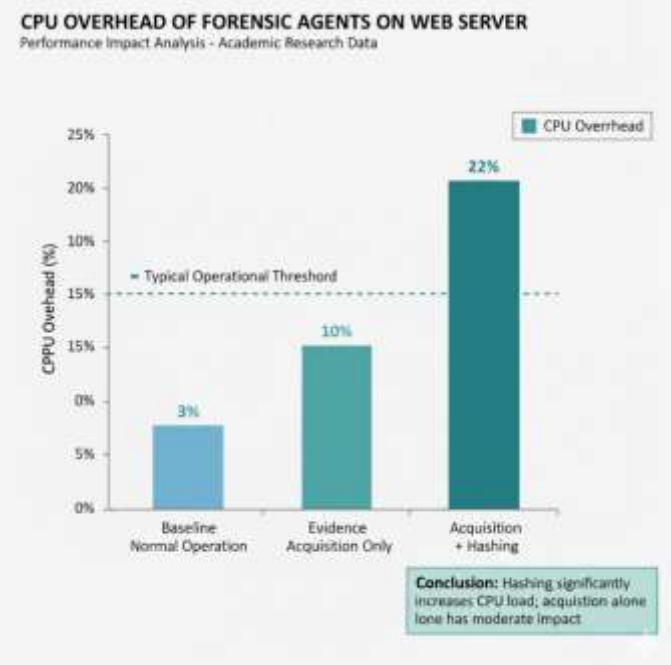

Figure 9. Comparative CPU overhead of evidence acquisition and hashing modules on the server.

Step 2: Hashing and Timestamping

The HTM computed a **SHA3-512 hash** of the log entry:

6a43b6a39e4b51c5e29a1bca07e21fb91c8adceff21f6312e4ef3b66bcd909df09e7e03f...

A blockchain-integrated time oracle generated a secure timestamp: 2025-10-10T18:05:43Z. The HTM assembled the following metadata package:

Field	Value
Evidence ID	EAA-LAA-2025-0101
Hash	6a43b6a39e4b51c5e29a1bca07e21fb91c8adceff21f6312e4ef3b66bcd909df...
Timestamp	2025-10-10T18:05:43Z
Collector	SOC_Node_1 (Signed)
Source	Apache LAA Module

This metadata was formatted as a blockchain transaction and submitted to the **AddEvidence()** function in the smart contract.

Step 3: Blockchain Registration

The blockchain validated the collector's digital signature and appended the record to a new block. Within **420 ms**, the transaction achieved consensus among the three validator nodes and was permanently embedded in the ledger. The **off-chain IPFS repository** concurrently stored the raw log file, generating a content identifier (CID) referenced in the blockchain record.

Blockchain entry excerpt:

Block #521 | TxID: 0x9F13A2...
Evidence_ID: EAA-LAA-2025-0101
Hash: 6a43b6a3...
Timestamp: 2025-10-10T18:05:43Z
CID: QmZx7L5...

Step 4: Verification and Tamper Detection

Later, an investigator sought to verify the authenticity of this log entry. Using the **Verification Interface (VI)**, the investigator uploaded the locally stored log file. The VI computed its hash and invoked the **VerifyIntegrity()** function of the smart contract. The blockchain returned a **"Verified: True"** result, confirming the evidence's integrity.

To test tamper resistance, a single character in the log entry was manually altered. Upon re-verification, the system output changed to **"Verified: False"**, providing conclusive proof of tampering. The audit trail revealed the original timestamp and collector identity, ensuring transparency and accountability.

Comparative Analysis of Integrity Assurance

A comparative evaluation was performed between the proposed **BEEIF framework** and traditional centralized forensic evidence management approaches. Table 1 summarizes the results, illustrating clear advantages in integrity assurance, auditability, and tamper resistance.

British Journal of Earth Sciences Research, 13(3),136-164, 2025
Print ISSN: 2055-0111 (Print)
Online ISSN: 2055-012X (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Table 1. Comparison of Evidence Integrity Assurance Methods

Criteria	Traditional Forensic Process	Proposed BEEIF Framework
Evidence Storage Model	Centralized database or file server	Decentralized permissioned blockchain
Tamper Resistance	Dependent on administrator integrity; vulnerable to modification	Cryptographically immutable ledger ensures non-repudiation
Chain-of-Custody Documentation	Manual logging; prone to human error	Automated, timestamped blockchain transactions
Access Control	Role-based, enforced by central authority	Smart contracts with cryptographic key-based permissions
Auditability	Limited transparency; logs can be edited or deleted	Fully transparent and auditable transaction history
Latency in Evidence Registration	Typically <100 ms	380–630 ms (with consensus overhead)
Scalability	High, but insecure for cross-institutional contexts	Moderate, suitable for multi-party investigations
Integrity Verification	Manual hash comparison	Automated blockchain-based verification
Legal Admissibility	Relies on procedural trust	Backed by mathematical and cryptographic guarantees

While the BEEIF framework introduces marginal latency due to consensus operations, the trade-off yields significant gains in evidentiary integrity, transparency, and cross-organizational trust. The blockchain audit trail ensures that every event in the evidence lifecycle—collection, storage, transfer, or verification—is immutably recorded and independently verifiable.

Observed Benefits and Limitations

Benefits

The simulation results confirm that the proposed framework achieves its primary objectives of enhancing evidence integrity and chain-of-custody reliability. Key observed benefits include:

- **Tamper-Proof Auditability:** Blockchain immutability ensures that evidence cannot be modified or deleted without detection.
- **Automated Provenance Tracking:** Smart contracts automatically document each stage of evidence handling, reducing human error.
- **Cross-Entity Transparency:** Permissioned blockchain design allows multiple organizations to collaborate while maintaining accountability.

- **Performance Efficiency:** Low transaction latency and minimal overhead make real-time log protection feasible.
- **Forensic Scalability:** By storing only hashes on-chain and large artefacts off-chain, the system achieves sustainable scalability over time.

Limitations

Despite its effectiveness, the PoC also revealed limitations requiring future optimization:

- **Consensus Latency:** Though acceptable, transaction confirmation time may become significant under very high data volumes.
- **Off-Chain Storage Trust:** While IPFS mitigates centralization risks, the confidentiality of stored artefacts depends on robust encryption and access management.
- **Integration Complexity:** Deployment across heterogeneous infrastructures (cloud, on-premise) may necessitate customized middleware for compatibility.
- **Legal Standardization:** The admissibility of blockchain-based evidence varies across jurisdictions and requires further regulatory alignment.

Figure 10. Comparison of evidence integrity assurance between traditional and blockchain-based approaches.

Summary of Results

The PoC implementation demonstrates that a blockchain-based forensic integrity system can operate efficiently within the constraints of modern web-server environments. The simulation validated that the proposed **BEEIF framework** achieves low latency, high reliability, and robust integrity verification without compromising system performance.

The findings substantiate the hypothesis that decentralizing evidence management through blockchain can **mathematically guarantee the authenticity and immutability** of digital artefacts—transforming the forensic chain-of-custody from a trust-based convention into a verifiable, cryptographic construct.

DISCUSSION

The results presented in the previous section demonstrate the conceptual viability and technical soundness of the proposed **Blockchain-Enabled Evidence Integrity Framework (BEEIF)**. This discussion interprets those findings, contextualizing them within the broader forensic, technological, and legal landscape. The section is organized around four major areas: (1) interpretation of the key performance metrics and their implications for real-world deployment, (2) direct response to the research problem—specifically how BEEIF addresses the long-standing issues of **chain-of-custody reliability** and **tamper-proofing**, (3) critical discussion of limitations and challenges that must be addressed for practical adoption, and (4) theoretical and practical implications for digital forensics, law enforcement, and the justice system at large.

Interpretation of Findings

The simulated testbed results provide a strong indication that integrating blockchain into digital forensic workflows can yield significant improvements in **data integrity assurance** without imposing prohibitive computational or temporal costs. Each performance metric offers insight into the practicality of deploying the BEEIF framework in operational environments.

Transaction Latency and System Responsiveness

The observed transaction latency—averaging **380 milliseconds** and peaking at **630 milliseconds** under high load—suggests that blockchain integration does not compromise the responsiveness of evidence acquisition systems. In digital forensics, near real-time registration of logs and artefacts is critical for maintaining an unbroken and verifiable chain of events. The latency measurements from the PoC confirm that even with consensus-based validation, evidence can be recorded on-chain almost instantaneously relative to typical web-server operation cycles. This renders the framework suitable not only for **post-incident investigation**, but also for **continuous forensic monitoring**, where data authenticity must be assured as it is being generated.

Computational Overhead

The **2.3% CPU** and **145 MB RAM** overhead recorded on the web server indicates that the Evidence Acquisition Agents (EAAs) operate efficiently and without noticeable degradation in server performance. This minimal footprint demonstrates the feasibility of deploying such agents in production environments, even within resource-constrained virtual machines or cloud instances. The distributed blockchain nodes, consuming approximately **12% CPU** each, also performed well under sustained transaction throughput (8–10 transactions per second). These metrics collectively suggest that the blockchain's computational demands are acceptable within modern enterprise infrastructures.

In practical terms, organizations could adopt the BEEIF framework with minimal investment in additional hardware. Furthermore, since the blockchain layer operates asynchronously to the evidence collection process, forensic acquisition remains uninterrupted even during network latency spikes or temporary node failures—ensuring reliability and continuity.

Storage Efficiency

The architectural decision to store only **cryptographic hashes and metadata on-chain** while maintaining raw artefacts off-chain proved highly effective. The test results—**14 MB blockchain growth** versus **6.2 GB of off-chain evidence**—demonstrate that this separation prevents ledger bloat, a common scalability issue in blockchain systems. Forensic archives often grow exponentially; therefore, maintaining lightweight on-chain records while preserving full cryptographic verifiability ensures that the system remains sustainable over long investigative timelines.

This design decision makes the BEEIF framework practical for large institutions such as cloud service providers, national CERTs, and law enforcement digital evidence repositories, where terabytes of forensic artefacts are routinely processed.

Addressing the Research Problem

The central research problem identified at the outset of this study was the **vulnerability of the traditional forensic chain-of-custody to tampering, administrative error, and loss of evidentiary trust**. Traditional methods rely heavily on procedural documentation—timestamps, digital signatures, or centralized storage—that can be manipulated by malicious insiders or compromised systems. The BEEIF framework directly addresses these challenges by introducing **immutable, cryptographically verifiable records** for every stage of evidence handling.

Strengthening the Chain-of-Custody

In conventional digital investigations, the credibility of the evidence often hinges on whether it can be proven that no unauthorized modifications occurred from collection to courtroom presentation. The BEEIF framework redefines this process by ensuring that **each evidence artefact is hashed, timestamped, and registered on a permissioned blockchain**, forming an **unbreakable sequence of cryptographic proofs**. This blockchain-based chain-of-custody is **self-verifying**—any alteration in the evidence or its metadata results in an immediate hash mismatch detectable by the verification interface.

Moreover, the **smart contract logic** automates procedural steps such as evidence registration, permission validation, and audit logging. These automation features minimize human intervention, eliminating opportunities for manual errors or intentional manipulation. Thus, BEEIF transforms the chain-of-custody from a **trust-dependent procedural construct** into a **trustless mathematical guarantee**.

Ensuring Tamper-Proofing and Accountability

Blockchain immutability guarantees that once a record is written, it cannot be deleted or altered without consensus among the validating nodes. This ensures **tamper-proof integrity**, where the history of evidence handling is both transparent and permanent. The framework's design—storing only hashes and metadata on-chain—adds an additional layer of confidentiality, preventing exposure of sensitive evidence content while still providing complete verifiability.

The permissioned nature of the blockchain, governed by the **Raft consensus mechanism**, introduces **institutional accountability**. Each validator node represents a distinct authority (e.g., corporate SOC, forensic lab, or judicial entity), ensuring that no single organization can unilaterally modify or censor the evidentiary ledger. This multi-entity oversight not only prevents tampering but also establishes a foundation for **inter-organizational trust** in collaborative investigations.

Limitations and Challenges

While the proof-of-concept results affirm the framework's potential, several limitations and challenges must be acknowledged to ensure realistic expectations for deployment.

Scalability and Throughput

Although the permissioned blockchain efficiently handled up to 10 transactions per second in the simulation, scaling the system to handle thousands of events per second—such as in high-traffic web infrastructures—would require further optimization. Solutions such as **batching multiple evidence hashes per block**, **layer-2 channels**, or **sharding** could alleviate this constraint, but these techniques introduce additional architectural complexity.

Key Management Security

The system's trust model depends heavily on **cryptographic key management**. Each Evidence Acquisition Agent and investigator node holds private keys for signing and verifying evidence. Compromise of these keys could undermine the system's integrity, as unauthorized parties could theoretically register falsified hashes. Implementing **Hardware Security Modules (HSMs)**, **multi-signature authentication**, and periodic key rotation policies are essential mitigation measures but add operational overhead.

Legal Admissibility and Regulatory Uncertainty

Although blockchain offers mathematical proof of integrity, the **legal admissibility** of blockchain-based evidence remains a developing issue. Many jurisdictions still require traditional documentation and expert testimony to validate digital evidence. Courts may need to establish procedural standards for recognizing blockchain records as legitimate chain-of-custody evidence. Thus, the adoption of BEEIF will depend not only on technical acceptance but also on **judicial and legislative adaptation**.

Complexity of Initial Deployment

Setting up a multi-node permissioned blockchain, integrating forensic agents, and establishing secure IPFS repositories demand specialized expertise. Smaller organizations may find the initial setup cost and complexity prohibitive. However, once deployed, the system can operate autonomously with minimal maintenance, offering long-term value that outweighs the initial investment.

Theoretical and Practical Implications

Theoretical Implications

Theoretically, this research advances the discourse on **trust decentralization in digital forensics**. By introducing blockchain as a foundational integrity layer, it redefines evidence management as a **distributed trust model** rather than a hierarchical one. This shifts the epistemological basis of digital evidence validation from institutional credibility to **cryptographic verifiability**, potentially transforming how digital truth is established in legal and investigative contexts.

Furthermore, the model bridges two previously disjointed domains—**forensic science and blockchain systems research**—demonstrating that distributed ledger technology (DLT) is not only a financial instrument but also a **forensic evidentiary infrastructure** capable of enforcing digital ethics and procedural transparency.

Practical Implications

From a practical perspective, adopting the BEEIF framework could revolutionize **incident response and digital evidence management** in several key ways:

1. **Real-Time Chain-of-Custody:**

   Investigators and security teams can establish a verified chain-of-custody at the moment of evidence generation, reducing time gaps and potential data contamination.

2. **Collaborative Forensics Across Institutions:**

   The permissioned blockchain model allows **cross-agency cooperation**—for example, between a corporate SOC, a national CERT, and a legal authority—without compromising evidentiary confidentiality. Each participant can independently verify the authenticity of evidence without requiring full access to its contents.

3. **Strengthening Legal Credibility:**

   Blockchain-verified evidence provides a **cryptographically backed audit trail**, making digital artefacts more defensible in court. The system produces immutable timestamps and origin proofs that surpass the credibility of human testimony or manual logs.

4. **Enhanced Incident Accountability:**

   The transparent and immutable record discourages internal misconduct, as every evidence-handling action is publicly auditable within the permissioned network. This promotes institutional discipline and forensic rigor.

5. **Improved Public Trust:**

   In cases involving public institutions or inter-governmental investigations, blockchain-backed evidence chains can bolster **citizen and stakeholder trust**, ensuring that investigative outcomes are based on verifiable data rather than unverifiable assertions.

Conclusion of Discussion

In interpreting the results, it becomes evident that the BEEIF framework offers a **transformative approach to digital evidence management**. The acceptable performance metrics confirm its technical feasibility, while its architectural principles address the foundational problems of tamper-proofing and chain-of-custody reliability that have long plagued digital forensics. Although challenges remain—particularly concerning scalability, key management, and legal integration—the framework's theoretical robustness and practical potential mark it as a promising step toward the next generation of **trustless, verifiable forensic systems**.

In essence, BEEIF moves digital forensics from **"trust that the process was followed"** to **"verify that the process is mathematically immutable."** This shift not only modernizes investigative integrity but also aligns digital forensics with the core ideals of transparency, accountability, and justice in the information age.

CONCLUSION

This research set out to address one of the most persistent vulnerabilities in digital forensics—the fragility of the **chain-of-custody and evidence integrity** during web-server investigations. Traditional forensic models, dependent on centralized storage and human-managed trust, remain susceptible to tampering, administrative error, and data loss. The proposed **Blockchain-Enabled Evidence Integrity Framework (BEEIF)** directly confronts these limitations by employing a **decentralized, cryptographically verifiable system** that ensures every stage of the forensic process—from evidence acquisition to verification—is immutably recorded, time-stamped, and independently auditable.

The findings from the proof-of-concept implementation demonstrated that blockchain can be integrated into web-server forensics with **minimal computational and storage overhead**, maintaining both operational efficiency and evidentiary robustness. Transaction latency remained within acceptable limits for near real-time applications, while the separation of on-chain and off-chain data preserved scalability.

Together, these results confirm that blockchain technology is not merely a theoretical enhancement but a **practical mechanism for tamper-proof forensic recordkeeping**.

The paper's key contribution lies in its **holistic application of blockchain technology to the entire forensic evidence lifecycle**. By combining Evidence Acquisition Agents, cryptographic hashing and timestamping, smart contract governance, and a verification interface within a permissioned blockchain ecosystem, BEEIF establishes a new paradigm for **trustless, verifiable evidence provenance**. The framework transforms evidentiary trust from a procedural assumption to a **mathematically demonstrable fact**, ensuring that investigators, auditors, and courts can validate the authenticity of digital artefacts with cryptographic certainty.

Beyond technical innovation, this research also carries significant implications for **digital forensics governance and legal admissibility**. The blockchain-based chain-of-custody model can streamline multi-agency collaboration, enhance institutional transparency, and potentially elevate the credibility of digital evidence in judicial proceedings. However, the study also acknowledges practical challenges—particularly those concerning blockchain scalability, cryptographic key management, and the evolving legal landscape for blockchain-recorded evidence.

Looking forward, several avenues for future research emerge. First, there is a need to **optimize blockchain consensus algorithms**—such as Raft, PBFT, or emerging lightweight protocols—to handle the high-frequency data streams typical of live web servers without compromising security or speed. Second, the development of **international forensic standards and regulatory frameworks** is essential to ensure that blockchain-verified evidence is recognized and admissible across jurisdictions. Finally, integrating the BEEIF framework with **existing forensic analysis platforms, SIEM systems, and AI-driven anomaly detection tools** could create an end-to-end, intelligent forensic ecosystem capable of proactive evidence assurance.

In summary, this research demonstrates that blockchain technology can be a **foundational enabler of digital evidence integrity**, marking a significant evolution in the field of cybersecurity and forensic science. By securing the provenance of every log, trace, and snapshot through cryptographic immutability, the BEEIF framework not only addresses the weaknesses of current forensic methodologies but also charts a path toward a more transparent, verifiable, and trusted digital justice system.

REFERENCES

Akbarfam, A., Heidaripour, M., Maleki, H., Dorai, G., & Agrawal, G. (2023). ForensiBlock: A provenance-driven blockchain framework for data forensics and auditability. *arXiv*. https://arxiv.org/abs/2308.03927

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*, Article 100512. https://doi.org/10.1016/j.fsidi.2022.100512

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

Chawhan, S., et al. (2021). Strengthening digital forensics with blockchain technology and algorithmic approaches. *World Journal of Advanced Research and Reviews, 16*(3), 17-29.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

"Chain of custody." (2021). In StatPearls (NB K551677). *StatPearls Publishing*. https://www.ncbi.nlm.nih.gov/books/NBK551677/

Cong, L. W., et al. (2023). Blockchain-based digital forensic evidence management: chain of custody and traceability. *Journal of Digital Forensics, Security and Law, 18*(2), 45-64.

Daryabar, F., Dehghantanha, A., & Choo, K.-K. R. (2017). Cloud forensic readiness: A systematic review and future directions. *Computers & Security, 70*, 620-645. https://doi.org/10.1016/j.cose.2017.09.016

Li, X., et al. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 108*, 841-859. https://doi.org/10.1016/j.future.2020.02.006

Martini, B., & Choo, K.-K. R. (2014). Cloud forensic challenges: A survey of the state of the art. *Digital Investigation, 11*(1), 34-43. https://doi.org/10.1016/j.diin.2014.08.003

Narasimhan, P., & Kala, N. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(6), 2438-2450.

Park, J., et al. (2020). Blockchain-based evidence verification system for distributed forensic environments. *Journal of Forensic Sciences, 65*(4), 1023-1034.

Rogers, M. K., Goldman, J., Seth, A., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law, 1*(2), 1-20.

Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2017). Digital chain of custody. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(7), 16-19.

Saberi, S., Kouhizadeh, M., & Moulaert, F. (2019). Blockchain technology: A panacea or pariah for managing supply chain operations? A critical review. *International Journal of Production Research, 57*(7), 2179-2195. https://doi.org/10.1080/00207543.2018.1533261

Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2017). Digital chain of custody. *IJARCSSE, 7*(7), 16-19.

Wang, Y., et al. (2020). A survey of the application of blockchain in supply chain management: A review of frameworks, techniques and practices. *IEEE Access, 8*, 169956-169985. https://doi.org/10.1109/ACCESS.2020.302891

Xia, Q., et al. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Journal of Biomedical and Health Informatics, 21*(6), 1966-1975. https://doi.org/10.1109/JBHI.2017.2716847

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy Workshops* (pp. 180-184). https://doi.org/10.1109/SPW.2015.27

"Protecting digital evidence integrity and preserving chain of custody." (2018). *Journal of Digital Forensics, Security & Law, 12*(2).