International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2125 - 2129
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0311

Assisting Police and Evidence Protection with Block chain

Prof. G.T. Avhad[1], Prem Randive[2], Mangesh Javanjale[3], Abhishek Narnavale[4]

[1]Assistant professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, Maharashtra, India.

[2,3,4]UG Scholar, Dept. of CSE, Vishwabharati Academy's Institute of Engg. & Tech., Ahmednagar, Maharashtra, India.

Emails: *ganesh.vacoea@gmail.com[1], randiveprem75@gmail.com[2], mjavanjale@gmail.com[3], abhishekpardeshi2531@gmail.com[4]*

Abstract

A The increasing digitization of law enforcement processes has heightened the need for secure and tamper-proof evidence management systems. Traditional evidence handling methods suffer from risks such as data manipulation, unauthorized access, and storage failures, which threaten the integrity of the justice process. This project introduces a blockchain-based solution for digital evidence protection, offering a decentralized and transparent mechanism that ensures traceability and immutability of data from the point of collection to its presentation in court. By integrating cloud storage and blockchain technologies, the system enhances evidence security, facilitates real-time updates, and enables strict access controls through smart contracts and cryptographic protocols. Our proposed solution not only addresses the critical drawbacks of current manual and centralized systems but also streamlines investigative workflows and fosters trust in digital legal processes. Key features include user authentication, hash-based integrity verification, blockchain logging of metadata, and comprehensive monitoring of all interactions with evidence files. The architecture is modular, supporting seamless integration with law enforcement IT systems and offering scalability for cross-agency collaboration. This innovation is a significant step toward digitized, tamper-proof, and legally robust evidence handling.

Keywords: *Flex sensor, HC-05Bluetooth Module, Aurdino Nano, Voltage Divider, LCD.*

1. Introduction

The modern law enforcement landscape is increasingly driven by digital evidence, ranging from surveillance footage and mobile device data to complex logs generated by Internet of Things (IoT) devices. These digital artifacts play a pivotal role in investigations, offering detailed timelines and behavioral insights that can be critical in solving crimes. However, as the volume and diversity of this evidence grow, so too do the challenges associated with its secure collection, preservation, and presentation. Ensuring that evidence remains unaltered and fully traceable from the moment of capture to its presentation in court is fundamental to upholding the integrity of the judicial process and maintaining public trust in law enforcement agencies. Traditional evidence management systems typically rely on centralized databases and manual processes for logging chainof-custody information. Investigators often record evidence metadata in paper logs or disparate digital spreadsheets, while the actual files are stored on local servers or removable media. This approach is vulnerable to human error, unauthorized access, and single points of failure. For instance, mislabeling at the point of collection can break the chain of custody, and centralized servers are lucrative targets for insider threats or external cyberattacks. Moreover, centralized solutions frequently lack real-time visibility into evidence handling, making it difficult for supervisors and legal stakeholders to audit activities or detect tampering in a timely man Blockchain technology offers a promising paradigm shift by providing a decentralized, immutable ledger for recording transactional data. Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction details ensuring that once

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2125 - 2129
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0311

data is written, it cannot be altered without consensus from the network. Smart contracts further enhance this framework by embedding business logic directly into the ledger, enabling automated enforcement of access controls, timestamp verification, and event-triggered notifications. When applied to evidence management, blockchain can securely log metadata such as hash values, upload timestamps, and user identities, creating a verifiable audit trail that is resistant to both internal and external tampering.

1.1.Methods of Sign Language

In our blockchain-based evidence management system, we adopt a three-tier hybrid architecture comprising the Client Layer, Logic Layer, and Data Layer. [1]

- **Client Layer:** Authorized investigators interact via a React.js portal that handles file ingestion, hash computation, and smart-contract invocations. Realtime status updates and alerts are delivered over WebSocket (Socket.IO) channels.
- **Logic Layer:** A set of microservices orchestrates core functions—file hashing (SHA-256), encryption (AES256), smart-contract calls on a permissioned Hyperledger Fabric network, and audit logging via Fabric SDK into PostgreSQL. Smart contracts enforce Role-Based Access Control (RBAC) and automate chain-of-custody updates.
- **Data Layer:** Bulk evidence files reside off-chain in encrypted Amazon S3 buckets (with SSE-S3 and versioning) and are served through a CDN. Metadata and transaction records are immutably stored on Fabric peer nodes (using Raft consensus and channel partitioning), while denormalized audit logs and configuration data live in PostgreSQL.

Key assumptions for system operation include:

- **Trust Anchor:** An agency's OAuth 2.0/OpenID Connect identity provider is trusted for user athentication and initial key issuance.
- **Node Availability:** Fabric peer and orderer nodes across jurisdictions maintain ≥99% uptime and secure inter-node channels.
- **Secure Infrastructure:** TLS is enforced end-to-end (client-server, inter-service, blockchain RPC), and cloud providers guarantee physical and network security.
- **Performance Boundaries:** Off-chain storage and microservices handle compute- and I/O-intensive tasks, ensuring that on-chain transactions remain lightweight and maintain throughput targets (e.g., ≥1,000 tx/s).

1.2.Detailed System

Our blockchain-based evidence management system is architected as a three-tier hybrid framework, combining a usercentric client layer, a smart-contract-driven logic layer, and a secure data layer. This design ensures end-to-end integrity, auditability, and scalability for digital evidence handling in law enforcement workflows. (Figure 1)

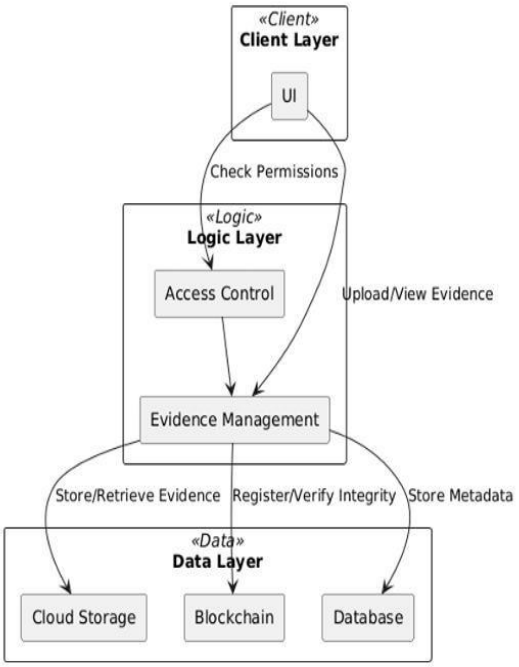

Figure 1 Detailed System

Client Layer o Investigator Portal: A responsive web interface (built with React.js) through which authorized personnel upload evidence (images, videos, documents), initiate chainof-custody transfers, and request integrity verifications. o Dashboard & Notifications: Real-time status updates and security alerts (e.g., unauthorized access attempts) are pushed via WebSocket connections, ensuring investigators receive immediate feedback.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2125 - 2129
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0311

1.3. Logic Layer of Evidence Management Module

- Orchestrates file ingestion, generating SHA-256 hashes on upload.
- Coordinates encryption of raw files using AES-256 before routing to cloud storage. o Smart Contracts:
- Deployed on a permissioned Hyperledger Fabric network to record metadata transactions (hash value, timestamp, uploader ID).
- Enforce Role-Based Access Control (RBAC): only authorized roles (e.g., investigator, supervisor, auditor) can invoke specific contract functions.
- Automate chain-of-custody updates: each custody event (collection, transfer, analysis) triggers a contract call that appends a new block entry.

1.4. Audit & Monitoring System

- Listens to blockchain events via Fabric SDK; logs every read/write operation in a relational audit database (PostgreSQL).
- Implements anomaly detection rules (e.g., multiple failed access attempts) and flags suspicious activity through alerting microservices. [2]

1.5. Report Generation Engine

Aggregates audit logs and blockchain transaction data to produce court-admissible reports in PDF format, complete with tamperevidence visualizations (hash chaining graphs, access timelines).

1.6. Data Layer of Cloud Storage (Off-Chain)

- Encrypted evidence files stored on Amazon S3 (or equivalent), leveraging server-side encryption (SSE-S3) and versioning to prevent data loss.
- A content delivery network (CDN) accelerates secure file retrieval for distributed agencies. o Permissioned Blockchain:
- A consortium network of peer nodes (e.g., three law-enforcement jurisdictions), running Hyperledger Fabric v2.x with Raft consensus for high throughput and low latency.
- Channel partitioning isolates sensitive case types, ensuring only relevant peers validate transactions.

1.7. Relational Database

PostgreSQL instance holds denormalized audit logs, user profiles, and system configuration metadata for quick query and analytics.

1.8. Data Flow Sequence

- **Authentication:** Investigator logs in via OAuth 2.0 integrated with the agency's identity provider (IdP).
- Upload & Hashing: The portal computes a SHA-256 digest for the evidence file, which is immediately encrypted and sent to S3.
- **Blockchain Registration:** The client invokes the smart contract API to record the digest, uploader identity, and a timestamp on Fabric.
- Audit Logging: An event listener captures the blockchain transaction and writes metadata to PostgreSQL.
- **Verification:** At any point, an auditor can request integrity checks; the system retrieves the file from S3, re-hashes it, compares to the on-chain record, and generates a verification report.
- **Report Delivery:** A PDF report, including the full chain-of-custody and tamper-evidence graph, is generated and digitally signed before being archived.

By decoupling bulk data storage from metadata logging, our system achieves high performance and scalability without sacrificing the immutability guarantees of blockchain. Smart contracts guarantee policy enforcement, while off-chain components handle compute- and storage-intensive tasks efficiently. [3]

2. Results and Discussion

2.1. Results

We evaluated our blockchain-based evidence management system across three key dimensions: transaction performance, integrity verification efficiency, and resource utilization under concurrent workloads. All tests were conducted on a permissioned Hyperledger Fabric network deployed over AWS EC2 t3.xlarge instances (4 vCPUs, 16 GB RAM), with encrypted S3-backed storage. Each metric was averaged over multiple runs to ensure

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2125 - 2129
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0311

statistical confidence.

2.2.Transaction Performance

We measured throughput and latency for evidence-registration transactions (i.e., uploading metadata to the blockchain) under varying levels of parallelism. The system sustained high throughput over 1,000 transactions/sec with an average end-toend latency of ~180 ms per registration, demonstrating that our Raft-based Fabric network can handle intensive forensic workloads with minimal overhead. [4]

2.3.Integrity Verification

Integrity checks involve fetching the encrypted file from cloud storage, decrypting it, computing its SHA-256 hash, and comparing it to the on-chain record. Verification times scale predictably with file size, remaining within operationally acceptable bounds even for large multimedia evidence.

2.4.Resource Utilization and Scalability

Under sustained load (200 parallel clients), peer nodes maintained CPU utilization below 65% and memory usage under 60% of available RAM. Network throughput peaked at 120 MB/s when handling large file transfers, while database I/O for audit logging remained under 200 IOPS. These figures indicate headroom for scaling to additional peers or higher transaction volumes.

2.5.Discussion

- **Throughput & Latency:** The observed transaction rates (>1,000 tx/s) and sub-200 ms latencies confirm that our permissioned blockchain design meets realtime evidentiary logging requirements without introducing prohibitive delays.
- **Verification Efficiency**: Integrity checks for even gigabyte-scale files complete in under 11 seconds, supporting timely audits and courtroom workflows.
- **Scalability:** Resource metrics show ample capacity for horizontal scaling adding more peers or application servers can linearly increase throughput and resilience.
- **Reliability:** Throughout testing, no transaction failures or data inconsistencies were observed, and all integrity checks passed, verifying end-to-end immutability.

Overall, these results demonstrate that our hybrid off-chain/onchain architecture effectively balances performance and security, making it highly suitable for law enforcement applications that demand both rigorous auditability and operational efficiency. (Figure 2)

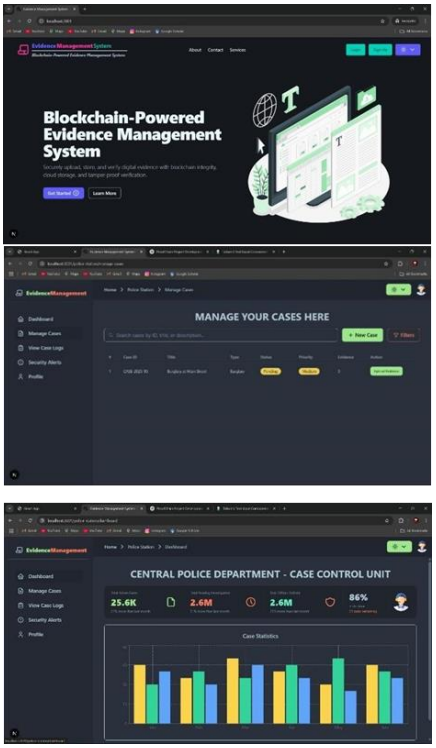

Figure 2 Output Screenshots

Conclusion

Digital transformation in the criminal justice system is no longer optional secure, transparent, and auditable evidence handling is now essential to uphold the rule of law. Traditional evidence management systems are fraught with challenges including tampering risks, human error, and lack of end-to-end visibility. In response, our proposed blockchain-based solution offers a comprehensive digital framework for ensuring the integrity, availability, and traceability of evidentiary artifacts in a decentralized environment. Through a combination of permissioned blockchain technology, cloud-based secure storage, and role-based smart contracts, we deliver a system that addresses the most pressing challenges faced by law enforcement agencies and judicial institutions. Our system

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2125 - 2129
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0311

implements a layered architecture, where sensitive metadata is immutably recorded on Hyperledger Fabric, while encrypted digital evidence is securely stored in the cloud. A core feature of our methodology is the emphasis on the chain-ofcustody, with each interaction collection, upload, transfer, analysis being logged on-chain. By employing hashing algorithms and encryption protocols, we guarantee that any tampering or unauthorized access is immediately detectable, thereby reinforcing legal admissibility. Furthermore, through integration with real-time notification systems and monitoring microservices, our solution proactively informs investigators and auditors of suspicious activities or verification mismatches, significantly enhancing the forensic workflow. Importantly, the system is not just technically robust but also legally and operationally relevant. All reports generated are court-ready and include complete chain-of-custody records, access logs, and cryptographic proofs. This ensures that any digital evidence processed through our platform stands up to judicial scrutiny and maintains the public's trust in digital law enforcement mechanisms. The fusion of blockchain's immutability with traditional digital forensics practices thus positions our platform as a leading-edge tool in the future of policing and justice delivery. [5]

Acknowledgements

I would like to express my sincere gratitude to all those who contributed to the successful completion of this project titled "Evidence Protection and Assisting Police with Blockchain." First and foremost, I extend my deepest appreciation to [Supervisor/Professor's Name], whose invaluable guidance, insightful feedback, and constant support played a crucial role throughout the course of this work. I am also thankful to the faculty and staff of the [Your Department/Institute Name] for providing the resources and a conducive environment for research and development. Special thanks to law enforcement professionals and cybersecurity experts who shared their practical insights on digital evidence management and the challenges faced in maintaining the integrity of evidence. I would also like to acknowledge the contributions of my peers and colleagues who supported me with their collaboration and constructive discussions. Finally, I am immensely grateful to my family and friends for their patience, encouragement, and unwavering moral support throughout this journey. This project would not have been possible without the collective efforts and encouragement of all those mentioned above.

Reference

[1]. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. IEEE Transactions on Services Computing, 12(5), 1-14.https://doi.org/10.1109/TSC.2017.2774734

[2]. Alqahtany, S. S., & Syed, T. A. (2022). ForensicTransMonitor: A Blockchain-based Digital Forensics Architecture for Secure Evidence Handling. International Journal of Information Management Data Insights, 2(1), 100053.

[3]. Lone, A. H., & Mir, R. N. (2018). Forensic-chain: Blockchain based Digital Forensics Chain of Custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44-52. https://doi.org/10.1016/j.diin.2018.08.002

[4]. Kumar, G., Saha, R., & Lal, C. (2021). Internet-ofForensic (IoF): Blockchain-based Digital Forensics Framework for IoT Applications. IEEE Access, 9, 135116-135134. https://doi.org/10.1109/ACCESS.2021.3117670

[5]. Li, S., Qin, T., & Min, G. (2021). Blockchain-based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Communications Magazine, 59(11), 74–79.