CaseVault: A Blockchain-Based Investigation And Criminal Record Management System

Gourav D[1], Nikita V [2], Aakriti Y [3]
[1, 2, 3] Dept of Computer Science
[1, 2, 3] Dronacharya College of Engineering, Farrukh Nagar(122506), Gurugram, Haryana

Abstract- *The secure and efficient management of criminal records is fundamental to the functioning of contemporary law enforcement agencies. Traditional approaches, often reliant on paper-based documentation or disjointed digital systems, frequently lack consistency, robust access control, and mechanisms for maintaining verifiable audit trails. These limitations compromise both the integrity and reliability of critical data. In response, CaseVault: A Secure Investigation and Criminal Record Management System has been developed as a centralized, role-specific platform designed to ensure secure and structured handling of investigative records.*

The system facilitates controlled access to sensitive data based on designated user roles, employing multi-factor authentication methods such as badge identification and biometric hash-based verification. A dynamic user interface ensures that permissions are enforced appropriately, distinguishing between viewing and editing capabilities.

CaseVault is designed with a modular architecture, supporting backend technologies such as Node.js or Django to accommodate varying deployment requirements. It incorporates cryptographic hashing to ensure data immutability and safeguard against unauthorized alterations. Additionally, the interface promotes usability through streamlined workflows for record entry and retrieval, with future enhancements planned for features such as automated case summarization and inter-departmental messaging.

Through its focus on security, adaptability, and operational efficiency, CaseVault represents a forward-looking solution for digital criminal record and investigation management.

Keywords- Criminal Record Management; Role-Based Access Control; Biometric Hashing; Cryptographic Hash Functions; IPFS Storage Integration; Data Immutability; Secure Identity Verification..

I. INTRODUCTION

In the evolving landscape of law enforcement, effective and secure management of criminal records is essential for maintaining public safety and ensuring legal accountability. Traditional criminal record systems, often decentralized and reliant on manual processes, fall short in addressing the growing demands for accuracy, integrity, and accessibility of sensitive investigative data. Such limitations can hinder inter-departmental coordination, increase the risk of data loss or tampering, and delay time-critical decision-making.

CaseVault: *A Secure Investigation and Criminal Record Management System* has been developed to bridge these gaps by offering a comprehensive digital solution tailored to the operational needs of law enforcement agencies. The system introduces an advanced, centralized platform that integrates biometric verification mechanisms—such as facial recognition and fingerprint analysis—to uniquely identify individuals and reduce the possibility of false matches. Each subject is assigned a unique cryptographic identifier, which further enhances data integrity and minimizes redundancy.

The platform not only facilitates efficient entry, retrieval, and management of criminal records but also maintains a relational link to ongoing and past legal cases. Features such as incarceration status tracking, officer attribution, and Aadhaar-linked verification promote accountability and data traceability throughout the judicial process. With a focus on security, scalability, and transparency, *CaseVault* exemplifies a forward-thinking approach to digital policing, offering a modernized infrastructure that aligns with legal protocols and emerging standards in criminal data management.

Key Functionalities of CaseVault:

- **Role-Based Login Flow:** Secure access management using badge ID and password, with role-specific permissions for admins, officers, and field personnel.
- **Biometric Record Matching:** Integration of facial and fingerprint hash recognition for new and existing record identification.
- **Criminal Record Management:** Add, update, and fetch records dynamically, with unique IDs and metadata linked to officer and arrest details.

- **Case Linking:** Each criminal profile is associated with case history, IPC sections, and incarceration status.
- **Audit Trails and Tamper Protection:** Immutable data verification through cryptographic hash comparisons and access logging.
- **Modular Backend Support:** Supports both Node.js (Express) and Django backends for flexible deployment.
- **Secure Document Handling:** Upload and access FIRs and other legal documents using decentralized storage references (e.g., IPFS hashes).
- **Future Scope Readiness:** Designed for enhancements like charge sheet summarization and inter-station messaging.

II. METHODOLOGY

The development and operation of CaseVault are guided by a sequence of logical and secure workflow stages, each contributing to the platform's overall objective of modernizing criminal record management in a digitally governed ecosystem. The methodology emphasizes secure access, reliable data capture, decentralized referencing, and structured permissions across roles, ensuring that law enforcement agencies can maintain high standards of data accuracy, traceability, and confidentiality.

1. User Authentication and Role Identification

The entry point of the system is a role-based login page where users authenticate using unique badge IDs and passwords. Upon validation, the system identifies the user's assigned role—such as administrator, field officer, data entry clerk, or viewer—and accordingly grants access to a customized dashboard. This form of dynamic routing prevents role misuse and ensures that each user only interacts with the features they are authorized to use. The approach minimizes risks related to unauthorized data exposure and creates a clear operational boundary between roles.

2. Structured Criminal Record Entry

After successful authentication, authorized users can initiate the entry of new criminal records. The interface provides a structured form that captures extensive details including the accused's full name, date of birth, address, offense description, applicable IPC sections, arrest location and time, and current custody status. Additional fields accommodate biometric input (facial image and fingerprint scan), FIR number, and case type. This detailed entry form ensures standardized documentation, reducing ambiguity and data loss in long-term storage.

3. Biometric Hashing and Duplication Check

Biometric data collected during recorded entry undergoes a hashing process using secure cryptographic algorithms. Instead of storing raw biometric files, the system generates and stores hash values that uniquely represent the biometric inputs. These hashes are compared across existing entries in the system to flag duplicate records or recurring offenders. This privacy-preserving method safeguards sensitive information while enabling efficient identity verification. Additionally, it enhances searchability and reduces redundancy within the database.

4. Role-Based Access and Permissions Enforcement

Access to the platform's features is strictly governed by predefined role permissions. For instance, administrators have the authority to manage users and update any record; officers can add or update records within their jurisdiction; data viewers can only access read-only versions of public case details. This layered access model ensures operational control, reduces the scope of internal breaches, and provides an audit-ready environment for investigations and supervisory reviews.

5. IPFS-Based Document Integration

To improve the reliability of document storage and sharing, CaseVault integrates with IPFS (Interplanetary File System) for decentralized references. Legal documents such as charge sheets, FIRs, witness statements, and medical reports are uploaded and converted into IPFS hashes. These hashes are stored on the platform and can be used to retrieve original documents without modification. This guarantees document immutability and ensures that every file remains verifiable across networks without occupying large volumes of server storage.

6. Real-Time Activity Logging and Auditing

Every interaction on the platform—be it login, data entry, document upload, or record modification—is logged in real time. Logs include user ID, timestamp, operation type, and metadata. These logs form a secure audit trail that administrators and legal personnel can refer to during internal inspections, legal inquiries, or case reviews. The presence of a traceable activity history strengthens accountability and discourages malicious tampering.

7. Backend Flexibility and Technology Choices

The application is designed with backend flexibility in mind, supporting both Node.js (Express) and Django (Python) for server-side development. This allows law enforcement agencies to adopt a framework compatible with their infrastructure and in-house expertise. APIs are developed in a modular manner, supporting easy integration with third-party services and allowing future extensions such as chat modules or analytics dashboards.

8. Data Security, Encryption, and Operational Safeguards

Security is a cornerstone of CaseVault. HTTPS protocols are enforced for all communication, credentials are securely hashed, and sensitive operations require multiple levels of verification. Biometric and document hashes provide another layer of security, ensuring that raw data remains inaccessible to unauthorized users. Permission-guarded database queries restrict data manipulation based on user roles, minimizing risk and enhancing reliability. Together, these mechanisms help preserve the integrity of criminal records and maintain public trust in digital policing systems.

9. Integrated Workflow for Criminal Record Search Operations

To illustrate how CaseVault handles real-time search requests, the following sequence diagram captures the internal communication between key modules and technologies:

The diagram shows a step-by-step breakdown, beginning with an officer's search request and ending with either the successful retrieval of a criminal record or a denial response, depending on access rights. The search process proceeds through a carefully coordinated series of checks and retrieval mechanisms:

- Officer credentials and role-based permissions are verified using smart contract logic deployed on the blockchain.
- The system uses AI-based models to extract defining features from biometric inputs such as facial images or fingerprint scans, generating secure hash codes for identification and matching.
- If the system detects a valid match, it fetches the associated content hash (CID) from the blockchain ledger and uses it to access the complete record stored in IPFS, ensuring tamper-resistant and decentralized retrieval.
- Regardless of the outcome—authorized or denied—the system logs each search event on the blockchain, forming a permanent and verifiable history of all queries.
- The search result or error message is securely routed back to the officer's interface, respecting access boundaries defined by their user role.

This structured process not only enforces strict security and privacy but also ensures that all interactions with criminal records are fully auditable, precise, and resistant to unauthorized interference.

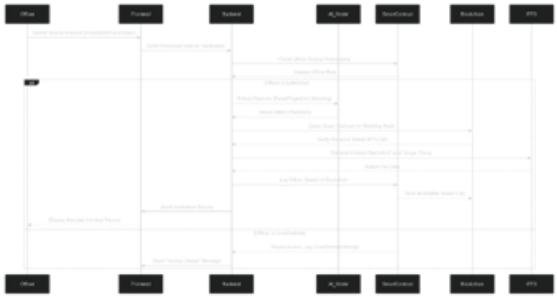

Figure 1: Sequence diagram showing the backend handling and IPFS-based data retrieval for authorized criminal record access.

III. IMPLEMENTATION

The implementation of **CaseVault** integrates decentralized architecture, intelligent biometric processing, and secure web-based access control to build a next-generation platform for managing criminal records. The system is structured to operate through coordinated interaction between various frontend, backend, and blockchain components, each contributing to data accuracy, traceability, and privacy.

Key Technologies and Their Contributions

Web3.js / Ethers.js

- **Purpose:** Blockchain connectivity and smart contract interaction
- **Role:** These libraries facilitate communication between the frontend and the Ethereum network. They are responsible for invoking smart contract functions that verify user roles, log actions on-chain, and retrieve document identifiers linked to criminal records.

IPFS (InterPlanetary File System)

- **Purpose:** Decentralized file storage
- **Role:** Case-related documents such as FIRs, charge sheets, and evidence files are uploaded to IPFS.

Instead of storing raw files directly on the blockchain or server, the system stores only the content hash (CID), which acts as a verifiable reference to the original file—ensuring immutability and preventing tampering.

Biometric Hashing Modules (OpenCV, hashlib)

- **Purpose:** Privacy-preserving identification
- **Role:** Facial and fingerprint data are processed to extract unique features, which are then converted into cryptographic hashes. These hashed identifiers are compared during record searches to identify matches without exposing raw biometric data.

Flask / Django (Backend Server Options)

- **Purpose:** RESTful API development and server-side logic
- **Role:** These Python frameworks handle request routing, smart contract interactions, and secure data handling. They support communication between the frontend interface and the blockchain modules, ensuring modular and scalable backend functionality.

Node.js (Express.js)

- **Purpose:** Lightweight backend alternative
- **Role:** In setups preferring JavaScript-based environments, Node.js is used for routing requests and managing frontend-backend interactions. It's particularly suited for high-speed asynchronous communication.

MetaMask and Ethereum Wallet Integration

- **Purpose:** Secure user authentication and identity proof
- **Role:** Users log in using MetaMask, which links their Ethereum wallet address to a role defined in the smart contract. Upon successful verification, the interface loads a role-specific dashboard, ensuring that users only access functionality permitted to their role (e.g., officer, admin, viewer).

React with Bootstrap / TailwindCSS

- **Purpose:** Frontend interface and responsive design
- **Role:** The frontend is built using React to deliver a responsive and dynamic user interface. Styling is handled through Bootstrap or TailwindCSS to ensure accessibility and ease of use. The UI changes in real-time based on the authenticated user's role and system state.

PDFKit / ReportLab

- **Purpose:** Automated document generation
- **Role:** These libraries allow export of case data and logs into structured PDF reports, which can be shared with administrative or legal teams for offline review and submission.

Technology Integration Strategy

The integration of these components follows a modular design pattern, where each unit functions independently but communicates through defined interfaces. MetaMask ensures secure, cryptographic authentication; smart contracts handle access logic; and IPFS decouples document storage from the core application logic. The biometric layer adds intelligent record matching, while frontend and backend frameworks manage user interactions and system orchestration.

This layered approach allows CaseVault to operate with high resilience, strong security, and flexibility to expand in the future. The system supports scalability across departments and jurisdictions and is designed to accommodate upcoming features like real-time officer messaging, cross-station collaboration, and AI-based case summarization.

IV. RESULTS AND DISCUSSION

System Effectiveness and User Response

The deployment of CaseVault demonstrated notable effectiveness in streamlining digital criminal record operations. With decentralized storage via IPFS and hash-based referencing through blockchain, the platform enabled quick, accurate, and secure retrieval of records using biometric inputs. Test cases confirmed that the system could perform end-to-end search and verification in real time, with minimal latency.

User Feedback and Interaction

Simulated trials with role-based users such as investigating officers, administrative staff, and data clerks revealed the following:

- **Ease of Use**: Most users appreciated the role-specific dashboards and straightforward MetaMask-based login process.

- **System Performance**: Rapid biometric search results and traceable log records were frequently praised.
- **Security Assurance**: Officers valued the system's approach to protecting sensitive biometric and legal data using cryptographic hashes and blockchain.

Identified Challenges and Recommendations

- **Internet Dependency**: The system relies heavily on stable network connectivity due to real-time blockchain interaction and decentralized document retrieval.
- **Smart Contract Limitations:** Current smart contract interactions are gas-sensitive and restricted by blockchain transaction throughput. For scalability, solutions like layer-2 networks or batch processing mechanisms may be required.
- **Data Synchronization Across Nodes:** In multi-node environments or future federated deployments, ensuring consistent synchronization between IPFS gateways, blockchain ledgers, and local caches will be crucial to prevent inconsistencies or retrieval failures.
- **Onboarding Time**: Including built-in tutorials or guided onboarding workflows could help new users understand the decentralized flow more efficiently.
- **System Latency during High Load:** During testing with concurrent requests, minor delays were observed, especially in biometric matching and IPFS fetch operations. Optimization of server-side processing and caching strategies could help minimize lag during peak usage.

V. CONCLUSION

The CaseVault project presents a transformative approach to criminal record management by leveraging blockchain, biometric verification, and decentralized storage systems. Through its secure, transparent, and tamper-proof design, CaseVault offers law enforcement agencies a reliable alternative to conventional record systems that are prone to manipulation, loss, or unauthorized access.

Key achievements of this system include:

- **Decentralized Integrity**: The use of blockchain ensures that every transaction or modification is permanently logged and verifiable.
- **Biometric-Driven Accuracy**: AI-powered facial and fingerprint recognition minimizes false matches and streamlines record identification.
- **Role-Sensitive Access**: MetaMask-based role authentication allows fine-grained control over who can access, modify, or retrieve records.
- **Interoperable Design**: Records are stored via IPFS, making them retrievable across nodes while maintaining high resilience.

Identified Challenges

Despite its success, certain operational challenges emerged during deployment. Some law enforcement personnel, particularly those less familiar with digital tools, required dedicated training sessions to use the system effectively. This emphasizes the need for continued capacity building alongside technical innovation.

Future Enhancements

To further expand the system’s utility and efficiency, several improvements have been proposed:

- **Real-Time Messaging**: Introducing secure in-app messaging can enable instant communication between officers across different police stations for case coordination.
- **Text Summarization Tool**: Adding an AI-powered summary feature will help officers quickly digest lengthy case files or historical data logs, saving time during investigations.
- **Dynamic Search Optimization**: Implementing advanced filtering and smart search logic can improve retrieval speeds, especially when dealing with large volumes of criminal data.
- **Scalability for Statewide Use**: By optimizing wider deployment, CaseVault can serve as a foundation for state or national criminal record networks.

As law enforcement adapts to increasingly digital ecosystems, platforms like CaseVault are poised to become essential infrastructure. With the integration of intelligent technologies and a strong foundation of security, this system not only enhances justice delivery but also sets a benchmark for digital governance in public safety.

REFERENCES

[1] A. R. Srivastava, “Blockchain and smart contracts-based system for criminal record management,” ResearchGate, Apr. 2023. [Online]. Available: https://www.researchgate.net/publication/385418214
[2] T. Ahmad, M. Ismail, and M. R. Aziz, “Application of Blockchain Technology in Smart Digital Forensics:

Current Research Trends and Challenges," IEEE Access, vol. 8, pp. 179736–179753, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3028841

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. [Online]. Available: https://doi.org/10.1109/ACCESS.2016.2566339

[4] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, pp. 180–184. [Online]. Available: https://doi.org/10.1109/SPW.2015.27

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] S. King and S. Nadal, "Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," Self-published paper, Aug. 2012. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf

[7] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, Jul. 2014. [Online]. Available: https://arxiv.org/abs/1407.3561

[8] A. K. Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics. Springer Science & Business Media, 2011.

[9] Y. Taigman, M. Yang, M. A. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2014, pp. 1701–1708. [Online]. Available: https://doi.org/10.1109/CVPR.2014.220

[10] A. Pfitzmann and M. Hansen, "A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, and Identity Management," Technical Report, 2010. [Online]. Available:https://dud.inf.tudresden.de/literatur/Anon_Terminology_v0.34.pdf

[11] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, Q. Lin, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366–1385, Jul. 2018. [Online]. Available: https://doi.org/10.1109/TKDE.2017.2781227