IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

Safeguarding Crime Digital Evidence Using SHA Hash and AWS

Devaraju H K[1], Sufiya Salam[2], Hajeera Suhani [3], Mohammed Abid I S[4], Mohammed Ibrahim Khan[5]

Assistant Professor, Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India[1]

Undergraduate Student, Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India[2-5]

Abstract: Crime is an illegal activity that is punished by the government, evidence is required to prove the crime. The evidence gained from a crime place is crucial because it serves as proof of the offense. The digitization of evidence is an urgent necessity. In the digital era, the management and integrity of crime evidence present substantial challenges due to risks of tampering and loss of data integrity. Throughout the investigation process, and the integrity of sensitive data must be maintained as it passes through the various levels of intermediaries that form the Chain of Evidence (CoE).

The evidence needs to be tamper-proof and protected against any alterations. To build robust systems with immutability, integrity, and legitimacy, SHA & AWS S3 is superior. Using SHA & AWS S3 service, digital evidence can be transferred between parties without a central authority in a transparent manner. We focused on how SHA algorithm & AWS S3 based solutions can help in building a strong secure system. The system is implemented using SHA algorithm platform to achieve integrity, immutability transparency as well as tampering can be identified.

Keywords: **:** Digital Evidence, SHA algorithm, AWS S3, Chain of Evidence, Integrity check

I. INTRODUCTION

In today's digital landscape, the prevalence of cybercrimes and technology-assisted offenses has underscored the critical importance of managing digital evidence with precision and security. Digital artifacts such as CCTV footage, audio recordings, forensic reports, and communication logs play a vital role in modern investigations and judicial proceedings. However, their admissibility in court hinges on maintaining data integrity, authenticity, and a verifiable Chain of Custody (CoC) throughout their lifecycle.

Traditional evidence management systems—largely based on centralized storage and manual logging—are prone to tampering, unauthorized access, and data loss, thereby compromising the credibility of legal investigations.

The project titled "Safe Guard Crime Digital Evidence with SHA Hash & AWS S3" aims to overcome these limitations by introducing a secure, scalable, and traceable digital evidence management system.

The architecture integrates SHA-256 cryptographic hashing for verifying data integrity, Amazon Web Services (AWS) S3 for encrypted and redundant cloud storage, and XML-based structured logging for standardized metadata management. This ensures that each piece of evidence—be it collected from the crime scene, forensic laboratory, or field investigations—is securely stored, hashed for immutability, and accessible only to authorized users through role-based access control.

In this system, Police Stations initiate the evidence upload process, FSL staff conduct forensic analysis and submit reports, and Court Judges verify evidence authenticity using stored hash values. An integrated MySQL database maintains user credentials, access logs, and case metadata, supporting full traceability and accountability across all interactions. The use of AWS S3's object-locking and versioning features further ensures evidence cannot be altered or deleted post-upload.

By automating evidence handling, enforcing cryptographic verification, and utilizing cloud infrastructure, the proposed system enhances transparency, security, and operational efficiency. It addresses key gaps in existing solutions and offers a legally robust framework for managing digital evidence across investigative and judicial domains. This paper presents a detailed view of the current limitations, the proposed system design, and its potential to revolutionize digital forensics and case integrity in the criminal justice system.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

II. LITERATURE REVIEW

Several recent studies have explored the integration of blockchain technology into digital evidence management, aiming to improve transparency, security, and integrity in forensic investigations.

In [1], Krishna et al. present a comprehensive survey on the application of blockchain in digital evidence handling. The authors examine how consensus mechanisms, smart contracts, and decentralized platforms contribute to the reliability and immutability of digital records. However, they also identify significant challenges such as scalability, privacy, and legal concerns, which must be addressed before blockchain can be fully adopted in legal contexts.

Namitha et al. in [2] propose a dual-layer blockchain model combining public and private blockchains to enhance digital evidence security. The public layer ensures transparency through metadata logging, while the private layer provides restricted access using asymmetric cryptography. Although effective in theory, the model highlights the complexities of integrating such systems with law enforcement and the need for proper key management across stakeholders.

A hybrid approach involving blockchain and the InterPlanetary File System (IPFS) is explored in [3] by Hussain et al. Their "Evidence Vault" model enhances data availability and fault tolerance while ensuring tamper-proof storage. Despite its potential, the paper notes that the model lacks end-to-end coverage of the evidence lifecycle, particularly from crime scene acquisition to court presentation.

In [4], Patil et al. focus on improving forensic evidence security using blockchain. They detail how each transition in the evidence handling chain—from crime scene to courtroom—can be recorded immutably. The study emphasizes transparency and accountability but is limited by its focus on physical forensic evidence, without addressing digital data types such as video or image files.

Finally, Turukmane et al. in [5] propose a blockchain-based forensic evidence management system built on the Ethereum platform. Their system includes evidence addition, retrieval, and user access controls with digital signature verification. While ensuring integrity and non-repudiation, the implementation lacks integration with broader justice system workflows and omits validation techniques for digital media like CCTV footage.

III. EXISTING SYSTEM

In most traditional setups, the management of digital crime evidence is handled through centralized databases or local digital storage systems maintained by individual law enforcement agencies. While these systems provide a basic infrastructure for storing and retrieving evidence files, they come with significant limitations in terms of security, transparency, and integrity. Centralized repositories create a single point of failure—meaning that if the system is compromised, all evidence stored within it is at risk of being altered, deleted, or accessed by unauthorized parties. Additionally, such systems often lack detailed, tamper-evident audit trails, making it difficult to track changes or verify who accessed the data and when. This is particularly problematic in maintaining the Chain of Evidence (CoE), a legal requirement that ensures the reliability of evidence presented in court. The absence of immutable logging and real-time verification mechanisms compromises the trustworthiness of the evidence. Moreover, digital files passing through multiple intermediaries such as police officers, forensic analysts, and legal personnel can be exposed to errors, inconsistencies, or intentional manipulation. Limited interoperability among departments and insufficient access controls further complicate the secure management of evidence. These issues collectively undermine the evidentiary value, weaken legal admissibility, and reduce operational efficiency in criminal investigations.

IV. PROPOSED SYSTEM

To address these deficiencies, the proposed system introduces a modern, cloud-enabled architecture that leverages SHA-256 cryptographic hashing and secure object storage through Amazon Web Services (AWS) S3. Each digital evidence file is uniquely identified using a SHA-256 hash, which serves as a digital fingerprint to verify its integrity. This hash, along with detailed metadata—such as the police station involved, date and location of collection, and descriptive attributes—is encapsulated in an XML format for standardized storage. These XML files are then securely uploaded to AWS S3, a robust and highly available cloud storage platform that offers built-in data versioning and encryption capabilities. The system employs strict role-based access control, ensuring that only authorized personnel—such as Police Station staff, Forensic Science Laboratory (FSL) analysts, and Court Judges—can access specific functionalities based on their roles. Any operation performed within the system, whether uploading, downloading, or verifying evidence, is automatically logged with a timestamp to maintain a

transparent audit trail. This not only enhances accountability but also provides strong legal proof of evidence integrity. In addition, the use of cloud infrastructure enables scalability, remote access, and disaster recovery features that traditional systems lack. By integrating cryptographic verification with cloud storage and role-based workflow

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

automation, the proposed system ensures that digital crime evidence remains secure, traceable, and tamper-proof throughout its lifecycle. This approach significantly strengthens the credibility and efficiency of criminal investigations and judicial proceedings.

V. SYSTEM REQUIREMENTS

To support the smooth development and execution of the proposed application, both hardware and software requirements must be met. On the hardware side, the system should have at least an Intel Core i3 processor or higher with **a** minimum clock speed of 1.2 GHz to ensure responsive performance. A minimum of 8 GB RAM is recommended to handle simultaneous tasks such as running the development environment, web server, and database. Additionally**,** 512 GB of available hard disk space is needed to store the operating system, development tools, project files, and backups.
On the software side, the system should run Windows 10 or later for compatibility with development tools and updates. The application is developed using Visual Studio 2010 as the IDE, with C# as the programming language and ASP.NET 4.0 as the web development framework. For backend storage, MySQL Server is used to manage digital evidence, user data, and access logs with reliable querying and data integrity features. This setup ensures a stable environment for secure and efficient application development.

VI. SYSTEM ARCHITECTURE

The proposed system, titled *"Safe Guard Crime Digital Evidence with SHA Hash & AWS S3,"* presents a comprehensive and secure architecture for digital crime evidence management by integrating multiple components including forensic laboratories, police stations, judicial systems, cloud infrastructure (AWS S3), and a relational database (MySQL Server). The system leverages cryptographic hashing through SHA-256, along with XML-based structured data storage, to ensure the authenticity, traceability, and confidentiality of evidence throughout its lifecycle. This approach is designed to protect sensitive data against tampering, unauthorized access, and accidental loss while providing a transparent and accountable workflow for all stakeholders involved.

Each stakeholder in the digital evidence ecosystem performs a critical and role-specific function. The Police Station serves as the first point of contact by registering crime cases, collecting digital evidence (e.g., CCTV footage, pen drive files), generating corresponding XML entries, and uploading them to AWS S3 after applying SHA-256 hashing. These hashes act as digital fingerprints, ensuring that any future modifications to the files can be detected with ease.

The Forensic Science Laboratory (FSL) Staff retrieves the uploaded evidence, performs forensic analysis (such as DNA testing, fingerprint analysis, and audio/video validation), and generates encrypted reports in XML or PDF format. These files are also hashed and uploaded to the cloud, accompanied by metadata such as timestamps and handover logs that support traceability and legal admissibility.

The Court Judge is authorized to access the case files, evidence metadata, and forensic reports stored in AWS S3. Using the stored hash values, the judge can independently verify the integrity of each document and ensure that the Chain of Custody (CoC) has not been compromised at any stage. This guarantees a tamper-evident trail from collection to trial. Additionally, the Application Manager acts as the administrator of the system, responsible for backend configuration tasks such as adding cities, courts, police stations, and mapping user roles. This role ensures system-wide consistency, data integrity, and secure access control across all modules.

The system is backed by a MySQL Server, which manages metadata related to user credentials, login activity, evidence mappings, investigation logs, and transaction history. This data provides comprehensive auditability and serves as a reference layer for the integrity verification of evidence stored in AWS S3. The integration of Amazon S3 cloud storage ensures highly available, scalable, and geographically redundant storage of digital files, enhancing disaster recovery capabilities and remote accessibility.

This architecture not only enforces strong data protection through SHA hashing and encryption but also promotes transparency through structured logging and traceability. The combined use of cloud infrastructure, relational databases, and role-based access mechanisms ensures that digital evidence is tamper-proof, audit-ready, and available only to authenticated personnel throughout its journey from collection to courtroom deliberation. This system addresses critical pain points in conventional evidence management workflows and offers a future-ready platform aligned with digital forensics best practices.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

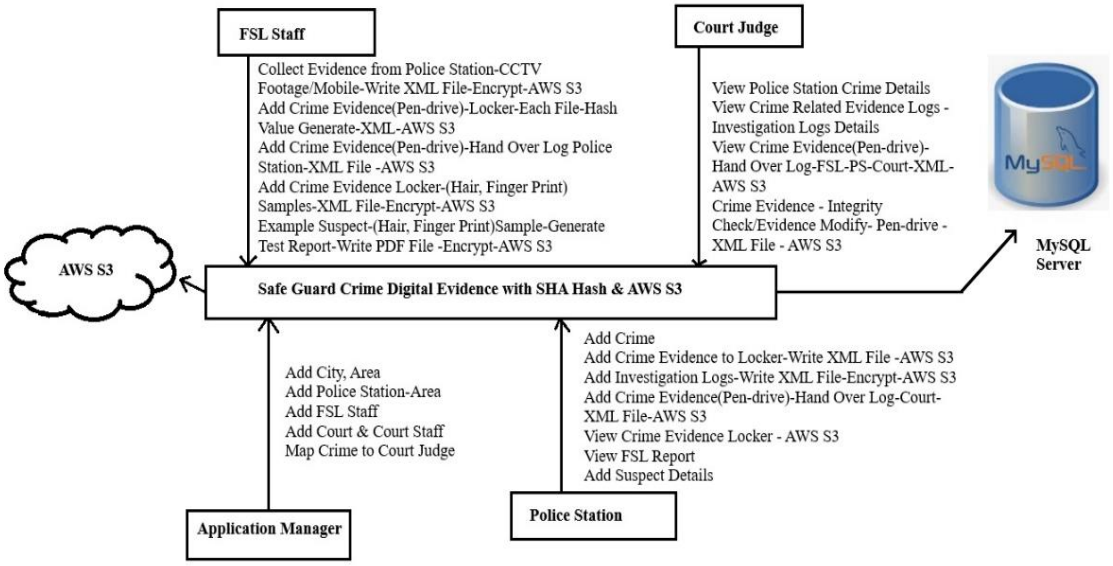

Fig.1 System Architecture of Safe Guard Crime Digital Evidence with SHA Hash and AWS S3
The diagram outlines interactions among FSL staff, court judges, police stations, and application managers, with centralized storage on AWS S3 and metadata handling via a MySQL server. Digital evidence is stored, hashed, and tracked using XML files and cryptographic encryption to ensure integrity and accountability

VII. PROPOSED SYSTEM FLOW

The proposed system for safeguarding digital crime evidence incorporates a role-based control flow mechanism, as illustrated in Fig. 2. The workflow initiates with the user accessing the system through a secure login interface. Upon initiation, the system requires the user to authenticate using pre-assigned credentials. This step is essential to ensure that only authorized personnel can proceed further into the system. If the authentication process is successful, the system then transitions to verifying the user's designated role within the platform. If the user fails authentication, the system re-initiates the login and verification process to prevent unauthorized access.

The role verification process is critical, as it determines the functionalities accessible to the authenticated user. The system is structured to support multiple user categories, each corresponding to specific responsibilities in the crime evidence handling lifecycle. These roles include:

Administrator: Responsible for configuring the foundational elements of the platform, such as adding jurisdictional information including cities and their associated police stations. The administrator also manages user accounts for various roles such as FSL staff, police personnel, and judicial officers.

Police Station Personnel: Authorized to register new crime cases and associate relevant information such as suspects, crime locations, and initial investigation logs. Police personnel are also involved in handing over digital evidence to forensic teams and tracking the movement of such evidence through the system.

Forensic Science Laboratory (FSL) Staff: Tasked with collecting, verifying, and uploading digital crime evidence. This may include CCTV footage, mobile data, physical samples such as hair or fingerprints, and reports generated from forensic tests. The FSL staff ensure that all files are securely converted to XML format, hashed using SHA algorithms, encrypted, and stored in the AWS S3 cloud environment to preserve integrity and traceability.

Court Judge: Granted access to view complete crime investigation logs, review evidence handover records, and verify the integrity of digital evidence using hash values and digital signatures. Judges can also assess whether any tampering has occurred by comparing stored logs and SHA hashes.

Each user's path through the system is determined by their role, ensuring strict segregation of duties and minimizing the risk of unauthorized actions. This modular and secure workflow culminates in the system executing the designated function—be it data addition, evidence registration, or integrity verification—based on the role-defined privileges. Once the required action is performed, the system gracefully concludes the process, ensuring all interactions are securely logged and monitored for transparency and auditability.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

This control flow model plays a pivotal role in maintaining the confidentiality, integrity, and availability (CIA) of digital evidence. It ensures that the chain of custody remains transparent and tamper-proof by integrating strong authentication, encrypted storage, and role-based access control, thereby supporting secure legal proceedings and forensic validations.

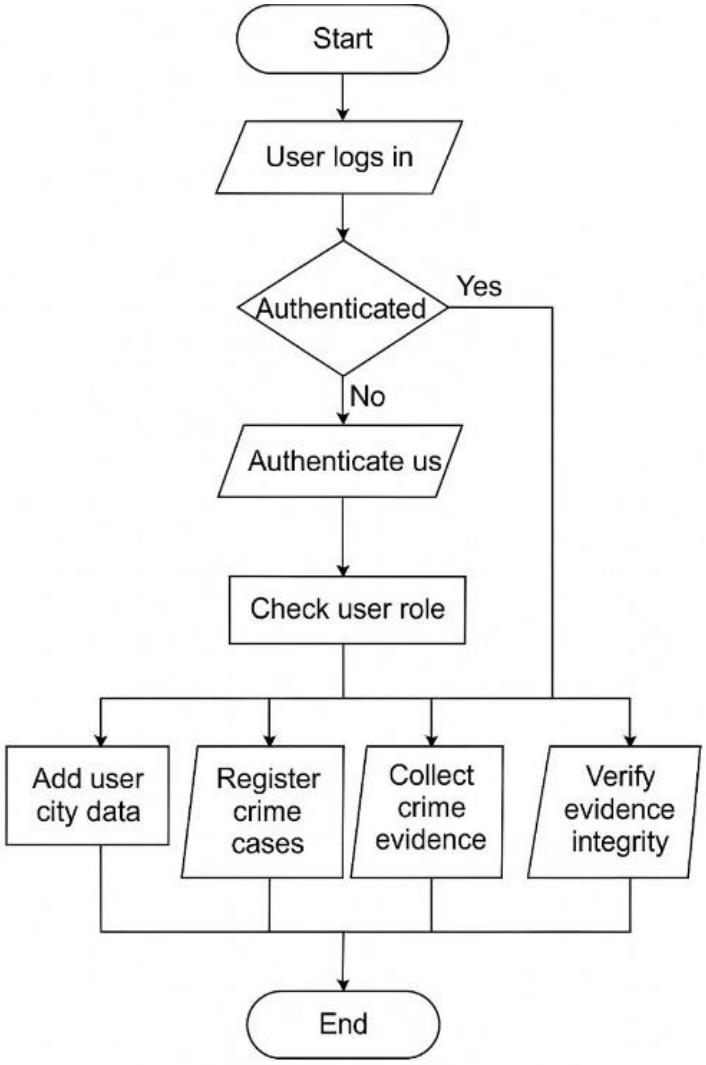

Fig.2**:** Role-Based Control Flow for User Authentication and Digital Evidence Management

This flowchart illustrates the sequential steps involved in authenticating users and assigning role-based permissions within the proposed digital crime evidence safeguarding system. It begins with a secure login process, followed by authentication and role verification. Depending on the authenticated user's role—whether Administrator, Police Station Personnel, FSL (Forensic Science Laboratory) Staff, or Court Judge—the system grants access to specific functionalities. Administrators can manage geographical data and user assignments, police officers can register crime cases and manage investigation logs, FSL staff are responsible for collecting and uploading encrypted evidence, and judges can verify evidence integrity and monitor judicial processes. This structured flow ensures that every user performs only authorized tasks, thereby enhancing security, traceability, and accountability in digital evidence management.

VIII. RESULTS AND DISCUSSION

The implementation of the project "SAFE GUARD CRIME DIGITAL EVIDENCE WITH SHA HASH & AWS S3" has produced promising and reliable outcomes that directly address the challenges of evidence integrity, security, and accessibility in the digital era. One of the most significant outcomes is the successful integration of the SHA-256 hashing algorithm, which ensures that every digital evidence file has a unique hash value. This allows any unauthorized modification of the file to be easily detected, ensuring the integrity of the evidence throughout its lifecycle. The hash is generated at the time of upload and re-verified during every access or download operation. Another major achievement

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

is the use of Amazon Web Services (AWS) S3 for cloud-based evidence storage. AWS S3 offers high durability, availability, and built-in encryption, making it an ideal platform for securely storing sensitive data. The system benefits from AWS's scalability and reliability, ensuring that digital evidence remains accessible to authorized personnel while being protected from accidental loss or deletion. The project also effectively implements role-based access control (RBAC), assigning different permissions to police officers, FSL staff, judges, and application managers. Each role has specific privileges such as viewing, managing, or verifying evidence. Compared to traditional local file storage systems, which lack tamper detection and access control features, this system greatly improves security and traceability. Furthermore, while blockchain-based systems provide immutability and high security, they often involve significant complexity, slower data handling, and increased costs. In contrast, this system offers a more practical and easily adoptable solution using well established cryptographic methods and cloud infrastructure. Overall, this approach demonstrates an optimal balance between data integrity, cost effectiveness, and ease of implementation. The combination of SHA-256 hashing, secure cloud storage, and structured access control makes this system a highly effective solution for managing digital evidence in legal and forensic environments.

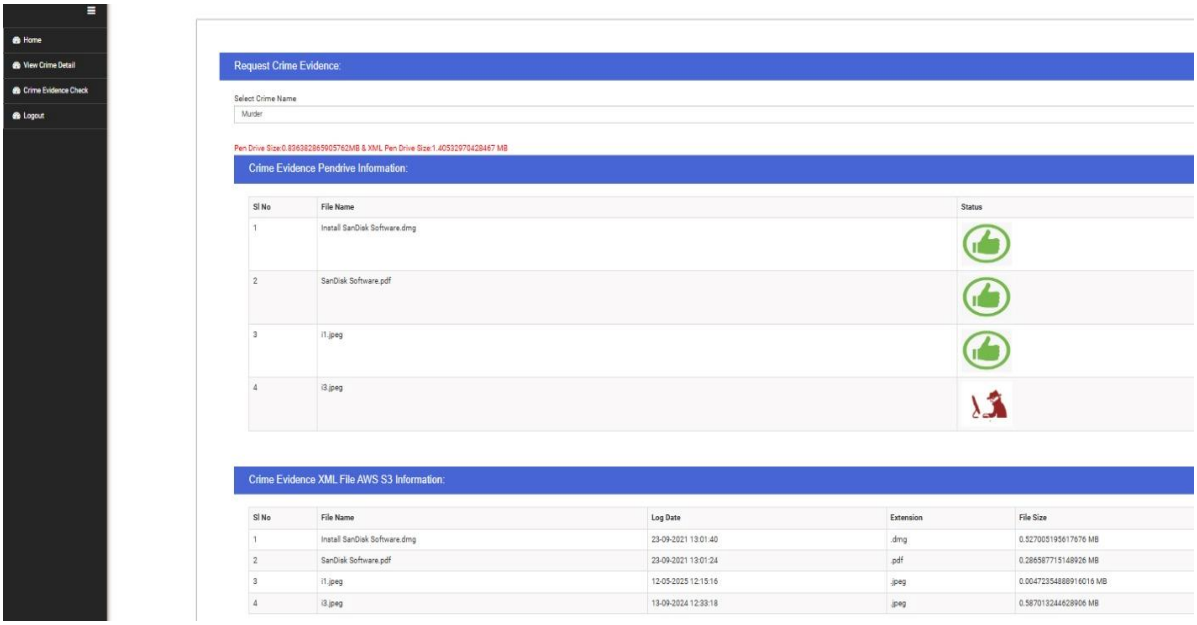

Fig.3: Crime Evidence Integrity Check, shows if the evidence is tampered or not

IX. CONCLUSION

The proposed system ensures a secure, transparent, and accountable digital framework for managing crime-related data and digital evidence across various law enforcement and judicial entities. By integrating cryptographic techniques like SHA-256 hashing and AES encryption, and leveraging AWS S3 for secure cloud storage, the application guarantees data integrity, confidentiality, and non-repudiation. The system automates and streamlines the workflows for crime logging, evidence handling, forensic analysis, and judicial review, thereby reducing the chances of human error, document tampering, and unauthorized access. Role-based access control and traceable evidence transfer logs further enhance the system's trustworthiness, supporting a fair and efficient criminal justice process.

X. FUTURE ENHANCEMENTS

The proposed system lays a strong foundation for secure digital evidence management; however, several enhancements can further improve its functionality, scalability, and usability in real-world criminal justice environments. One of the most promising advancements is the integration of blockchain technology to create an immutable ledger for all evidence-related transactions, significantly improving traceability, auditability, and legal trust. Additionally, the implementation of AI and machine learning algorithms can enable automated analysis of CCTV footage, voice recordings, and forensic samples, thereby assisting investigators with faster and more accurate insights. Integration with a national or inter-state crime database would allow seamless sharing of criminal records across jurisdictions, enabling better coordination between law enforcement agencies.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125361

To strengthen identity verification**,** biometric authentication methods such as fingerprint or iris scans can be used to accurately identify suspects and link them to prior records. Furthermore, a mobile application can be developed for field officers, allowing them to log FIRs and collect digital evidence on-site using secure camera integration and real-time upload to cloud storage. For added security, the system can support two-factor authentication (2FA) using OTPs or biometric verification during login, reducing the risk of unauthorized access. Additionally, real-time alerts and case tracking features can notify key stakeholders—such as police officials, forensic teams, and court personnel—about case updates, pending actions, or missing reports via SMS or email. Lastly, implementing multilingual support in the user interface will ensure broader accessibility and ease of use across different states and linguistic regions, thereby promoting inclusivity and user adoption at scale.

REFERENCES

[1] R. Sathyaprakash et al., "An implementation of blockchain technology in forensic evidence management," in Proc. 2021 Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE), Dubai, UAE, 2021, pp. 110–115, doi: 10.1109/ICCIKE51210.2021.9410737.

[2] J. Jeong, D. Kim, B. Lee and Y. Son, "Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric," J. Inf. Process. Syst., vol. 16, no. 4, pp. 866–876, 2020, doi: 10.3745/JIPS.03.0130.

[3] E. Yunianto, Y. Prayudi and B. Sugiantoro, "B-DEC: Digital evidence cabinet based on blockchain for evidence management," Int. J. Comput. Appl., vol. 181, no. 45, pp. 22–29, 2019, doi: 10.5120/ijca2019918820.

[4] C. Shilpa and A. H. Shanthakumara, "An Implementation of Blockchain Technology in Combination with IPFS for Crime Evidence Management System," in Proc. 2023 Int. Conf. Comput. Commun. Informatics (ICCCI), Coimbatore, India, 2023, pp. 1–6, doi: 10.1109/ICCCI56763.2023.10071289.

[5] A. H. Lone and R. N. Mir, "Forensic-chain: Ethereum blockchain based digital forensics chain of custody," Sci. Pract. Cyber Secur. J., vol. 1, pp. 21–27, 2018.

[6] B. M. Manjre, K. K. Goyal and S. Shivani, "A novel and custom blockchain approach for the integrity assurance of the digital evidences extracted during the extraction and decoding of mobile artifacts from the mobile forensic tools," in AIP Conf. Proc., vol. 2753, no. 1, Apr. 2023, Art. no. 020016, doi: 10.1063/5.0136227.

[7] A. V. Turukmane, "Forecasting the IoT-based cyber threats using the hybrid forage dependent ensemble classifier," Concurrency Computat.: Pract. Exper., vol. 35, no. 2, p. e7460, 2023, doi: 10.1002/cpe.7460.

[8] A. V. Turukmane et al., "Multispectral image analysis for monitoring by IoT based wireless communication using secure locations protocol and classification by deep learning techniques," Optik, vol. 271, p. 170122, 2022, doi: 10.1016/j.ijleo.2022.170122.

[9] A. V. Turukmane et al., "Smart farming using cloud-based IoT data analytics," Measurement: Sensors, vol. 27, p. 100806, 2023, doi: 10.1016/j.measen.2023.100806.

[10] K. P. Chaudhari and A. V. Turukmane, "Dynamic probabilistic packet marking," in Proc. Int. Conf. Adv. Inf. Technol. Mobile Commun., Berlin, Heidelberg: Springer, 2012, pp. 29–36, doi: 10.1007/978-3-642-27317-9_4. Safeguarding Crime Digital Evidence with SHA Hash & AWS Dept of CS&E, MITM 2024-2025 61

[11] Y. M. Roopa et al., "Power allocation model for residential homes using AI-based IoT," Measurement: Sensors, vol. 24, p. 100461, 2022, doi: 10.1016/j.measen.2022.100461.

[12] H. Chougule, S. Dhadiwal, M. Lokhande, R. Naikade and R. Patil, "Digital Evidence Management System for Cybercrime Investigation using Proxy Re Encryption and Blockchain," Procedia Comput. Sci., vol. 215, pp. 71–77, 2022, doi: 10.1016/j.procs.2022.11.009.

[13] J. Hanafi, Y. Prayudi and A. Luthfi, "IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management," Int. J. Comput. Appl., vol. 183, no. 41, pp. 24–32, 2021, doi: 10.5120/ijca2021921811.

[14] D. Kim, S.-Y. Ihm and Y. Son, "Two-level blockchain system for digital crime evidence management," Sensors, vol. 21, no. 9, p. 3051, 2021, doi: 10.3390/s21093051.

[15] S. Rao, S. Fernandes, S. Raorane and S. Syed, "A Novel Approach for Digital Evidence Management Using Blockchain," in Proc. Int. Conf. Recent Adv. Comput. Techn. (IC-RACT), 2020.

