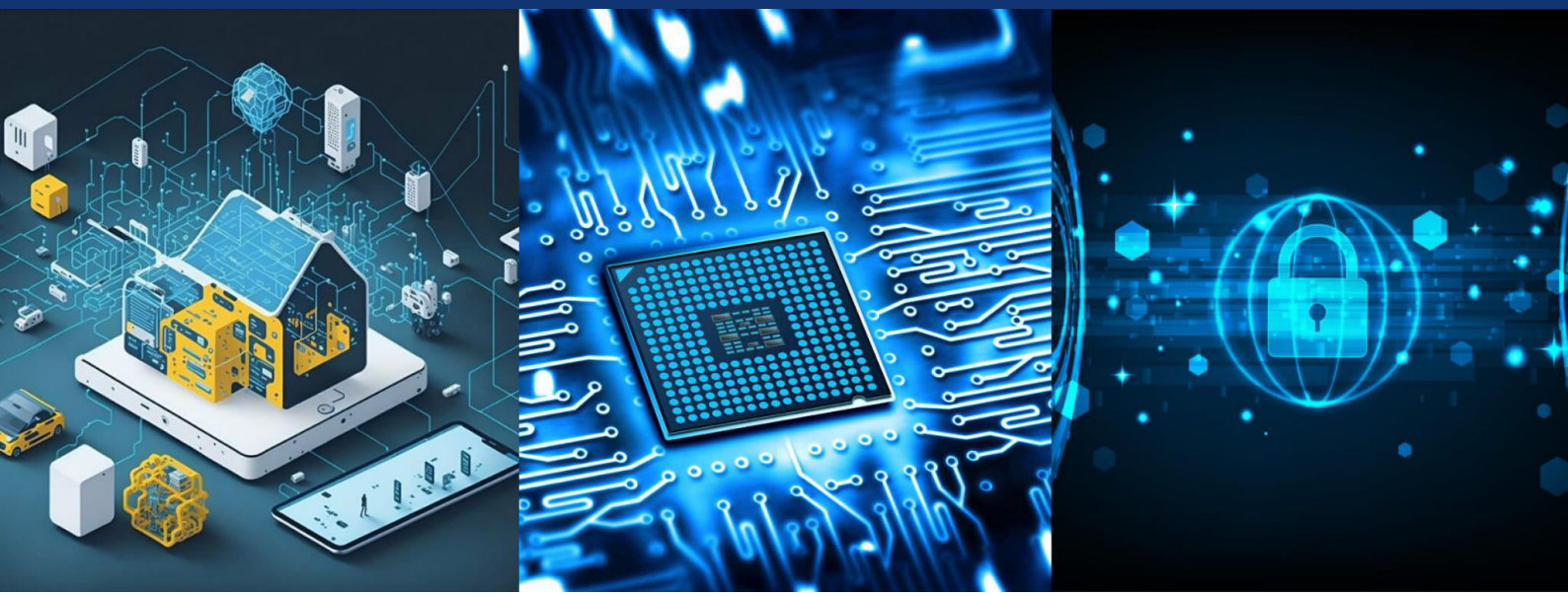
IJIRCCE

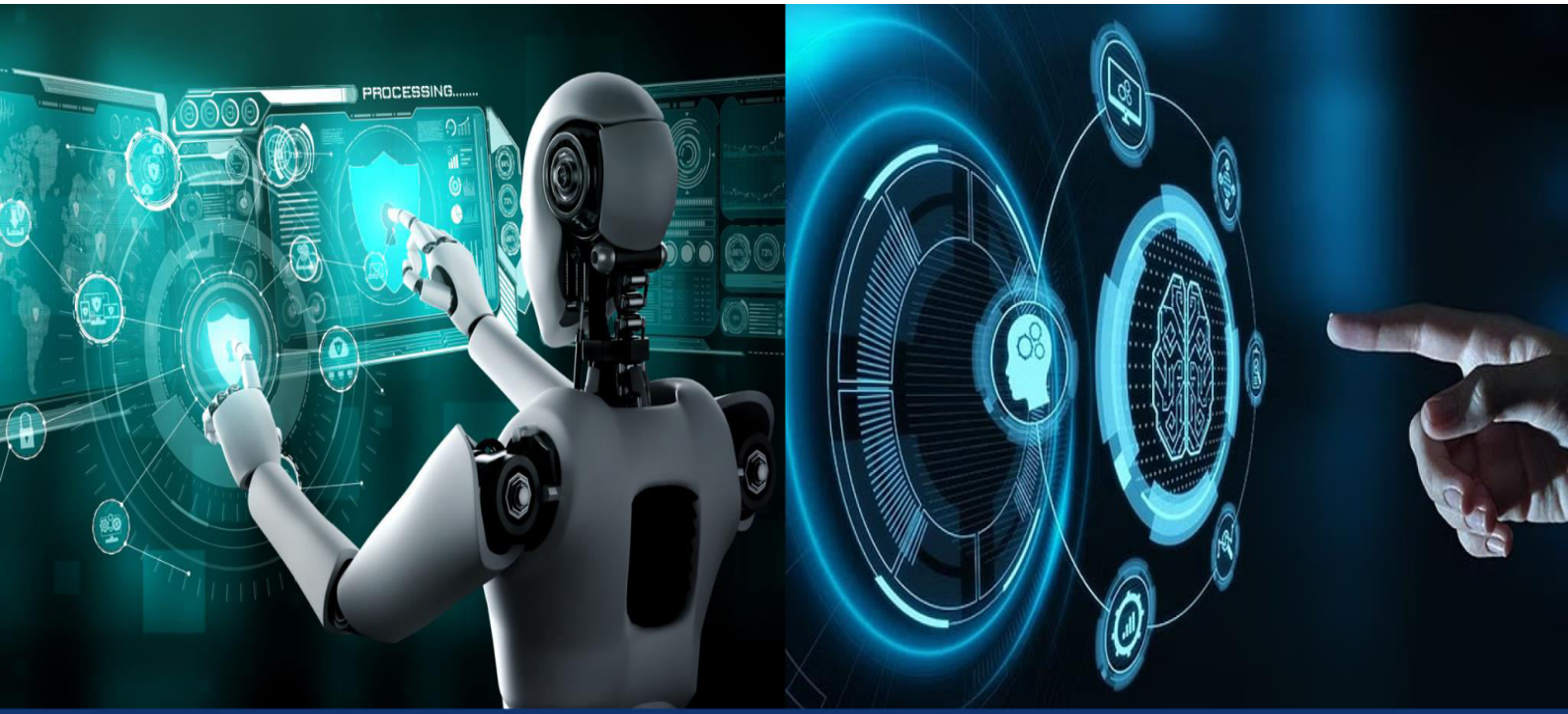
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406010

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Mobile-Based Forensic Case Management System with Evidence Integrity Verification

Harishkumar, Rajadhurai

PG Student, Department of Cyber Forensics and Information Security, DR. M. G. R. Educational and Research Institute, Chennai, Tamil Nadu, India

Assistant Professor, Department of Cyber Forensics and Information Security, DR. M. G. R. Educational and Research Institute, Chennai, Tamil Nadu, India

ABSTRACT: This paper presents a Secure Mobile-Based Forensic Case Management System with Evidence Integrity Verification, designed for digital and physical crime investigations. The system offers role-based authentication, secure case creation, evidence upload, suspect management, audio and text notes, and audit log tracking through a mobile platform. Uploaded evidence files, images, and videos are protected using SHA-256 hash generation to ensure integrity and immutability. AES-256 encryption is used for secure PDF report generation and evidence protection. The system also supports chain of custody documentation and manual hash verification for forensic validation. The proposed solution improves secure evidence handling, investigation efficiency, and forensic record management.

KEYWORDS: Forensic Case Management; SHA-256; AES-256; Mobile Forensics; Evidence Integrity; Chain of Custody; Flutter; Digital Investigation

I. INTRODUCTION

Digital investigations require secure handling, storage, and verification of forensic evidence to maintain integrity during criminal investigations. Traditional evidence management methods often face problems such as data tampering, poor record tracking, and inefficient documentation. This research introduces a Secure Mobile-Based Forensic Case Management System with Evidence Integrity Verification, aimed at managing digital and physical crime investigations through a mobile platform. The system provides role-based authentication, secure case management, evidence upload, suspect management, audit logs, and encrypted report generation. SHA-256 hashing maintains evidence integrity, while AES-256 encryption secures generated reports and stored records. The proposed system enhances forensic workflow efficiency, evidence security, and chain of custody management.

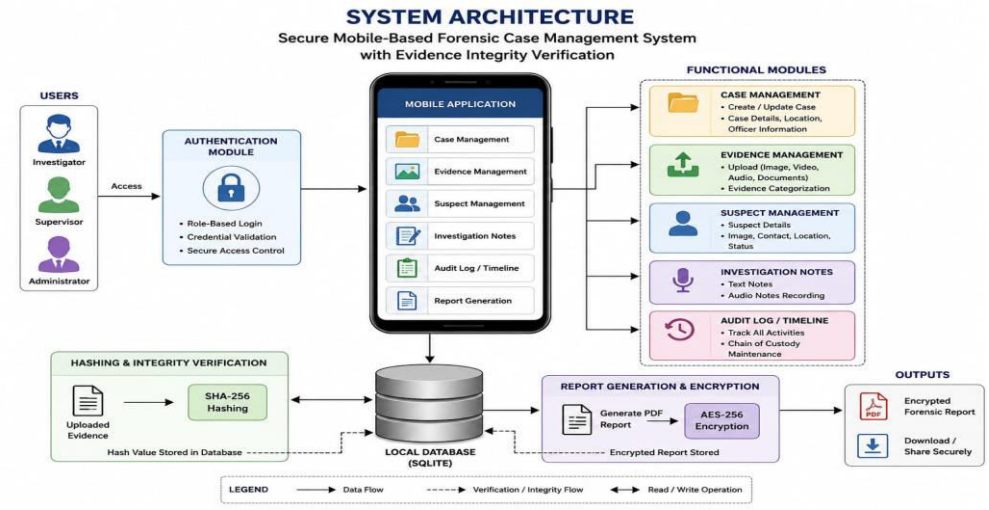


Fig. 1. System Architecture Overview of the Proposed Forensic Case Management System

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406010

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

Recent advancements in digital forensics focus on secure evidence handling, forensic readiness, and integrity verification techniques. Several researchers have proposed digital forensic analysis models to improve evidence reliability and reduce systematic investigation errors. Mobile forensic frameworks have been introduced to address the growing use of smartphones and portable devices in criminal investigations. Cryptographic methods, including AES encryption and secure hash algorithms, have been widely used to protect digital evidence and ensure forensic authenticity. Blockchain-based forensic evidence management systems have also been suggested to enhance chain of custody tracking and reduce tampering. Existing systems mainly focus on evidence acquisition and storage; however, there has been limited research on integrated mobile-based forensic case management systems that include secure evidence verification, encrypted reporting, audit logging, and suspect management. The proposed system aims to overcome these limitations by offering a secure and unified forensic investigation platform.

III. METHODOLOGY / APPROACH

The proposed Secure Mobile-Based Forensic Case Management System was developed to enhance secure evidence handling, integrity verification, and forensic investigation management using a mobile platform. The system follows a modular forensic workflow architecture that includes authentication, case management, evidence management, suspect management, audit logging, integrity verification, and encrypted report generation modules. This approach provides secure handling of digital evidence and improves forensic accountability during investigation processes.

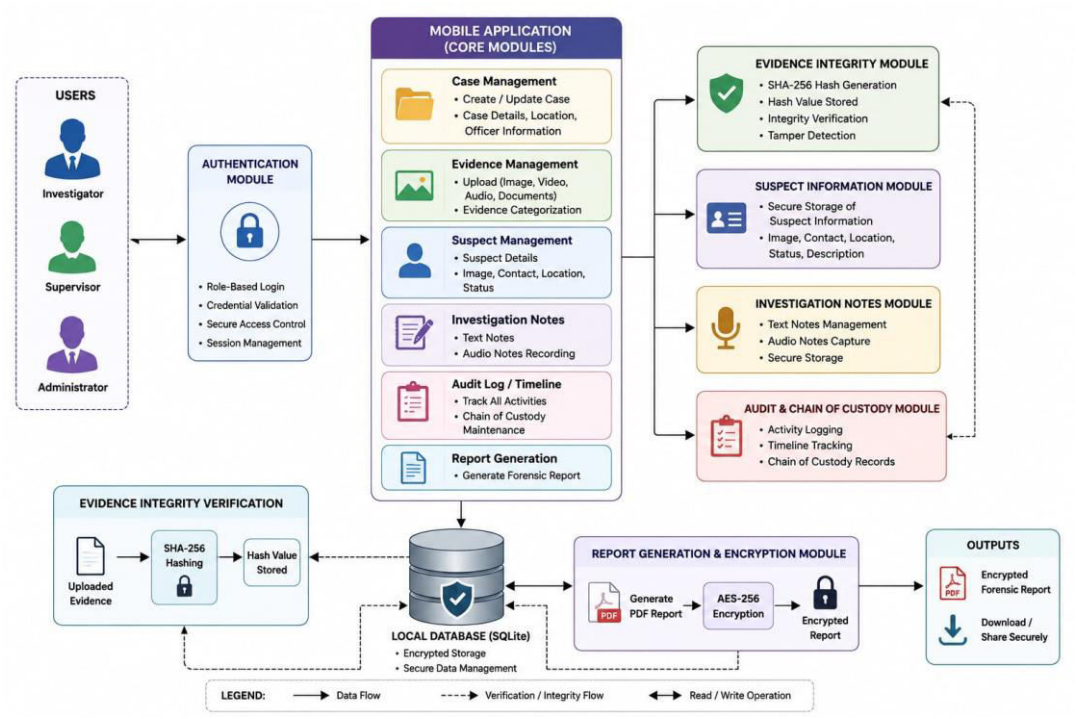


Fig. 2. Modular Forensic Workflow Architecture of the Proposed System

The authentication module uses role-based access control to prevent unauthorized access to forensic records and investigation data. Investigators, administrators, and authorized personnel can securely access the application using their login credentials. After successful authentication, users are directed to the centralized case management dashboard, allowing them to create and manage investigation records efficiently.

The case management module enables investigators to create new cases by entering the case number, case title, investigation officer details, investigation location, and case description. The centralized dashboard enhances

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

organization and monitoring of digital and physical crime investigations. All case-related information is securely stored in the local database system to maintain confidentiality and accessibility.

The evidence management module supports uploading images, videos, audio files, and digital documents related to forensic investigations. To maintain evidence integrity and immutability, SHA-256 hashing is automatically generated for every uploaded evidence file. The generated hash values are securely stored in the application database and can be manually verified during investigation and legal analysis processes. Any alteration to the original evidence generates a different hash value, allowing for tamper detection and verifying forensic reliability.

The system also includes audio and text-based forensic note management to aid in investigation documentation. Investigators can securely record observations, witness statements, case updates, and field investigation details within the application. Audio notes enhance real-time documentation during investigations, while text notes support organized forensic record keeping.

The suspect management module allows investigators to securely maintain suspect information related to each case. The module stores suspect images, names, phone numbers, locations, statuses, and other relevant details. This feature improves tracking of suspects and organization of investigations within the forensic workflow.

Audit logging and timeline tracking mechanisms are in place to ensure forensic accountability and maintain proper chain of custody records. All significant activities within the application are automatically recorded, including evidence uploads, case updates, note additions, and integrity verification operations. This audit trail enhances transparency and helps uphold the legal admissibility of digital evidence.

The report generation module creates PDF-based forensic investigation reports containing case summaries, uploaded evidence details, suspect information, investigation notes, and chain of custody records. AES-256 encryption is applied to the generated forensic reports and sensitive investigation records to ensure confidentiality and secure digital storage. This encryption protects forensic documents from unauthorized access and increases data security.

The proposed system was implemented using Flutter and Dart for cross-platform mobile application development, while SQLite was used for secure local database management. SHA-256 hashing was used for evidence integrity verification, and AES-256 encryption secured forensic report protection. The implemented methodology enhances evidence security, integrity verification, forensic workflow efficiency, and secure digital investigation management for both physical and digital crime investigations.

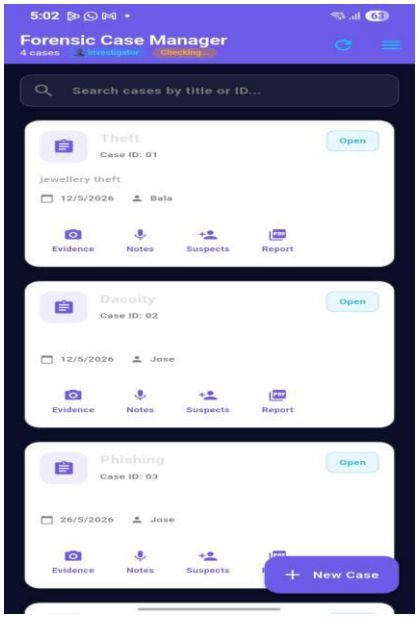


Fig. 3. Mobile Application Interface: Case Management Dashboard

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406010

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

TABLE I
TECHNOLOGIES USED IN THE PROPOSED SYSTEM

Technology	Purpose
Flutter	Mobile Application Development
Dart	Application Logic
SQLite	Local Database Management
SHA-256	Evidence Integrity Verification
AES-256	Secure Report Encryption
PDF Generator	Forensic Report Generation

IV. RESULTS & DISCUSSION

The proposed Secure Mobile-Based Forensic Case Management System was successfully implemented and tested for secure forensic investigation management, evidence handling, integrity verification, and encrypted report generation. The developed mobile application integrated role-based authentication, case management, evidence uploads, suspect management, audit logging, and forensic documentation within a single platform. The implemented modules functioned effectively under multiple testing conditions without data loss or integrity failure.

The authentication module successfully restricted unauthorized access through role-based login validation. Investigators efficiently created and managed cases using the centralized dashboard interface. The case management workflow improved organization and monitoring of investigation records related to both digital and physical crime scenes.

The evidence management module effectively supported uploading images, videos, audio files, and digital documents linked to investigations. SHA-256 hash values were automatically generated for all uploaded evidence items to ensure integrity verification and tamper detection. Manual verification tests confirmed that any modification to the original evidence created different hash values, validating the reliability of the integrity verification mechanism.

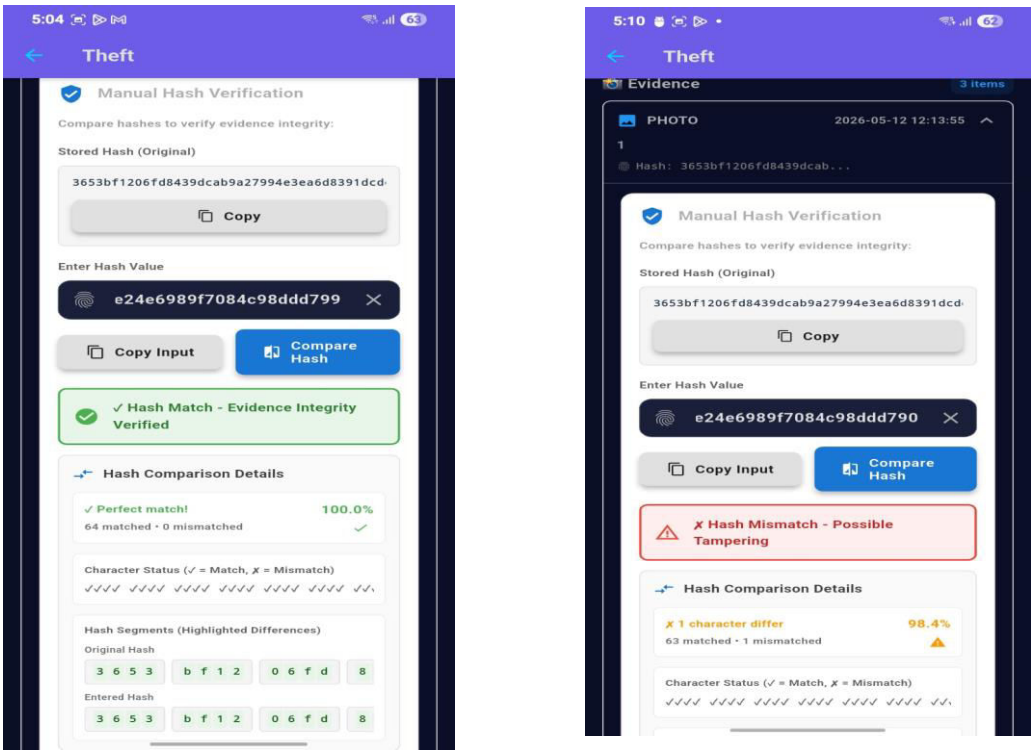


Fig. 4. SHA-256 Hash Generation and Manual Verification Process

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406010

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The forensic notes module successfully supported secure storage of text and audio notes during investigation processes. The suspect management module efficiently maintained suspect details, including images, locations, contact information, and investigation status records. The audit logging and timeline tracking modules accurately logged investigation activities, enhancing chain of custody maintenance for forensic accountability.

AES-256 encryption was successfully applied during PDF report generation to safeguard sensitive forensic records and investigation details. Generated reports, which included case summaries, evidence records, suspect details, and chain of custody information, were securely encrypted and protected from unauthorized access.

Compared to traditional forensic documentation methods, the proposed system enhances evidence security, speeds up case tracking, allows for secure digital storage, ensures integrity verification, and boosts forensic accountability. Existing forensic systems tend to focus on evidence storage and analysis, while the proposed system integrates secure case management, evidence integrity verification, audit logging, suspect management, and encrypted report generation into a single mobile-based forensic platform.

TABLE II
COMPARISON OF EXISTING SYSTEM AND PROPOSED SYSTEM

Feature	Traditional Investigation Method	Proposed System
Case Documentation	Manual Records	Digital Case Management
Evidence Security	Limited	SHA-256 Integrity Verification
Report Protection	Basic Storage	AES-256 Encryption
Investigation Notes	Paper-Based	Audio & Text Notes
Chain of Custody	Manual Tracking	Automated Audit Logging
Accessibility	Physical Files	Mobile-Based Access

The experimental results indicate that the proposed system significantly improves forensic workflow efficiency, secure evidence handling, integrity verification, and digital investigation management. The implemented security measures and forensic workflow modules offer a reliable solution for managing digital evidence in modern forensic investigations.

Fig. 5. AES-256 Encrypted PDF Forensic Report Generation

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. CONCLUSION

The proposed Secure Mobile-Based Forensic Case Management System with Evidence Integrity Verification was successfully designed and implemented for secure management of digital and physical crime investigations. The system features role-based authentication, secure case management, digital evidence handling, suspect management, forensic note management, audit logging, integrity verification, and encrypted report generation within a single mobile platform. SHA-256 hashing effectively ensured evidence integrity and tamper detection, while AES-256 encryption provided secure protection for forensic reports and sensitive investigation records.

The implemented system enhanced forensic workflow efficiency, secure handling of evidence, maintenance of the chain of custody, and accountability during investigations compared to traditional forensic documentation methods. The experimental results showed consistent performance across all implemented modules, with no integrity failures or data loss during testing.

Future enhancements of the proposed system may include cloud-based evidence synchronization, biometric authentication, AI-assisted evidence analysis, and real-time collaboration features for investigators.

REFERENCES

1. R. Cuomo, D. D'Agostino, and M. Ianulardo, "Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments," Sensors, vol. 22, no. 18, p. 7096, 2022. DOI: 10.3390/s22187096.
2. Cellebrite, "2022 Industry Trends Survey: Digital Evidence Management in Law Enforcement," Cellebrite DI Ltd., Petah Tikvah, Israel, Tech. Rep., Nov. 2022. [Online]. Available: https://www.cellebrite.com.
3. Delhi Police, "e-Sakshya: Digital Evidence Management System for Streamlined Collection and Documentation of Crime Scene Evidence," Ministry of Home Affairs, Government of India, New Delhi, 2023. Available: https://www.mha.gov.in.
4. G. V. Kumar, "Mobile-Based Digital Forensic Case Management for Andhra Pradesh Law Enforcement: Architecture and Implementation," Int. J. of Creative and Emerging Engineering (IJCEE), vol. 5, no. 2, pp. 112–124, 2023.
5. Monolith Forensics, "Monolith: A Case, Evidence, and Analysis Management Platform for Digital Forensic Labs," Monolith Forensics Inc., 2023. Available: https://www.monolithforensics.com.
6. Nuix, "Nuix Neo Investigations: Automated Workflows and Multi-Source Digital Evidence Review for Law Enforcement," Nuix Ltd., Sydney, Australia, White Paper, Mar. 2023. Available: https://www.nuix.com.
7. T. Nath, P. Sharma, and R. Singh, "Digital Evidence Chain of Custody: Integrity Constraints and Operational Categories for Admissibility and Trustworthiness," J. of Digital Forensics, Security and Law, vol. 19, no. 1, pp. 45–62, 2024.
8. I. Ismail and K. A. Z. Ariffin, "The Admissibility of Digital Evidence from Open-Source Forensic Tools: Development of a Framework for Legal Acceptance," PLOS ONE, 2025. DOI: 10.1371/journal.pone.0331683.
9. A. Arooj, M. Farooq, and T. Umer, "Blockchain-Based Chain-of-Custody Models for Tamper-Proof Digital Evidence Management Using SHA-256 Hashing," Int. J. of Engineering, Mathematics and Technology Sciences (IRJMETS), vol. 6, no. 7, pp. 34–48, 2022.
10. S. Sumithra and K. Sakshi, "Recent Challenges and Strategies in Mobile Device Forensics: Encryption, Data Fragmentation, and Legal Considerations," J. of Information Security and Its Applications (JISIS), vol. 12, no. 2, pp. 67–79, 2024.
11. T. D'Anna, M. Puntarello, G. Cannella, G. Scalzo, R. Buscemi, S. Zerbo, and A. Argo, "The Chain of Custody in the Era of Modern Forensics: From the Classic Approach to Blockchain-Assisted Models," Forensic Sciences Research, 2023. DOI: 10.1016/j.scijus.2022.02.006.
12. E. Cunha and Z. Obertova, "Forensic Identification in a Multidisciplinary Perspective: Big Challenges in Digital Evidence and AES-256 Protected Reporting," Forensic Sciences Research, vol. 9, no. 3, p. owae063, 2024. DOI: 10.1093/fsr/owae063.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details