International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 06 June 2026
Page No: 4481 - 4485
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0587

A Secure Digital Evidence Management System for Public Safety Applications

Arpita[1], G M Bindu [2], Manali[3], Neha T N4, Dr. Manas M N[5]
[1,2,3,4] UG – CSE-CY, RV College of Engineering, Bangalore, Karnataka
[5] Assistant Professor, CSE, RV College of Engineering, Bangalore, Karnataka
Emails: *arpita.cy24@rvce.edu.in[1], gmbindu.im23@rvce.edu.in[2], manali.ec24@rvce.edu.in[3], nehatn.cy24@rvce.edu.in[4], manasmn@rvce.edu.in[5]*

Abstract
This paper presents a Secure Digital Evidence Management System for Public Safety Applications that integrates IoT devices, cryptographic security, and cloud storage to ensure the confidentiality, integrity, and traceability of digital evidence. The system uses an ESP32 microcontroller connected to an ultrasonic sensor for real-time object detection. When an object is detected within a predefined range, the ESP32 sends a trigger signal to a laptop through serial communication. A Python-based application then captures video evidence using a webcam and the OpenCV library, enabling automated real-time evidence collection. The system includes a secure dashboard with role-based access control, allowing authorized users to upload, manage, and retrieve evidence efficiently. To protect sensitive data, a hybrid cryptographic framework is implemented, combining Advanced Encryption Standard (AES) for file encryption and RSA-based key encapsulation for secure key exchange. SHA-256 hashing is used to generate unique digital fingerprints for each evidence file, ensuring data integrity. A blockchain-inspired hash chaining mechanism links records sequentially, making any tampering or unauthorized modifications easily detectable. Encrypted evidence files are stored securely in Microsoft Azure Blob Storage, while metadata such as timestamps, file hashes, user information, and tamper status are maintained in a MySQL database. The system also performs automated cloud integrity checks and chain validation to identify missing or altered records. By combining IoT-based sensing, real-time video acquisition, cryptographic protection, cloud storage, and secure access control, the proposed system provides a reliable and tamper-resistant platform for digital evidence management, significantly improving the effectiveness and trustworthiness of digital forensic investigations in public safety environments.

Keywords: *Digital Evidence Management System, IoT-Based Surveillance, Digital Forensics, Hybrid Cryptography, AES-RSA Encryption, SHA-256, Blockchain-Inspired Hash Chaining, Cloud Security.*

1. Introduction
The increasing use of Internet of Things (IoT) devices, surveillance systems, and cloud computing technologies has led to a significant growth in the volume of digital evidence generated in public safety and forensic investigations. Digital evidence, including videos, images, documents, and other unstructured data, plays a critical role in incident analysis, crime investigation, and legal proceedings. However, traditional evidence management systems are often vulnerable to unauthorized access, data tampering, loss of evidence, and inadequate integrity verification, which can compromise the reliability of forensic investigations. This paper proposes a Secure Digital Evidence Management System that integrates IoT-based object detection, real-time video acquisition, cryptographic security mechanisms, and cloud-based storage. The system utilizes an ESP32 microcontroller and ultrasonic sensor for automated event detection and evidence collection. Captured evidence and user-uploaded digital files, including videos, images, and other unstructured data, are protected using AES encryption, RSA-based key exchange, SHA-256 hashing, and a blockchain-inspired hash chaining mechanism for tamper detection.Furthermore, the system incorporates role-based access control, secure cloud storage, and integrity verification mechanisms to support authorized evidence management and retrieval. The proposed framework provides an end-to-end solution for secure evidence acquisition, storage, monitoring,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 06 June 2026
Page No: 4481 - 4485
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0587

and retrieval, thereby enhancing the reliability and trustworthiness of digital forensic investigations in public safety applications.

1.1. PROBLEM STATEMENT

Digital evidence collected in public safety and forensic investigations is vulnerable to unauthorized access, tampering, and loss [1-9]. Existing evidence management systems often lack secure storage, integrity verification, and effective access control, making it difficult to ensure the confidentiality, authenticity, and traceability of digital evidence throughout its lifecycle.

1.2. OBJECTIVES

The primary objective of this work is to develop a secure and reliable Digital Evidence Management System for public safety and forensic applications. The system aims to automate evidence collection through IoT-based object detection and real-time video capture while ensuring the confidentiality, integrity, and traceability of digital evidence. It utilizes AES and RSA cryptographic techniques for secure encryption and key management, SHA-256 hashing for integrity verification, and blockchain-inspired hash chaining for tamper detection.

2. Methodology

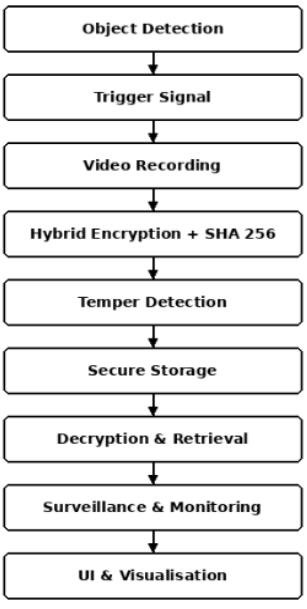

Figure 1 Flowchart

The proposed Secure Digital Evidence Management System begins with object detection using an ultrasonic sensor interfaced with an ESP32 microcontroller. The sensor continuously monitors the surrounding environment and measures the distance of nearby objects. When an object is detected within a predefined threshold range, the ESP32 identifies the event and initiates the evidence collection process automatically. This IoT-based sensing mechanism minimizes human intervention and enables real-time monitoring. Once an object is detected, the ESP32 sends a trigger signal to a computer through serial communication. Upon receiving the signal, a Python-based application activates a webcam and starts video recording using the OpenCV library. This process ensures automatic acquisition of digital evidence, capturing relevant events in real time without requiring manual operation. After the evidence is collected, the recorded video file undergoes cryptographic processing. A hybrid encryption approach is employed, where AES is used to encrypt the evidence file efficiently, while RSA is utilized for secure key exchange and key protection. Additionally, a SHA-256 hash value is generated for every evidence file, creating a unique digital fingerprint that can later be used for integrity verification. To prevent unauthorized modification of evidence, a tamper detection mechanism based on blockchain-inspired hash chaining is implemented. Each evidence record contains the hash of the previous record, creating a secure chain of evidence entries. Any alteration, deletion, or insertion of records changes the chain structure and can be immediately detected during validation. The encrypted evidence is then uploaded to secure cloud storage using Microsoft Azure Blob Storage. Along with the evidence file, metadata such as timestamps, file hashes, user information, and integrity status are stored in a MySQL database. This architecture ensures secure, scalable, and reliable storage of videos, images, documents, and other unstructured digital evidence. During retrieval, authorized users access the system through a secure dashboard featuring role-based access control. The system verifies user credentials, validates file integrity using stored hash values, and performs decryption and retrieval of evidence. The dashboard also provides surveillance, monitoring, and visualization capabilities, enabling users to upload, manage, track, and analyze digital evidence

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 06 June 2026
Page No: 4481 - 4485
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0587

efficiently while maintaining complete traceability and security.

3. Results and Discussion

3.1. Results

The proposed system successfully automated digital evidence collection, encryption, storage, and retrieval. Object detection accurately triggered video recording, while AES-RSA encryption, SHA-256 hashing, and hash chaining ensured evidence security and integrity. The cloud-based storage and role-based dashboard enabled secure evidence management, demonstrating the system's effectiveness for public safety and forensic applications.

3.2. Discussion

The results demonstrate that the proposed system provides a secure and efficient approach for digital evidence management. The integration of IoT-based detection, automated video capture, encryption, hashing, and cloud storage ensures evidence confidentiality, integrity, and traceability. The implementation of role-based access control and tamper detection mechanisms further enhances security, making the system suitable for public safety and digital forensic applications shown in Figures 1-11

Figure 2 Role based access

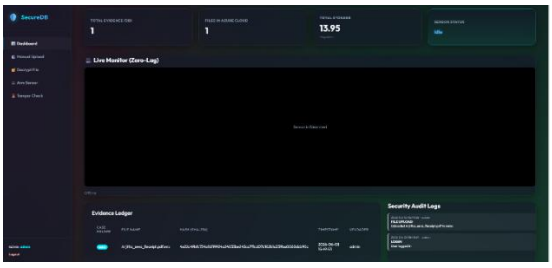

Figure 3 Secure evidence dashboard

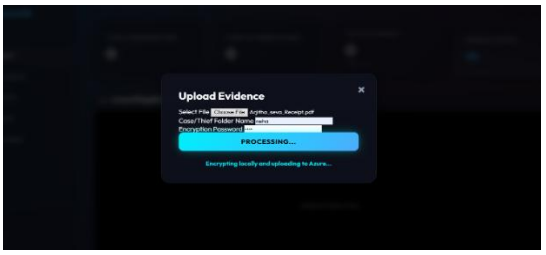

Figure 4 Uploading encrypted files

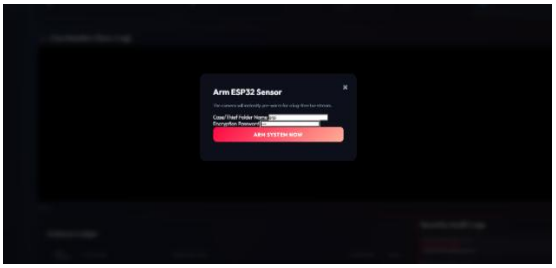

Figure 5 Accessing webcam through secure credentials

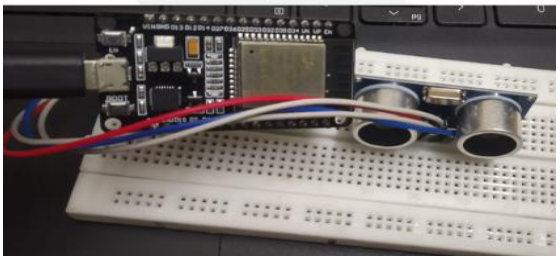

Figure 6 Object detection

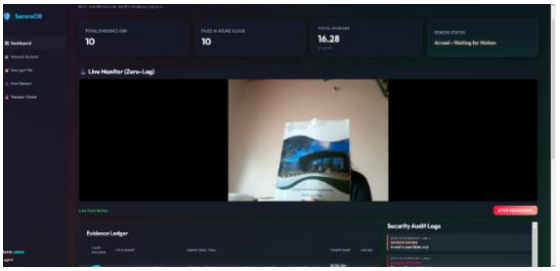

Figure 7 Evidence video capturing

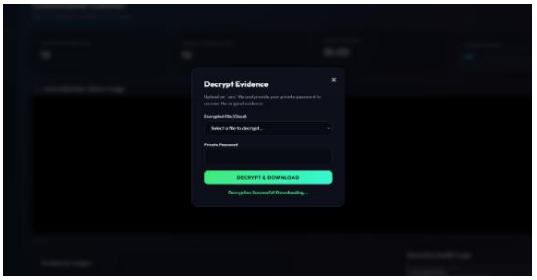

Figure 8 Decrypting files

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 06 June 2026
Page No: 4481 - 4485
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0587

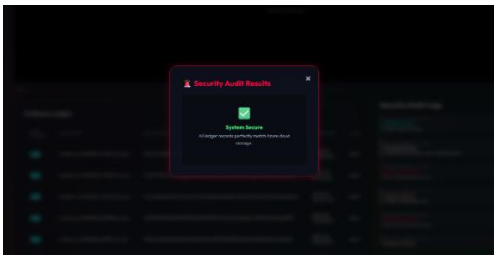

Figure 9 Tempering check

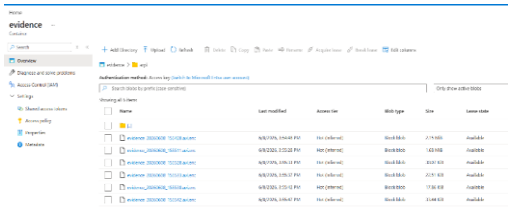

Figure 10 Encrypted files

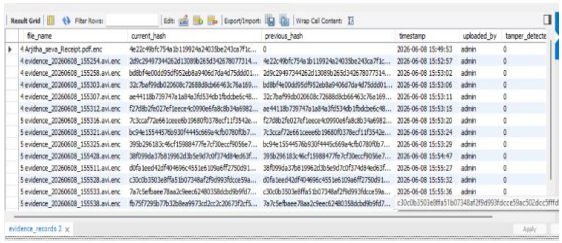

Figure 11 Cryptographic hash for each file for integrity check

Figure 11 Tempering detection

Conclusion

The proposed Secure Digital Evidence Management System provides a reliable and secure framework for collecting, storing, and managing digital evidence. By integrating IoT-based object detection, automated video capture, hybrid cryptography, SHA-256 hashing, and cloud storage, the system ensures evidence confidentiality, integrity, and traceability. The implementation of tamper detection and role-based access control further enhances security, making the system suitable for public safety and digital forensic applications. The results demonstrate the effectiveness of the proposed approach in maintaining secure and trustworthy digital evidence throughout its lifecycle.

Acknowledgements

The authors intend to convey their heartfelt gratitude to the institution and the faculty members for their insightful guidance and continuous support throughout the course of this research work and study. The authors acknowledge the contribution of publicly accessible patent databases and resources to the successful execution of the system. The research was conducted without any external financial support.

References [

[1]. A. Singh, R. A. Ikuesan, and H. Venter, "Secure Storage Model for Digital Forensic Readiness," IEEE Access, vol. 10, pp. 19469–19480, Feb. 2022. doi: 10.1109/ACCESS.2022.3151403.

[2]. L. Malina, P. Muzikant, M. Nohava, J. Hajny, A. Dufka, P. Svenda, and V. Stupka, "Secure Cloud Storage System for Digital Evidence," in Proc. 15th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2023, pp. 134–139. doi: 10.1109/ICUMT61075.2023.10333268.

[3]. S. G, V. Narendhran, K. D, M. A, and K. K, "Blockchain-Based Evidence Tracking System for Forensic Integrity and Secure Chain of Custody," in Proc. 1st Int. Conf. on Radio Frequency Communication and Networks (RFCoN), 2025. doi: 10.1109/RFCoN62306.2025.11085167.

[4]. S. G, V. Narendhran, K. D, M. A, and K. K, "Blockchain-Based Evidence Tracking System for Forensic Integrity and Secure Chain of Custody," in Proc. 1st Int. Conf. on Radio Frequency Communication and Networks (RFCoN), 2025. doi: 10.1109/RFCoN62306.2025.11085167.

[5]. V. V. R. Gudlur, "Enhanced Digital Forensic Model for Securing the Internet of Things," in Proc. IEEE 14th Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2024, pp. 5–9. doi: 10.1109/ISCAIE61308.2024.10576479.

[6]. L. Li, D. Jin, T. Zhang, and N. Li, "A Secure,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 06 June 2026
Page No: 4481 - 4485
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0587

Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data," IEEE Access, vol. 11, pp. 97318–97330, Sep. 2023. doi: 10.1109/ACCESS.2023.3311712.

[7]. S. Nath, K. Summers, J. Baek, and G. J. Ahn, "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics," in Proc. IEEE 6th Int. Conf. on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2024, pp. 11–20. doi: 10.1109/TPS-ISA62245.2024.00012.

[8]. J. Richter, N. Kuntze, and C. Rudolph, "Securing Digital Evidence," in Proc. 5th Int. Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2010, pp. 119–130. doi: 10.1109/SADFE.2010.31.

[9]. V. Balmiki, "An Evidence Collection Using Blockchain for Cybercrime Detection," in Proc. 4th IEEE Global Conf. for Advancement in Technology (GCAT), Bangalore, India, Oct. 2023. doi: 10.1109/GCAT59970.2023.10353259.