Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Improving Digital Forensic Security A Secure Storage Model With Authentication And Optimal Key Generation Based Encryption

H. Sathish[1], S. Hima Bindhu[2], T. Shirisha[2], M. Shashank[2], M. Someshwar[2]

[1]Assistant Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India
[2]UG Students, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Correspondence

H Sathish

Assistant Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

- Received Date: 25 Jan 2026
- Accepted Date: 14 Mar 2026
- Publication Date: 20 Mar 2026

Abstract

Digital forensic data plays a critical role in cybercrime investigation and must be stored securely to prevent unauthorized access, tampering, and data loss. Traditional digital forensic systems rely on centralized storage mechanisms, which are vulnerable to security threats such as data modification, insider attacks, and integrity violations. To address these challenges, this project proposes a secure digital forensic data storage model with authentication and optimal key generation. The system uses strong cryptographic techniques to ensure confidentiality, integrity, and controlled access to sensitive forensic evidence. In the proposed approach, users must register and authenticate before accessing the system. When forensic data is uploaded, the system encrypts the data using AES encryption algorithm to protect confidentiality. A hash value is generated using secure hashing techniques to maintain data integrity and detect any unauthorized modifications. The encrypted data is stored securely in the database or cloud storage. Authorized users can search and retrieve forensic data, and decryption is performed only after successful authentication. The admin module monitors system activities, manages users, and verifies data integrity.

The proposed system improves security by preventing unauthorized access, ensuring tamperproof storage, and enabling secure data retrieval. The implementation is developed using Java, MySQL database, and secure cloud-based storage. Experimental results demonstrate that the system provides reliable security, efficient data management, and integrity verification. This approach enhances trust in digital forensic investigations and ensures safe handling of critical forensic evidence.

Keywords

Digital Forensics, Secure Storage, Data Security, Encryption, AES Algorithm, Hashing, Data Integrity, Authentication, Secure Access, Cloud Storage, Key Generation, Cyber Security, Digital Evidence Protection, Secure Data Retrieval, Confidentiality, Access Control, Java, MySQL Database, Forensic Data Management, Secure System.

Introduction

Digital forensics is an important field used for collecting, analyzing, and preserving digital evidence during cybercrime investigations. The evidence may include files, images, logs, emails, and other digital data collected from computers, networks, or mobile devices. Since this data is highly sensitive, it must be protected from unauthorized access, modification, and deletion. If digital evidence is tampered with, it may affect investigation results and reduce the reliability of forensic analysis. Therefore, providing secure storage and controlled access for digital forensic data is very important.

Traditional digital forensic systems mainly use centralized storage methods to store evidence. These systems often lack strong security mechanisms, making them vulnerable to cyber-attacks, insider threats, and unauthorized modifications. In addition, many existing systems do not provide proper authentication and data integrity verification. Without encryption and integrity checking, digital evidence can be accessed or altered by unauthorized users. This creates major challenges in maintaining confidentiality, integrity, and availability of forensic data.

To overcome these issues, a secure digital forensic data storage model is required. The proposed system focuses on protecting forensic data using encryption, authentication, and integrity verification techniques. When users upload forensic data, the system encrypts the data using AES algorithm to ensure confidentiality. A hash value is generated for each file to verify integrity and detect tampering. Only authorized users with valid credentials are allowed to access and decrypt the data. This ensures that sensitive forensic information remains protected.

Background

The rapid growth of the internet and digital technologies, cyber crimes have increased significantly. Digital evidence such as files, logs, and datasets is often used in cyber investigations to identify criminal activities. Therefore, it is very important to maintain the security and integrity of such data. Traditional digital forensic systems usually rely on centralized storage systems. These systems may face several issues such as single point of failure, unauthorized access, and data

Citation: Sathish H, Hima Bindhu S, Shirisha T, Shashank M, Someshwar M. Improving Digital Forensic Security A Secure Storage Model With Authentication And Optimal Key Generation Based Encryption. GJEIIR. 2026;6(3):0190.

modification. If the stored evidence is tampered with, it may affect the investigation process. To overcome these issues, modern systems use advanced security mechanisms such as cryptography and secure data storage techniques. Encryption protects data confidentiality, while hashing ensures that the data has not been altered. This project focuses on improving the security of digital forensic datasets by integrating encryption, hashing, and secure database management techniques.

Problem Statement

Digital forensic investigations require secure storage and handling of sensitive digital evidence. Traditional forensic systems store data in centralized databases without strong security mechanisms. These systems are vulnerable to unauthorized access, data tampering, and accidental deletion. If digital evidence is modified or lost, it may affect investigation accuracy and reduce trust in forensic results.

Another major problem is the lack of proper authentication and access control. Unauthorized users may access confidential forensic data due to weak login and security mechanisms. Existing systems also do not provide proper encryption, which makes the stored data exposed to cyber-attacks. Additionally, many systems do not include data integrity verification, making it difficult to detect whether the stored evidence has been altered.

Literature Survey

- P. M. Bachiphale and N. S. Zulpe (2023) proposed an optimal multi-secret image sharing scheme using lightweight visual sign-cryptography with optimal key generation. The method improves data confidentiality and secure key generation. However, the approach mainly focuses on image security and does not address secure storage of digital forensic data.
- G. Kumar et al. (2021) introduced a blockchain-based Internet-of-Forensic (IoF) framework for IoT applications. The system provides tamper-proof storage and improves transparency in forensic investigations. However, blockchain implementation increases computational overhead and lacks efficient encryption-based storage.
- L. Raji and S. T. Ramya (2022) proposed a secure forensic data transmission system using fuzzy-based butterfly optimization and modified ECC. The method improves secure data transmission and encryption efficiency. However, it focuses only on transmission and not on secure data storage.
- E. A. Abdel-Ghaffar and M. Daoudi (2023) presented authentication and cryptographic key generation using EEG signals. The method improves security and generates unique keys.
- However, it requires special hardware and is not suitable for general forensic storage systems.
- H. Chen et al. (2019) proposed multi-key homomorphic encryption for secure data processing. The method allows computation on encrypted data and improves privacy. However, it introduces high computational complexity and is not optimized for forensic storage applications.

Proposed System

The proposed system, Digital Forensic Architecture – Authentication with Optimal Key Generation Encryption (DFA-AOKGE), introduces a secure and decentralized architecture for digital investigations. Unlike traditional centralized systems, DFA-AOKGE ensures tamperproof evidence storage by leveraging blockchain technology, which maintains an immutable ledger of all forensic data, logs, and access events. The Enhanced Equilibrium Optimizer (EEO) is employed to generate optimal cryptographic keys, 7 enhancing the strength and reliability of encryption processes while reducing the risk of brute-force or cryptanalytic attacks. For authentication, the Secure Block Verification Mechanism (SBVM) provides a robust, multifactor verification system that ensures only authorized investigators can access sensitive evidence, preventing unauthorized manipulation or viewing.

Modules Used

- **User Registration Module:** The User Registration Module allows new users to create an account in the system by entering their personal details such as username, password, email, mobile number, address, date of birth, gender, and a profile picture.
- **Dataset Upload Module:** The Dataset Upload Module allows users to upload Excel datasets containing digital forensic records such as Pid, Date-Time, and Post Content. Old logs are cleared before inserting the new dataset. Every record is also backed up in a secondary table for safety.
- **Data Encryption Module:** The Data Encryption Module converts plaintext post content into secure encrypted text before storing it in the database. AES encryption combined with Base64 encoding is performed , ensuring that the original content cannot be accessed by unauthorized users.
- **Data Decryption Module :** The Data Decryption Module retrieves encrypted dataset records and converts them back into readable text when required. Decryption takes place during search operations or dataset display in pages . Only authenticated users can view decrypted content, maintaining controlled access.
- **Admin Management Module:** The Admin Management Module handles system supervision and user approval. Admins log in, and after authentication, they can approve new users, check user activity, review uploaded datasets, and monitor system usage patterns. Admins serve as the authority controlling who can access the system.

Advantages of proposed system

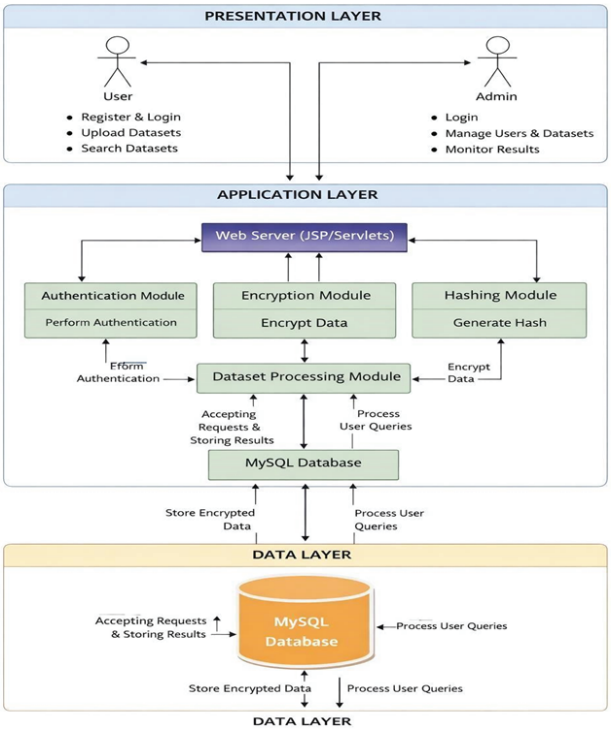
- **Decentralized Evidence Management:** Blockchain ensures evidence is stored across multiple peers, eliminating a single point of failure.
- **Tamper-proof Records:** Immutable blockchain logs maintain a verifiable chain-of custody, increasing legal admissibility.
- **Strong Authentication:** SBVM provides multi-factor verification to ensure only authorized investigators can access data.
- **Optimized Encryption Keys:** EEO algorithm generates robust encryption keys, improving cryptographic strength.
- **Privacy-preserving Data Processing:** Multi-key homomorphic encryption allows secure computation on encrypted evidence.
- **Scalable and Flexible:** Supports cloud-based environments and distributed data sources efficiently.
- **Reliable Evidence Integrity:** Continuous hash verification ensures that evidence remains unaltered

throughout its lifecycle.

- **Enhanced Security:** Combines authentication and encryption for comprehensive protection against cyber threats.
- **Improved Investigation Efficiency:** Automated verification, logging, and encryption reduce manual effort and investigation time.

System Architecture

The system architecture of the Digital Forensic Security Model defines the overall structure of the system and how different components interact with each other. The architecture integrates user interfaces, server-side processing, encryption mechanisms, and database storage to ensure secure handling of digital forensic data.



Results

The proposed digital forensic secure storage system was successfully implemented and tested using different user scenarios. The system allows users to securely upload, store, search, and retrieve digital forensic data. During testing, the encryption module successfully protected the uploaded data using AES algorithm, ensuring that the stored files were not readable without proper authorization. This confirms that the system maintains confidentiality of sensitive forensic information.

The authentication mechanism was tested with valid and invalid login credentials. The system allowed access only to authorized users and blocked unauthorized users. This demonstrates that the access control mechanism works correctly. The admin module successfully monitored user activities and managed uploaded files, which improves system security and accountability.

Conclusion

In this project, we developed the DFA-AOKGE system to improve the security and reliability of digital forensic data, particularly digital images. The system combines blockchain technology for tamper-proof and decentralized evidence storage, strong authentication using SBVM to ensure that only authorized investigators can access data, and optimized key generation using EEO to create secure encryption keys for protecting sensitive information. The experimental results show that DFA-AOKGE is more secure and efficient compared to traditional systems. It helps prevent unauthorized access, ensures data integrity, and maintains privacy while allowing investigators to collect, store, and analyze evidence safely. The system's decentralized design also improves flexibility and reliability, making it suitable for real-world digital forensic investigations.

Future Scope

The Proposed secure storage model can be further enhanced to support emerging digital forensic requirements and advanced security needs. In the future, the system can be integrated with machine learning–based anomaly detection to automatically identify suspicious uploads or unauthorized access attempts. The cryptographic layer can be strengthened by upgrading AES to advanced hybrid encryption methods such as AES + RSA or ECC-based key generation to provide stronger resistance to modern cyberattacks. Cloud integration can also be implemented to store encrypted forensic evidence in decentralized or blockchain-based environments, allowing tamper-proof logging and improved traceability. Additionally, the system can include role-based access control so investigators, analysts, and administrators have different privileges. Support for larger file formats such as videos, images, and log files can be added to handle real forensic datasets. In future versions, automated report generation, real-time monitoring dashboards, and mobile accessibility may also be included to make the system more user-friendly and efficient. Overall, there is significant scope to extend the platform into a fully automated, AIdriven, highly secure digital forensic management system.

.

References

1. P. M. Bachiphale and N. S. Zulpe, "Optimal multi secret image sharing using lightweight visual sign-cryptography scheme with optimal key generation for gray/color images," Int. J. Image Graph.,Jul. 2023, Art. no. 2550017.
2. G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications," Future Gener. Comput. Syst., vol. 120, pp. 13– 25, Jul. 2021.
3. L. Raji and S. T. Ramya, "Secure forensic data transmission system in cloud database using fuzzy based butterfly optimization and modified ECC," Trans. Emerg. Telecommun. Technol., vol. 33, no. 9, p. e4558,Sep. 2022.
4. E. A. Abdel-Ghaffar and M. Daoudi, "Personal authentication and cryptographic key generation based on electroencephalographic signals," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 5, May 2023, Art. no. 101541.
5. H. Chen,W. Dai, M. Kim, and Y. Song, "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference," in Proc. ACM SIGSAC Conf. Comput. Commun.Secur., Nov. 2019, pp. 395–412.