

# An Implementation Of Block Chain Technology In Forensic Evidence Management

Mr B.Narsingham<sup>1</sup>, D.Karthik<sup>2</sup>, J.karthik<sup>3</sup>, K.Ashwitha<sup>4</sup>

<sup>1</sup> Assistant Professor, Department of Computer Science and Engineering

<sup>2,3,4</sup> B.Tech Students, Department of Computer Science and Engineering  
Teegala Krishna Reddy Engineering College, Telangana, India

\*\*\*

**Abstract** - Digital forensic evidence management requires high levels of security, integrity, and reliability due to the sensitive nature of legal data. Traditional systems suffer from weak encryption mechanisms, centralized storage, and vulnerability to data tampering. This paper proposes a secure digital forensic architecture integrating blockchain technology with advanced encryption techniques, namely Authentication with Optimal Key Generation Encryption (DFA-AOKGE). The system employs Multikey Homomorphic Encryption to ensure confidentiality while enabling secure data processing. A Secure Block Verification Mechanism is used to maintain data integrity across distributed nodes. The architecture supports multiple stakeholders, including users, administrators, and judicial authorities, enabling controlled access and secure evidence sharing. Experimental analysis demonstrates improved security, scalability, and efficiency compared to existing approaches. The proposed system provides a robust and trustworthy solution for modern digital forensic investigations.

**Key Words:** Digital Forensics, Blockchain, Data Security, Encryption, Multikey Homomorphic Encryption, DFA-AOKGE, Cloud Forensics, Evidence Management, Data Integrity, Cybersecurity.

## 1. INTRODUCTION

In recent years, the rapid growth of digital technologies and cybercrime has significantly increased the importance of secure digital forensic evidence management. Digital evidence plays a critical role in criminal investigations, legal proceedings, and cybersecurity analysis. However, maintaining the confidentiality, integrity, and availability of such sensitive data remains a major challenge due to evolving cyber threats and system vulnerabilities [9], [10].

Traditional forensic systems rely on centralized storage and outdated encryption techniques such as Data Encryption Standard (DES), which are highly vulnerable to brute-force attacks and unauthorized access [5]. These limitations raise serious concerns regarding data tampering, evidence authenticity, and trustworthiness in legal scenarios. Furthermore, centralized architectures increase the risk of single points of failure, making systems more susceptible to cyberattacks and data breaches [7].

Blockchain technology has emerged as a promising solution for ensuring secure and tamper-proof data management. Its decentralized and immutable nature enables transparent and verifiable record-keeping, making it highly suitable for digital forensic applications [1], [2]. Blockchain ensures that once data is recorded, it cannot be altered without consensus, thereby preserving the integrity of digital evidence [3].

In addition to blockchain, advanced cryptographic techniques such as homomorphic encryption provide enhanced security by allowing computations on encrypted data without exposing the original content [4]. This is particularly useful in forensic investigations where sensitive data must be processed securely. Modern cryptographic frameworks further strengthen data protection by incorporating secure key generation and distribution mechanisms [8].

Cloud computing has also become an integral part of digital forensic systems due to its scalability, flexibility, and storage capabilities. However, it introduces new security challenges, including data privacy risks and unauthorized access [14]. Therefore, integrating blockchain with secure encryption techniques in a cloud environment can significantly improve the reliability and security of forensic evidence management systems.

To address these challenges, this paper proposes a secure digital forensic architecture that combines blockchain technology with advanced encryption mechanisms such as Authentication with Optimal Key Generation Encryption (DFA-AOKGE). The system ensures secure storage, controlled access, and reliable sharing of digital evidence among multiple stakeholders, including investigators, administrators, and judicial authorities. By leveraging decentralized storage, strong encryption, and secure verification mechanisms, the proposed system enhances data security, integrity, and operational efficiency in modern digital forensic investigations.

## 2. PROPOSED SYSTEM

The proposed system introduces a secure and efficient digital forensic evidence management framework by integrating blockchain technology with advanced encryption mechanisms. The system is designed to overcome the

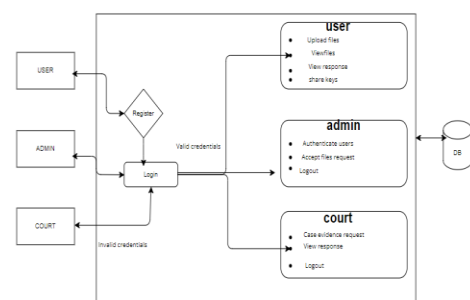
limitations of traditional forensic systems such as weak encryption, centralized storage, and lack of data integrity.

The core of the proposed model is the Digital Forensic Architecture using Authentication with Optimal Key Generation Encryption (DFA-AOKGE). This architecture ensures secure storage, transmission, and access of forensic evidence in a distributed cloud environment. The system utilizes blockchain technology to maintain an immutable and tamper-proof record of all evidence transactions, thereby enhancing trust and transparency. To strengthen data confidentiality, the system employs Multikey Homomorphic Encryption (MHE), which allows secure operations on encrypted data without exposing the original content. Additionally, an Enhanced Equilibrium Optimizer (EEO) is used for optimal key generation, ensuring stronger encryption keys and improved resistance against attacks. A Secure Block Verification Mechanism (SBVM) is integrated to validate all transactions within the blockchain network, ensuring data integrity and authenticity.

The proposed system is designed with three major modules: User (Forensic Investigator), Admin, and Court. Each module operates independently with role-based access control. Users can upload encrypted evidence, request access permissions, and share data securely with the court. The admin manages user authentication, monitors encryption processes, and controls access permissions. The court can request evidence files and decrypt them only after receiving authorized keys from users, ensuring controlled and secure data sharing. The integration of blockchain with cloud forensics provides decentralized storage, reducing the risks associated with single-point failures and unauthorized modifications. The system also supports secure communication through email notifications and key-based decryption, ensuring that only authorized entities can access sensitive information.

### A. System Architecture

The system architecture illustrates the interaction between different modules and the flow of encrypted forensic data across the platform. It consists of users uploading encrypted evidence to the cloud, blockchain maintaining transaction records, and the admin controlling authentication and key distribution. The court interacts with the system by requesting access to evidence and decrypting it using authorized keys.



**Fig 1: System Architecture of Proposed Digital Forensic System**

- Enhanced Security: Uses DFA-AOKGE with Multikey Homomorphic Encryption for strong data protection.
- Decentralization: Blockchain-based distributed storage prevents data tampering.
- Secure Access Control: Role-based modules for User, Admin, and Court.
- Data Integrity: Secure Block Verification Mechanism ensures authenticity of evidence.
- Efficient Key Management: Optimal key generation improves encryption strength.
- Scalability: Cloud integration supports large-scale forensic data storage and access.

### 3. IMPLEMENTATION DETAILS

The implementation of the proposed digital forensic evidence management system is carried out using a combination of web technologies, cloud storage, and advanced cryptographic techniques. The system is developed using Python and the Django framework, ensuring a scalable and secure web-based application. The system is implemented with the following hardware and software requirements:

Component	Specification
Processor	Intel i3 or higher
RAM	Minimum 8 GB
Storage	128 GB Hard Disk
Operating System	Windows 10
Programming Language	Python
Framework	Django
Frontend	HTML, CSS, Bootstrap, JavaScript
Database	MySQL
IDE	Visual Studio Code

### System Modules Implementation

The system is divided into three primary modules: User, Admin, and Court. Each module is implemented with specific functionalities to ensure secure and controlled access.

#### User Module (Forensic Investigator)

The user module allows investigators to register and log into the system after admin approval. Users can upload forensic evidence in encrypted format using secure encryption techniques. The uploaded data is stored in the cloud, and its transaction details are recorded in the blockchain. Users can request permission from the admin to share evidence with the court. Upon approval, users receive decryption keys, which can be securely shared with authorized entities.

#### Admin Module

The admin module acts as the central authority for monitoring and controlling system operations. Admins authenticate users, manage uploaded evidence, and oversee encryption and key generation processes. The admin also handles requests for data sharing and provides decryption keys to authorized users. This ensures that only verified users can access or share sensitive forensic data.

#### Court Module

The court module enables judicial authorities to securely access forensic evidence. Courts can request specific case files from users through the system. Once the request is approved and the decryption key is shared, the court can decrypt and view the evidence. This module ensures that legal authorities can access data in a secure and controlled manner.

### 4. RESULTS AND PERFORMANCE ANALYSIS

The proposed digital forensic evidence management system was implemented and tested to evaluate its performance in terms of security, functionality, and efficiency. The system integrates blockchain technology with advanced encryption techniques, ensuring secure handling of sensitive forensic data. The system successfully demonstrates all major functionalities through different modules. The user module enables registration, login, and secure uploading of evidence data in encrypted form. The uploaded data is stored securely and can be viewed or downloaded only in encrypted format. The admin module efficiently manages user authentication, monitors evidence data, and controls access permissions. The court module allows authorized legal entities to request and access evidence files securely.

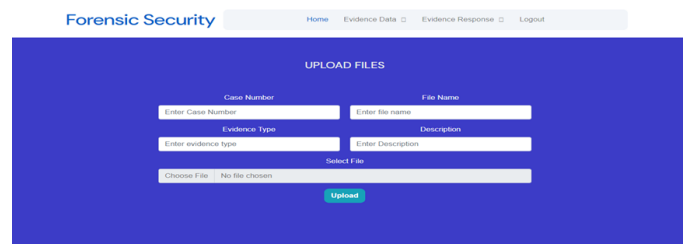


Fig - 2: Upload Files

The system ensures high-level security using Multikey Homomorphic Encryption and optimal key generation techniques. All evidence data is encrypted before storage, preventing unauthorized access. Blockchain technology guarantees immutability, ensuring that once evidence is stored, it cannot be altered. The Secure Block Verification Mechanism validates all transactions, maintaining data integrity.

Additionally, role-based access control ensures that only authorized users, admins, and courts can access specific functionalities. The use of decryption keys further enhances security, as evidence can only be accessed after proper authorization.

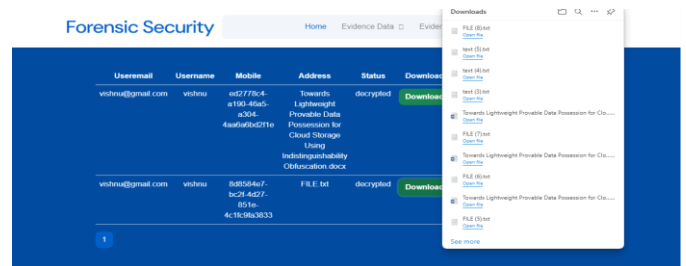


Fig - 3: Encrypted Data Storage and Download

The system demonstrates efficient performance in terms of response time and data handling. Encryption and decryption processes are executed with minimal delay, ensuring smooth user interaction. The integration of cloud storage improves scalability, allowing the system to handle large volumes of forensic data.

Compared to traditional systems using DES encryption, the proposed system provides significantly improved security and reliability. The decentralized nature of blockchain reduces risks of data loss and enhances system robustness.

Parameter	Existing System (DES)	Proposed System (DFA-AOKGE)
Security Level	Low	High
Data Integrity	Limited	Strong (Blockchain-based)

Parameter	Existing System (DES)	Proposed System (DFA-AOKGE)
Storage	Centralized	Decentralized
Encryption Strength	Weak	Advanced (MHE + Optimal Key)
Scalability	Limited	High (Cloud-based)

### 5. CONCLUSIONS

This paper presented a secure and efficient digital forensic evidence management system by integrating blockchain technology with advanced encryption techniques. The proposed DFA-AOKGE architecture effectively addresses the limitations of traditional systems, such as weak encryption, centralized storage, and vulnerability to data tampering. By utilizing Multikey Homomorphic Encryption and optimal key generation, the system ensures strong data confidentiality and secure processing of forensic evidence.

The incorporation of blockchain technology provides a decentralized and immutable environment, ensuring data integrity and transparency. The role-based modules for users, administrators, and judicial authorities enable controlled and secure access to sensitive information. Experimental results demonstrate that the proposed system significantly improves security, reliability, and scalability compared to existing approaches. Overall, the system offers a robust solution for modern digital forensic investigations, ensuring trustworthy evidence management and secure data sharing in cloud-based environments.

### 6. FUTURE WORK

Although the proposed system provides a secure and efficient framework for digital forensic evidence management, there are several areas for further enhancement. Future work can focus on improving scalability by integrating advanced distributed storage techniques such as InterPlanetary File System (IPFS) for faster and more efficient data retrieval. The system can also be enhanced by incorporating Artificial Intelligence and Machine Learning algorithms to automate evidence analysis and anomaly detection.

Additionally, implementing more advanced consensus mechanisms in blockchain can further improve transaction speed and reduce computational overhead. The integration of biometric authentication can strengthen user verification and access control. Future research may also explore cross-platform compatibility and mobile-based access for better usability. Furthermore, real-time monitoring and auditing mechanisms can be developed to enhance transparency and system performance in large-scale forensic environments.

### REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–19, 2016.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 2003–2026, 2017.

[4] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proc. ACM Symposium on Theory of Computing*, 2009, pp. 169–178.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[6] N. Kshetri, "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[7] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. CRC Press, 2014.

[9] E. Casey, *Digital Evidence and Computer Crime*, 3rd ed. Academic Press, 2011.

[10] K. R. Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers & Security*, vol. 30, no. 8, pp. 719–731, 2011.

[11] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[12] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," in *Advances in Cryptology (CRYPTO)*, 1987, pp. 369–378.

[13] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, 2020.

[14] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, 2011.

[15] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.