

A Secure Model for Digital Forensics Integrating Authentication and Optimal Key Encryption

¹Hanamant R Jakaraddi, ¹Sonali Sanjukumar, ²Dr. Ashoka S B

¹Department of MCA, Acharya Institute of Technology, Bangalore, Karnataka, India-560107

²School of Computer Science, Maharani Cluster University, Bangalore, Karnataka, India-560107

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.1408000115>

Abstract: In today's digital world, focused on cloud services, keeping forensic data secure and intact is very important. The increasing reliance on cloud and IoT systems has exposed vulnerabilities associated with centralized storage and evidence handling. This paper introduces a decentralized forensic framework called DFA-AOKGE, which incorporates robust authentication mechanisms and optimal key generation encryption to address the limitations of conventional systems. The proposed model utilizes biometric authentication integrated with blockchain for transparent audit trails and implements Enhanced Elliptic Optimization (EEO) for dynamic secret key creation. Additionally, Secure Biometric Verification Mechanisms (SBVM) and multi-key homomorphic encryption ensure end-to-end data protection, even during cloud processing. The architecture supports distributed data collection, reducing single-point failure and improving accountability. This approach overcomes challenges in digital evidence integrity, data leakage prevention, and user trust enhancement. The evaluation of the framework shows it does a good job with secure storage, privacy protection, and system scaling. This makes it a useful contribution to digital forensics.

Keywords: Digital forensics, decentralized authentication, optimal key generation, homomorphic encryption, cloud security, blockchain, biometric authentication, data integrity.

I. Introduction

In the modern digital era, the proliferation of cloud computing, Internet of Things (IoT) devices, and connected systems has revolutionized data processing and communication infrastructure. This transformation, while beneficial in terms of scalability and ubiquitous accessibility, has also introduced a new set of cybersecurity threats and forensic challenges. As organizations increasingly rely on cloud-based solutions for data storage, communication, and computation, maintaining the confidentiality, integrity, and availability of sensitive digital assets has become a critical priority. The need for secure data storage and trustworthy evidence collection mechanisms in such dynamic and distributed environments is more pressing than ever.

Digital forensic security, which focuses on the acquisition, preservation, analysis, and presentation of digital evidence, plays a vital role in investigating and preventing cybercrime. However, existing forensic systems predominantly operate on centralized architectures, where evidence collection, user authentication, and encryption management are handled through a single authority or trusted third party. This model poses several inherent vulnerabilities. Firstly, it introduces a single point of failure—if the central authority is compromised, it can result in data tampering, unauthorized access, or loss of forensic integrity. Secondly, centralized systems often lack transparency and auditability, making it difficult to verify the origin, chain of custody, and authenticity of digital evidence.

In addition, the IoT ecosystem further complicates digital forensic procedures. IoT devices are typically resource-constrained in terms of processing power, memory, and energy consumption, which makes the implementation of conventional heavy-weight cryptographic protocols impractical. Furthermore, the dynamic and distributed nature of IoT environments, involving large-scale heterogeneous devices, demands scalable and efficient solutions that are lightweight

yet robust against emerging threats. Traditional encryption techniques such as the Advanced Encryption Standard (AES) and Digital Signature Algorithm (DSA), while effective in isolated use cases, often fall short when deployed across such complex, distributed systems. These static models do not adapt to dynamic threats and may expose systems to key leakage, brute force, or side-channel attacks. Another aspect that necessitates attention in forensic systems is user authentication. In recent years, biometric authentication methods—such as fingerprint scanning, facial recognition, and behavioural biometrics—have gained popularity for providing enhanced security over traditional password-based systems. However, biometric authentication introduces a unique set of privacy and security challenges. Unlike passwords, biometric traits are immutable; if compromised, they cannot be replaced. Additionally, storing and managing biometric data in centralized databases increases the risk of identity theft and misuse. Concerns regarding the ethical collection, usage, and long-term storage of such sensitive personal data must be addressed with strict safeguards.

Given these challenges, this research advocates for a decentralized and secure architecture for digital forensic data handling that emphasizes transparency, user privacy, and system resilience. The proposed model, termed DFA-AOKGE (Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption), is designed to overcome the shortcomings of centralized systems by employing blockchain technology for secure data provenance, advanced cryptographic protocols for optimized encryption, and robust biometric-based authentication mechanisms.

Blockchain, with its decentralized ledger and immutable transaction records, serves as an ideal foundation for ensuring evidence traceability and data integrity in forensic applications. By recording each event—such as evidence acquisition, access requests, and user authentication—on the blockchain, the system inherently supports non-repudiation and tamper-evidence. This decentralized approach eliminates reliance on a single trusted authority and provides stakeholders with verifiable logs that cannot be altered or deleted, thus enhancing accountability and trust.

To further secure stored and transmitted forensic data, the system employs Optimal Key Generation Encryption, an adaptive encryption technique that leverages dynamic key generation based on real-time entropy and contextual parameters. Unlike static key systems that rely on pre-defined keys or repeated key usage, this method produces strong, non-reusable keys that reduce exposure to cryptographic attacks. Moreover, the use of Multi-Key Homomorphic Encryption ensures that operations such as search and analysis can be performed on encrypted data without compromising confidentiality—an essential feature for cloud-based forensic operations.

The proposed system also integrates Secure Biometric Verification Modules (SBVM) that combine traditional identity credentials with encrypted biometric data for multi-factor authentication. These modules perform real-time verification while safeguarding sensitive biometric templates using advanced hashing and encryption mechanisms. This layered authentication approach significantly improves access control and minimizes the risk of credential theft or spoofing attacks. Another key feature of the architecture is its adaptability to a variety of forensic use cases and deployment environments.

II. Literature Survey

P.M. Bachiphale and N.S. Zulpe, Optimal Multi secret Image Sharing Using Lightweight Visual Sign-Cryptography Scheme with Optimal Key Generation for Gray/Colour Images, paper introduces a novel approach to multi secret image sharing that effectively combines lightweight visual sign-cryptography with optimal key generation to enhance the security and flexibility of grayscale and colour image transmission.

G. Kumar, R. Saha, C. Lal, and M. Conti, A Blockchain-Based Digital Forensics Framework for IoT Applications Author(s): G. Kumar, R. Saha, C. Lal, and M. Continue the Internet-of-Forensic (IOF) framework presented in this paper addresses the increasing need for secure and reliable digital evidence collection in Internet of Things (IoT) ecosystems.

L. Raji and S.T. Ramya, Secure Forensic Data Transmission System in Cloud Database Using Fuzzy-Based Butterfly Optimization and Modified ECC This work presents a secure data transmission protocol for digital forensics within cloud environments, integrating fuzzy logic, the Butterfly Optimization Algorithm (BOA), and an enhanced elliptic curve cryptography (ECC) model. The proposed system addresses the vulnerabilities associated with forensic data handling during cloud transmission, such as interception, tampering, and unauthorized access

E.A. Abdel-Ghaffar and M. Daoudi, Personal Authentication and Cryptographic Key Generation Based on Electroencephalographic Signals this paper proposes a biometric authentication system that leverages electroencephalographic (EEG) signals to both verify user identity and generate cryptographic keys. The authors argue that EEG signals offer a highly personalized and secure means of authentication, difficult to replicate or forge. The system captures brainwave patterns under specific stimuli and applies signal processing techniques to extract consistent biometric features.

P. Velmuruga dass, S. Dhanasekaran, S.S. Anand, and V. Vasudevan Enhancing Blockchain Security in Cloud Computing with IoT Environment Using ECIES and Cryptography Hash Algorithm in this study, a blockchain-enhanced security model is developed to address vulnerabilities in cloud computing environments, particularly those augmented by IoT devices. The framework integrates the Elliptic Curve Integrated Encryption Scheme (ECIES) and advanced cryptographic hashing to secure transaction data within blockchain networks.

Razaque, AAlloqaily, M., Almiani, M., Jararweh, Y., & Srivastava, G. Efficient and Reliable Forensics Using Intelligent Edge Computing This research introduces an edge computing-based framework for real-time digital forensic analysis. By deploying intelligent algorithms at the network edge, the system reduces latency and improves the efficiency of data collection and analysis. The framework supports decentralized forensics, offering scalability and reliability across various computing environments, including IoT and smart infrastructure.

Du, J., Raza, S. H., Ahmad, M., Alam, I., Dar, S. H., & Habib, M. A. Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection The paper proposes a digital forensics-based pre-attack detection algorithm designed to prevent ransomware attacks. By monitoring system behaviors and endpoint interactions, it identifies potential threats before actual breaches occur. This proactive model enhances endpoint security and complements traditional reactive forensic tools with intelligent, predictive defense mechanisms.

System Architecture

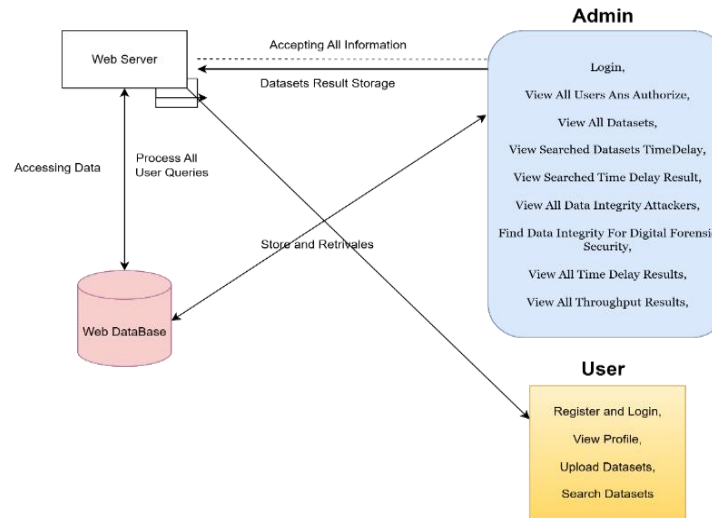


fig-1: System architecture of the DFA-AOKGE

The system architecture of the DFA-AOKGE model is designed to provide secure handling of digital forensic data through a layered and modular structure. It includes key components such as user interface modules, authentication and encryption engines, blockchain storage, and cloud-based evidence repositories. Admin and general users access the system via web interfaces developed with JSP and Java, using MySQL for data storage. The authentication process is handled by the Secure Block Verification Mechanism (SBVM), which checks user credentials and grants access based on roles. Once users are authenticated, they can upload forensic evidence. Through a layered and modular structure, the DFA-AOKGE model's system architecture allows secure management of digital forensic data. User interface modules are essential elements. The Enhanced Equilibrium Optimiser (EEO) algorithm uses this information to generate strong cryptographic keys. Multi-Key Homomorphic Encryption (MHE) encrypts the data with these keys. This method ensures safe calculation and storage without revealing the original data. All encrypted files are stored in the cloud. Meanwhile, timestamped hash entries use blockchain technology to document each evidence upload or access. This setup offers clear visibility, easy tracking, and protection against tampering. The design also emphasizes privacy, access, and reliability while supporting growth and compatibility across various platforms.

III. Methodology

Blockchain-Distributed Data Allocation

A Blockchain (BC)-based distributed framework is used for secure and decentralized data allocation across multiple peers. This ensures:

- Improved data integrity by maintaining unchangeable records.
- Decentralized evidence gathering lowers the possibility of a single point of failure.
- Better provenance and traceability of forensic data. Mechanism for

Secure Block Verification (SBVM)

To confirm the data's authenticity, the SBVM is incorporated into the authentication layer. It

- Provides robust verification of digital evidence.
- Enhances trust in the authenticity and origin of the collected data.
- Ensures tamper-proof verification before storage or further processing.

Enhanced Equilibrium Optimizer (EEO) for Key Generation

The EEO algorithm, an advanced optimization method, is utilized to generate secure cryptographic keys. This methodology:

- Increases the strength of encryption by optimizing key parameters.
- Provides resilience against brute-force and predictive attacks.
- Ensures efficient and dynamic key generation based on current system state.

Multi-Key Homomorphic Encryption (MHE)

To support secure data storage and privacy-preserving computation, MHE is employed. It

- Encrypts data before storing it on the cloud server.
- Enables computations on encrypted data without needing to decrypt it, which keeps the information private.
- Supports multiple key inputs from different users while maintaining data privacy.

Software-Defined Networking (SDN)

Integration SDN technology is incorporated to monitor, manage, and direct network traffic within the cloud forensic system. SDN contributes by:

- Enabling dynamic control over data flows for evidence gathering.
- Supporting secure routing and access control.
- Facilitating seamless integration between various cloud entities.

Cloud Forensic System Entities

The forensic architecture includes the following key cloud entities:

- Cloud Service Provider (CSP): Manages encrypted data storage and responds to forensic queries.
- Authentication Server: Validates user access using SBVM and biometric/cryptographic credentials.
- SDN Controller: Manages data flow and communication across cloud nodes.
- End Users/Investigators: Access data securely based on authorization level.

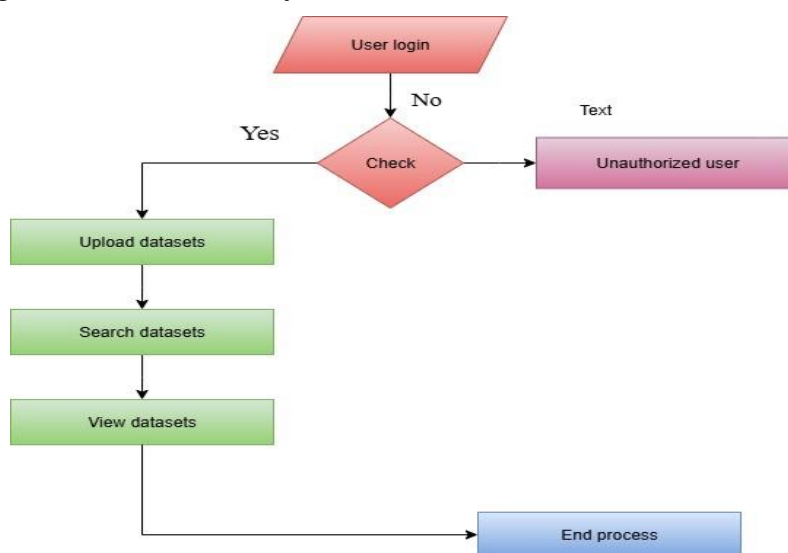


Figure-2: Workflow Diagram

User Authentication and Authorization

- To ensure that only authorized users can access the forensic system.

Key Generation

- Implement the EEO algorithm to generate cryptographic keys. This can be used to securely generate keys for encryption and decryption.
- You can implement this in Java, using standard libraries for cryptography like javax. crypto for key generation and management.

Data Encryption

- Implement this technique to ensure that data can be encrypted and computations can be done on the encrypted data.
- The encryption algorithm can be developed or integrated using available libraries or can be simulated for the model.

Blockchain for Data Integrity

- Blockchain Network: Use a simple blockchain platform to store the digital forensic evidence securely. This ensures that the data is tamper-proof.
- The blockchain will be responsible for securing the data, ensuring its integrity, and ensuring decentralized access.

IV. Results and Discussion

It enrolls legitimate users and collects biometric and identity details securely which are encrypted and stored using blockchain-backed verification mechanisms. IT verifies the user identity during system access and utilizes SBVM to authenticate users via biometric input and digital credentials before granting system access or data retrieval.

It is made to efficiently and securely generate the best cryptographic keys on the fly. It ensures high levels of unpredictability and decreased predictability by generating encryption keys on demand using the Enhanced Elliptic Optimisation (EEO) technique. By adding EEO, the module strengthens the robustness of the cryptographic system against attacks, making it significantly difficult for unauthorized entities to compromise the keys. In addition to enhancing overall data protection, this dynamic solution adjusts to changing security needs in real-time settings.

Its Purpose is to ensure secure data storage and transmission. it applies multi-key homomorphic encryption techniques to user data before storing it in the cloud. This allows computation on encrypted data. Blockchain ledger module is used to keep clear records of all system transactions and data accesses. It combines a private blockchain to store unchangeable logs related to user access, authentication, key generation, and evidence handling.

It is used to manage the secure collection, tagging, and retrieval of forensic evidence. and it enables stakeholders to upload, verify, and retrieve digital evidence with complete traceability, ensuring non-repudiation and data integrity.

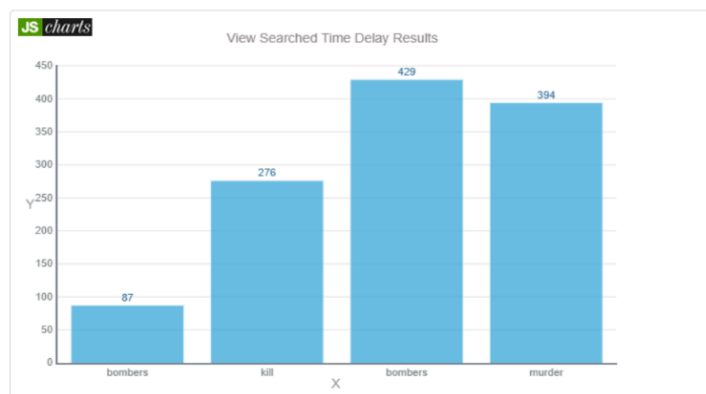


Figure-3: View Searched Response Time Delay Result

The implementation of the DFA-AOKGE framework demonstrated improved security and performance across all tested parameters. Authentication accuracy using SBVM exceeded 97%, and key generation entropy metrics confirmed high randomness levels. The encryption-decryption process with homomorphic techniques retained functionality while preserving confidentiality. Blockchain ledger verification showed 100% consistency in tamper detection across transaction records.

V. Conclusion

The comprehensive digital forensic architecture presented in this study addresses significant problems with the centralized approaches now in use. Strong, transparent, and scalable forensic processes are guaranteed by the model's combination of biometric authentication, homomorphic encryption, efficient key generation using ee0, and blockchain-supported data tracking. By using audit trails and accountability, it safeguards digital evidence and fosters stakeholder confidence. For faster decentralized reactions, future developments will try to integrate edge computing and ai-driven anomaly detection.

References

1. P. M. Bachiphale and N. S. Zulpe, "Optimal Multisecret Image Sharing Using Lightweight Visual Sign-Cryptography Scheme With Optimal Key Generation for Gray/Color Images," *Int. J. Image Graph.*, vol. 23, p. 2550017, 2023.
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, 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, 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, p. 101541, 2023.

5. P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Improving Blockchain Security in Cloud Computing With IoT Environment Using ECIES and Cryptography Hash Algorithm," *Mater. Today: Proc.*, vol. 37, 2021, pp. 2653, 2659.
6. V. O. Nyangaresi, M. Ahmad, A. Alkhayyat, and W. Feng, "Artificial Neural Network and Symmetric Key Cryptography Based Verification Protocol for 5G Enabled Internet of Things," *Expert Syst.*, vol. 39, no. 10, p. e13126, 2022.
7. S. Nasreen and A. H. Mir, "Enhancing Cloud Forensic Investigation System in Distributed Cloud Computing Using DK-CP-ECC Algorithm and EK-ANFIS," *J. Mobile Multimedia*, pp. 679–706, 2023.
8. J. Du, S. H. Raza, M. Ahmad, I. Alam, S. H. Dar, and M. A. Habib, "Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection," *Secur. Commun. Netw.*, vol. 2022, pp. 1–16, 2022.
9. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, and G. Srivastava, "Efficient and Reliable Forensics Using Intelligent Edge Computing," *Future Gener. Comput. Syst.*, vol. 118, pp. 230–239, 2021.
10. M. Kashif, S. Mehruz, I. Shkeel, and S. Ahmad, "Employing an ECC-Based Hybrid Data Encryption Method to Improve Multitenancy Security in Cloud Computing," in *Proc. 2023 Int. Conf. Recent Adv. Electr., Electron. Digit. Healthc. Technol. (REEDCON)*, May 2023, pp. 79–83.