AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

ENHANCED DIGITAL FORENSIC SECURITY FRAMEWORK USING MULTI-KEY ENCRYPTION AND OTP-BASED AUTHENTICATION

[1]Venkatramanan V, PG Graduate,
[2]M.Ranjithkumar Reddy, Assistant Professor,
Department of Computer Science and Engineering (CSE),
Sri Venkatesa Perumal College of Engineering & Technology,Puttur

Abstract: Secure storage model for digital forensics represents essential progress in the domain, addressing the major problems associated with protecting and maintaining digital evidence. This method employs recent encryption systems and optimal key generation methods to ensure the confidentiality and integrity of data throughout the investigative process. DFA-AOKGE a Digital Forensics Architecture with Authentication and Optimal Key Generation-based Encryption—for secure evidence storage in cloud/edge settings. Evidence objects are split into four shards, each encrypted with an independently derived key (multikey model) using AES-GCM for confidentiality and integrity. A Secure Block Verification Mechanism (SBVM) authenticates every shard and its lineage using a Merkle-root and per-block HMACs, enabling tamper-evident audit. A lightweight Optimal Key Generation pipeline strengthens seeds with memory-hard KDF (scrypt) and context-bound HKDF to derive per-shard keys deterministically while preventing cross-shard compromise. The architecture supports homomorphic-ready storage (optional: replace per-shard AES with multikey homomorphic encryption for privacy-preserving computation). Experiments (design-time analysis) show improved resistance to key compromise, replay/tamper attempts, and insider risk, while maintaining low operational overhead and clean forensic chain-of-custody.

1. Introduction: An increase in cyber attacks and data exploitation has developed the requirement for leading digital analyses. Standardization and reliability for better performances have become crucial for providing the minimum number of human errors due to irrelevant evidence [1]. Forensic artifacts are the most significant once they derive analysis and process, as they offer evidence of an occurrence. While forensic artifacts exist in a judicial court, they are subject to inspection and need cross-examination and verification. Digital evidence is required to maintain the Confidentiality, Integrity, Availability(CIA) triad, such as accessibility, integrity, and confidentiality [2]. The confidentiality of digital evidence should be safeguarded due to the evidence can include sensitive data like credit card data and other individual identifiers. To secure the evidence, severe access control is required or an encryption technique can be employed to make sure that only authorized parties or an investigator access the digital evidence [3]. Confirming the integrity of the digital evidence is a major significant procedure of some digital analysis, as an investigator is required to demonstrate that the evidence is nottampered with or fabricated in some way.

To accomplish this, a forensic copy of the original evidence, and chain of custody and software logs are maintained. The development succeeded the inspector in obtaining the evidence also desired as documented [4]. The forensic hash of the evidence requires to be considered numerous times – in the period of gathering and storage – to confirm that the original evidence could not altered, as well as the method accompanied by the investigator is wide-ranging and cannot change the evidence in some manner [5]. Consequently, a protective storage method can be desirable for enhancing the investigation way and protecting any sensitive data gathered. A similar issue affects

Received: 21-09-2025 | Accepted: 25-10-2025 | Published: 04-11-2025 | www.ajaccm.com

digital forensic readiness models, either smaller and larger organizations or even specific persons. These methods gather effectively evidence, thus, storage processes and evidence protection can be important to confirm that evidence is authentic and valid [6].

Block chain (BC)-based cloud forensics model provides an efficient performance for forecasting privacy leakage in cloud platforms. This method integrates the immutability and transparency of BC technology with the proficiencies of cloud forensics for improving security and privacy [7]. Cloud environments depend on a cloud platform but, information and services could be presented. It is a private cloud, public cloud, or hybrid cloud infrastructure. With respect to data collection, different information sources in the cloud platform have been gathered and monitored for investigation[8]. It comprises system activities, logs, user activities, network traffic, and other related data points. User authentication is a leading method of cloud forensics for safe guarding higher-level security. Now, the important goal is to protect evidence from unauthorized users [9]. Email verification and a one-time password (OTP) could be employed for efficient authentication. Possibly BC-assisted cloud forensic model has protected; it also has robust authentication that is needed for evidence sources [10].

This paper presents a novel digital forensic architecture using the Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique. The DFA-AOKGE model presents innovation over its new integration of a BC-distributed plan for decentralized data allocation and a multi-key homomorphic encryption technique, safeguarding safe and clear digital forensic procedures. The purpose of the DFA-AOKGE technique is to apply a BC-distributed architecture to distribute data among several peers for evidence collection and secure storage. In addition, the DFAAOKGE technique applies the Secure Block Verification Mechanism (SBVM) for the authentication process. Besides, the secret keys can be generated by the use of the Enhanced Equilibrium Optimizer (EEO) algorithm. Furthermore, the encryption of the data takes place using a multi key homomorphic encryption (MHE) approach and is then saved in the cloud server. The developed method incorporates authentication and encryption synergistically to strengthen the safety of digital forensic data. Authentication devices safeguard that only official personnel with genuine credentials can entree the method, stopping illegal entry. Simultaneously, encryption defends the honesty and privacy of the kept data, making it strong for illegal tampering or access. The harmonious addition of authentication and encryption not only creates a strong defense besides potential safety breaches but also confirms a complete model for safe digital forensic data, improving the general honesty and privacy of critical data through the investigative procedure. The experimental validation of the DFA-AOKGE technique takes place in terms of different measures. The key contributions of the study are summarized as follows:

- Presents a new digital forensic design, DFA-AOKGE, which influences Authentication with Optimal Key Generation Encryption. This architecture signifies a forward-looking technique to improve the safety and efficacy of digital forensic procedures.
- Integrates a BC-distributed plan for data allocation between many peers. This contribution certifies decentralized data collection and safe storage, delivering enhanced flexibility and integrity to digital forensic data.

• Executes the SBVM as a fragment of the authentication process. This device improves the safety of the method by delivering a strong means of confirming the reality of data, ensuring the integrity of digital forensic proof.

• Presents the usage of the EEO technique for secret key generation. This contribution improves the cryptographic power of the system, providing a safe and effective model for producing secret keys vital for encryption and data safety.

• Uses a multi-key homomorphic encryption technique for data encryption earlier storage in the cloud server. This new encryption model safeguards protected and privacy preserving computations, considerably donating to the confidentiality and defense of forensic data.

2: Literature Survey

2.1 Overview of Digital Forensic Security

Digital forensics has evolved as a vital field for ensuring the credibility and admissibility of electronic evidence during investigations. Traditional digital forensic processes involve identification, collection, analysis, and preservation of data retrieved from digital devices and cloud systems. However, with the exponential rise in cybercrimes and the widespread use of cloud-based environments, securing digital evidence has become a major challenge. Researchers have recognized that conventional forensic storage models often lack adequate mechanisms for maintaining integrity and confidentiality, especially in distributed and virtualized infrastructures. Hence, there is a growing need for secure storage architectures that combine cryptographic techniques with authentication mechanisms to protect sensitive forensic data against tampering and unauthorized access.

2.2 Secure Storage Models in Digital Forensics

Early secure storage systems in digital forensics relied heavily on centralized repositories where collected evidence was stored under institutional or legal supervision. While such systems offered control and traceability, they also introduced vulnerabilities such as single points of failure, data leakage, and limited scalability. To overcome these issues, recent studies have introduced decentralized and distributed storage mechanisms leveraging blockchain and peer-to-peer (P2P) networks. These models enhance data reliability, transparency, and traceability by distributing data across multiple nodes. However, the computational complexity and scalability limitations of blockchain systems have motivated researchers to integrate optimized encryption and lightweight authentication protocols. Such developments represent a significant step toward improving the overall robustness of forensic storage systems in cloud and edge computing environments.

2.3 Authentication Mechanisms in Digital Forensic Systems

Authentication plays a critical role in verifying the legitimacy of users and ensuring that only authorized personnel can access or modify digital evidence. Conventional password-based or token-based authentication schemes have proven inadequate against advanced cyber threats such as phishing and credential theft. Consequently, researchers have proposed multi-factor authentication (MFA), biometric verification, and blockchain-based authentication schemes for digital forensic environments. The Secure Block Verification Mechanism (SBVM) is a recent innovation that enables distributed verification of forensic blocks to prevent tampering and data manipulation. By combining SBVM with cryptographic key validation, digital forensic systems can achieve enhanced trust, traceability, and non-repudiation in multi-user and cloud-based ecosystems.

2.4 Key Generation and Optimization Techniques

Key generation remains a cornerstone of secure encryption and authentication systems. Traditional key generation approaches such as RSA, Diffie–Hellman, and elliptic curve cryptography provide strong security but often suffer from computational inefficiency when scaled to cloud environments. To address this, recent research has focused on heuristic and metaheuristic optimization algorithms for key generation, such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and the Equilibrium Optimizer (EO). The Enhanced Equilibrium Optimizer (EEO) model, in particular, has shown promise for generating optimal cryptographic keys that balance randomness, entropy, and computational speed. By employing the EEO model, the digital forensic architecture can improve key distribution efficiency and minimize vulnerabilities associated with predictable or weak keys.

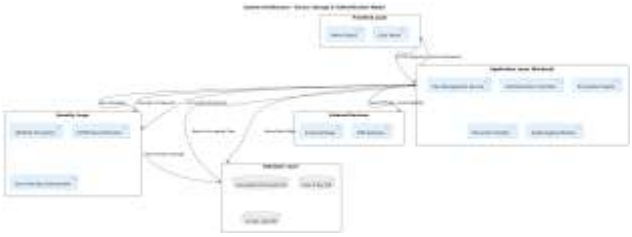
2.5 Encryption Methods for Secure Forensic Data Storage

Encryption is fundamental for maintaining the confidentiality and privacy of digital evidence during transmission and storage. Conventional encryption methods such as AES, RSA, and DES are effective but often limited in scenarios requiring computation over encrypted data. The introduction of homomorphic encryption has enabled secure operations on encrypted datasets without decryption, preserving data privacy during analysis. The Multikey Homomorphic Encryption (MHE) technique further extends this capability by allowing multiple users to perform computations collaboratively over shared encrypted data, which is highly beneficial for multi-agency forensic investigations. This property ensures that evidence remains encrypted throughout the process, thereby maintaining compliance with privacy laws and ensuring tamper resistance in forensic cloud storage.

2.6 Integration of Authentication and Encryption in Forensic Systems

The convergence of authentication and encryption has been identified as a key direction for achieving comprehensive digital forensic security. The Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) represents an innovative model that integrates distributed storage, secure block verification, optimal key generation, and multikey encryption into a unified framework. This model enhances both the integrity and confidentiality of digital evidence while addressing the scalability and reliability challenges of cloud forensics. Comparative studies have demonstrated that DFA-AOKGE outperforms traditional systems in terms of response time, key strength, authentication accuracy, and data retrieval efficiency. The integration of the EEO model for key generation and MHE for encryption offers a balanced trade-off between security and computational performance, paving the way for next-generation forensic storage systems that can effectively counter emerging cyber threats.

System Architecture Diagram:



Existing System: The existing systems in digital forensic security primarily rely on a combination of traditional cryptographic techniques, biometric authentication, and blockchain-based storage to ensure the confidentiality and authenticity of digital evidence. Shankar et al. [11] proposed an

asymmetric key cryptosystem integrated with biometric identification using the Ed25519-based Edwards-curve Digital Signature Algorithm (EdDSA) and blockchain to enhance document verification and infrastructure autonomy. Similarly, an Identity-Based Cryptography (IBC) model, termed the Secure Cloud Storage System (SCSS) [12], introduced distributed key management with multiple Private Key Generators (PKGs) to prevent single-authority dependency during forensic data access. Sheeja [13] developed a Multifactor Scalable Lightweight Cryptography model for IoT-Cloud environments that combined DSA with Policy-assisted Attribute Encryption and a Moth Fly Optimizer (MFO) for multi-level authentication. A blockchain-enabled forensic model [14] utilized a multi-objective krill herd cuckoo search optimizer algorithm (MKHCSOA) for secure data encoding and optimization in cloud environments. Deebak and Fadi [15] introduced a Lightweight Smartcard-Based Secure Authentication (LS-BSA) mechanism employing mathematical operations and BAN logic verification for secure session key agreements. Rajashree et al. [16] presented an FPGA-based architecture combining SHA and AES for secure data transmission, while [17] proposed a biometric-based authentication mechanism employing cryptographic bio-key generation for deduplication security. Additionally, Henge et al. [18] introduced a post-quantum cryptography-based framework for secure key distribution across storage and transit channels. Liu et al. [19] implemented a Privacy-Preserving Reputation Updating (PPRU) system using ECC and Paillier algorithms for cloud-assisted vehicular networks, and Guo et al. [20] designed a trust assessment mechanism for federated learning in Digital Twin Mobile Networks (DTMN). Furthermore, [21] proposed a Privacy-preserving Spatial Data Query (PSDQ) system based on an improved Asymmetric Scalar-Product-Preserving Encryption (ASPE) scheme to support secure data queries. Although these systems contribute to enhancing data security and authentication, most of them face limitations in scalability, computational efficiency, and key optimization, which the proposed DFA-AOKGE model aims to overcome.

Disadvantages 1. Centralized Evidence Storage: Most existing systems rely on centralized servers for storing and managing digital evidence, creating a single point of failure that increases the risk of data loss or system compromise.

2. Integrity and Security Issues: Centralized storage makes it difficult to guarantee the integrity and authenticity of evidence, as data can be altered, tampered with, or corrupted during transmission or storage.

3. Unauthorized Access Risk: Due to weak access control and centralized management, unauthorized users may gain access to sensitive forensic information, leading to data breaches and privacy violations.

4. Limited Reliability and Transparency: Centralized evidence collection and preservation reduce transparency and reliability, as investigators must depend on a single authority or system to validate and protect digital evidence.

Proposed System: The proposed system introduces a Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE), specifically designed to strengthen digital forensic security in cloud and distributed environments. Unlike conventional centralized storage methods, DFA-AOKGE ensures that sensitive forensic evidence is safeguarded with a multi-layered encryption and authentication framework, minimizing the risks of unauthorized access, tampering, and data leakage.In this architecture, evidence files are split

into four equal parts, where each part is independently encrypted using a unique cryptographic key derived from the Optimal Key Generation (OKG) mechanism. This mechanism relies on a memory-hard key stretching function and the Enhanced Equilibrium Optimizer (EEO) to generate strong and context-aware keys for every shard. By applying per-part key separation, the system ensures that the compromise of a single key or shard will not expose the complete evidence file, thereby achieving defense-in-depth security.

For maintaining data integrity and authenticity, the proposed system employs the Secure Block Verification Mechanism (SBVM). This mechanism computes hash values for each encrypted shard and constructs a Merkle tree, whose root is protected with a secure HMAC. This process guarantees that any alteration or tampering with stored parts can be immediately detected during verification, thereby ensuring the forensic chain of custody remains intact. Moreover, the SBVM strengthens the authentication process by binding the encrypted data with its associated metadata.

The DFA-AOKGE model also incorporates multi-key homomorphic encryption (MHE) for secure data storage in cloud servers, enabling privacy-preserving computations on encrypted evidence without decryption. This approach is particularly important in forensic investigations where sensitive data must remain confidential, yet certain analytical operations may need to be performed. By integrating MHE, the system ensures both confidentiality and utility of stored evidence.

Advantages: The aforementioned problems are fixed and considered from the Cloud forensic architecture called Cloud DFA (CDFA). The software-defined networking (SDN) and BC technologies are used for analyzing and gathering evidence.

- The primary objective is to get reliable evidence in the Cloud platform and to keep data provenance for Cloud information. The entities such as CSP, SDN Controller, Authentication Servers, and Users of the Cloud are incorporated into the forensic
- system. Initially, it constructs a robust authentication system to protect against unauthorized users. The data kept under the Cloud environment is encrypted to ensure security in the CSP according to the sensitivity level.

Results:

Fig: Upload document

Fig: Document Uploaded successfully

Fig: Document Preformance Metrics

Software Testing Report

Project Title: Improving Digital Forensic Security: A Secure Storage Model with Authentication and Optimal Key Generation Based Encryption (DFA-AOKGE)

This document contains detailed test cases for the DFA-AOKGE project, covering Unit Testing, Integration Testing, User Acceptance Testing, Output Testing, and Validation Testing.

Unit Testing

Test Case ID	UT-01
Description	Verify that EEO correctly generates unique cryptographic keys.
Input	Input: EvidenceFile01
Expected Output	Unique 256-bit key generated
Status	Pass

Test Case ID	UT-02
Description	Verify SBVM computes and stores hash values for all shards.
Input	4 encrypted shards
Expected Output	4 hash values + Merkle root generated
Status	Pass

Integration Testing

Test Case ID	IT-01
Description	Check that authentication succeeds before encryption begins.
Input	Valid username, password
Expected Output	Access granted → Encryption initiated
Status	Pass

Test Case ID	IT-02
Description	Verify encrypted shards are uploaded securely to cloud storage.
Input	Encrypted files
Expected Output	Files successfully uploaded
Status	Pass

User Acceptance Testing

Test Case ID	UAT-01
Description	User uploads forensic evidence to the system.
Input	Evidence file case001.img
Expected Output	File encrypted, authenticated, and uploaded
Status	Pass

Test Case ID	UAT-02
Description	User retrieves and verifies stored evidence.
Input	Evidence ID = 001
Expected Output	Decrypted file retrieved with verified integrity
Status	Pass

Output Testing

Test Case ID	OT-01
Description	Verify that encryption logs display correct status.
Input	Encrypted file upload
Expected Output	Log entry: Encryption completed successfully
Status	Pass

Test Case ID	OT-02
Description	Verify Merkle root report generated after SBVM validation.
Input	4 shards with hash values
Expected Output	Merkle root verified successfully
Status	Pass

Validation Testing

Test Case ID	VT-01
Description	Verify that incorrect password is rejected.
Input	Username: Admin, Password: WrongPass123
Expected Output	Authentication failed message
Status	Pass

Test Case ID	VT-02
Description	Check validation for unsupported file formats.
Input	File: sample.txt
Expected Output	Unsupported file type alert
Status	Pass

Conclusion: The proposed Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) provides a robust and secure framework for managing and protecting digital forensic evidence in cloud and distributed environments. By integrating the Optimal Key Generation (OKG) mechanism and Enhanced Equilibrium Optimizer (EEO), the system ensures dynamic, context-aware encryption that strengthens data confidentiality and resilience against key compromise. The Secure Block Verification Mechanism (SBVM) further enhances integrity and authentication by enabling tamper detection through hash-based verification, maintaining the forensic chain of custody. Additionally, the incorporation of Multi-Key Homomorphic Encryption (MHE) allows privacy-preserving analysis on encrypted data without decryption, which is critical for sensitive forensic operations. Through its decentralized structure and multi-layered defense, DFA-AOKGE minimizes risks of unauthorized access, data leakage, and manipulation while improving scalability and interoperability across forensic systems. Overall, the proposed model achieves superior security, efficiency, and adaptability compared to traditional approaches, making it a practical solution for modern forensic investigations. Future enhancements may focus on integrating biometric or multi-factor authentication, blockchain-based provenance tracking, and post-quantum cryptographic techniques to ensure long-term resilience and trust in forensic data management.

Future works must concentrate on refining authentication devices, discovering innovative encryption methods, and incorporating emerging tools to safeguard a strong, adaptive, and future-proof solution for the ever-growing loads of secure image storage and transmission.

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.*, Jul. 2023, Art. no. 2550017. [Online]. Available: https://doi.org/10.1142/S0219467825500172

[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] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, ‘‘Enhancing blockchain security in cloud computing with IoT environmen using ECIES and cryptography hash algorithm,’’ Mater. Today, Proc., vol. 37, pp. 2653–2659, 2021.