STM JOURNALS

Journal of
Control & Instrumentation

ISSN: 2229-6972 (Online)
ISSN: 2347-7237 (Print)
Volume 17, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoCI

https://journals.stmjournals.com/joci

Review JoCI

A Secure Storage Model with Authentication and Optimal Key Generation Based Encryption

R. Sasikala, M.E.[1], Maharaja M.[2,*], Mukesh M.[3], Nithish Kumar V.[3], Vidyadharan K.[3]

Abstract

In digital forensics, ensuring the secure storage of digital evidence is crucial. This paper introduces a new method that uses advanced encryption and key generation techniques to protect digital evidence throughout an investigation. Cloud forensics, a modern approach to digital forensics, aims to safeguard evidence from online hacking. However, storing all evidence in one central location can reduce its reliability. To address this, we propose a digital forensics architecture for cloud platforms, specifically infrastructure as a service (IaaS). In the DFA-AOKGE concept, a secure block verification mechanism (SBVM) is used to accomplish authentication. An enhanced equilibrium optimizer (EEO) model is used to generate secret keys, and a multikey homomorphic encryption (MHE) approach is used to guarantee data secrecy before cloud storage. The suggested DFA-AOKGE method beats current state-of-the-art techniques on a number of performance parameters, according to experimental simulations. The DFA-AOKGE architecture is specifically designed to simplify and enhance the processes of digital evidence collection, storage, and protection while ensuring the preservation of evidence integrity and provenance throughout the forensic lifecycle. By maintaining a verifiable chain of custody and preventing unauthorized modifications, the architecture strengthens the trustworthiness and legal admissibility of digital evidence in cloud computing environments. This architecture is designed to make it easier to collect and protect digital evidence while maintaining its integrity and origin in cloud computing environments. Our approach, called DFA-AOKGE (Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption), uses a decentralized system to distribute data across. For authentication, the DFA-AOKGE model uses SBVM. It also generates secret keys using an EEO model. Data is encrypted using an MHE method and then stored on the cloud server. Simulations show that the DFA-AOKGE method outperforms other recent approaches in various performance measures.

Keywords: Digital forensics, cloud forensics, secure evidence storage, multikey homomorphic encryption, decentralized forensic architecture

***Author for Correspondence**
Maharaja M.
E-mail: 717821y125@kce.ac.in

[1]Faculty, Department of Computer Science Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India
[2]Head, Department of Computer Science Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India
[3]Student, Department of Computer Science Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

Receiving Date: June 16, 2025
Accepted Date: February 06, 2026
Published Date: March 18, 2026

Citation: R. Sasikala, M.E., Maharaja M., Mukesh M., Nithish Kumar V., Vidyadharan K. A Secure Storage Model with Authentication and Optimal Key Generation Based Encryption. Journal of Control & Instrumentation. 2026; 17(1): 7–13p.

INTRODUCTION

In today's digital landscape, the security and integrity of digital evidence in cloud computing environments have become a critical challenge. Traditional centralized storage methods, though widely used, are increasingly vulnerable to cyber threats, including unauthorized access, data breaches, and manipulation [1]. These vulnerabilities compromise the reliability and admissibility of digital evidence in legal and investigative contexts. Cloud forensics has emerged as a modern extension of digital forensics, aiming to address these challenges by enabling the secure handling of evidence within cloud computing environments. However, many existing

cloud forensic solutions still depend on centralized evidence storage, which introduces single points of failure and limits scalability, reliability, and fault tolerance. Moreover, conventional encryption and key management mechanisms, although effective in protecting data confidentiality, often fail to meet the dynamic, scalable, and distributed requirements of cloud-based infrastructure as a service (IaaS) platform [2]. Numerous cloud forensic solutions now in use still rely on architectures for centralized evidence storage. Furthermore, a sizable portion of the cloud forensic systems that are already in use still depend on infrastructures for centralized evidence storage. Centralized architecture naturally introduces single points of failure that can significantly impair system availability, reliability, and resilience, even though they make administrative control, monitoring, and evidence management simpler [3]. Centralized storage systems are more susceptible to data loss, extended downtime, and illegal evidence modification in the event of cyberattacks, insider threats, hardware problems, or unplanned service interruptions (Figure 1). These flaws pose severe questions about the reliability and admissibility of digital evidence in judicial and investigative proceedings, in addition to endangering its availability and integrity. Centralized models create single points of failure by design, which can seriously impair system availability and reliability even though they make management and control easier. Centralized storage systems are particularly susceptible to data loss and extended downtime in the event of cyberattacks, hardware malfunctions, or service interruptions [4]. Additionally, as forensic data quantities rise, centralized methods become less effective at scaling, which restricts their use in expansive, dispersed cloud systems. These restrictions make it more difficult to offer continuous and safe access to digital evidence in dynamic cloud infrastructures and lower fault tolerance. The advancement of encryption techniques and secure key management has improved data protection, but existing methods often fail to address the scalability and dynamic requirements of cloud-based IaaS platforms [5]. We suggest a digital forensic design for cloud platforms, notably IaaS, to get over this restriction. The suggested architecture maintains the integrity and provenance of digital evidence in cloud computing settings while enabling effective evidence collection and safe storage. We propose a decentralized structure for data gathering and safe storage, which we call DFA-AOKGE (Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption) [6]. A robust storage model is needed to ensure secure collection, storage, and access control while maintaining data authenticity and confidentiality. This work proposes a secure storage model that integrates authentication mechanisms with optimal key generation based encryption techniques, aiming to enhance the overall security framework for digital evidence management in cloud environments.

CONTRIBUTION

This study focuses on transforming the way digital evidence is collected, stored, and authenticated in cloud environments. The key areas of focus include the following.

Development of a Decentralized Architecture

- Leverages distributed systems to prevent centralized vulnerabilities.
- Ensures redundancy and resilience in case of node failure.

Advanced Encryption Techniques

- Multikey homomorphic encryption (MHE) is used to encrypt data such that computations can be performed on encrypted data, ensuring confidentiality.

Optimized Key Management

- Introducing the enhanced equilibrium optimizer (EEO) for dynamic and secure key generation, addressing weaknesses.

Comprehensive Authentication

- Implements a secure blockchain verification mechanism (SBVM) to verify the origin and integrity of each block of evidence.

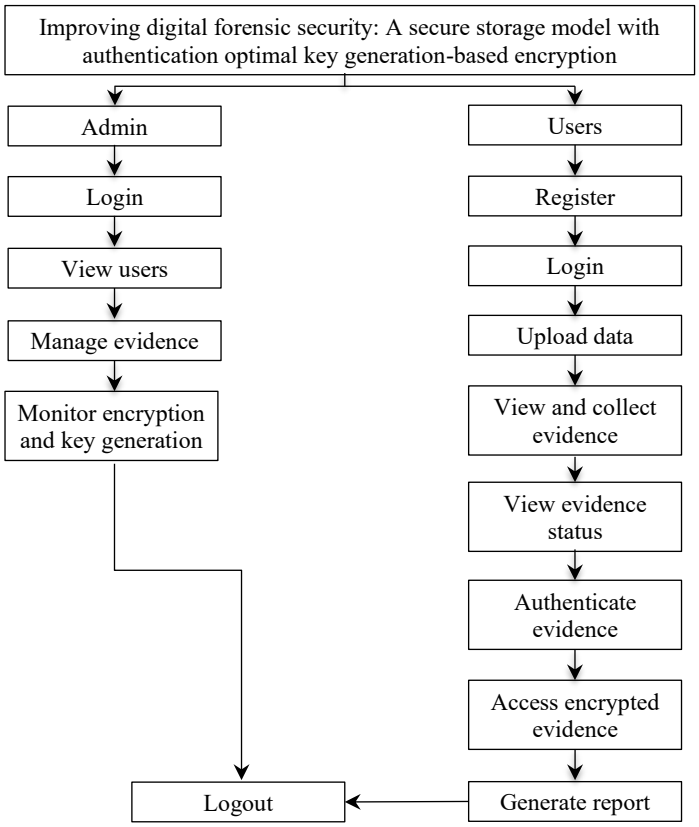

Figure 1. Secure digital forensic evidence management workflow for admins and users

Cloud-Specific Focus

- Tailored to IaaS platforms, which represent a significant portion of enterprise cloud usage.

Simulation and Benchmarking

- Evaluate the system's effectiveness in handling real-world forensic challenges through simulations.

This study addresses the gaps in current forensic systems, laying the foundation for future research in cloud forensics.

LITERATURE SURVEY

To improve the security of digital evidence in cloud computing settings, a cloud forensic framework has been developed that combines sophisticated encryption methods with extensive access control measures. In distributed and multi-tenant cloud infrastructures, the framework concentrates on tackling the main security issues related to gathering, storing, and handling forensic data. The strategy attempts to prevent unwanted access to sensitive forensic data while guaranteeing that only authorized and authenticated organizations can engage with the evidence during an investigation by combining encryption with stringent access control restrictions. The framework places a lot of focus on keeping the digital evidence's chain of custody trustworthy and verifiable. Maintaining the integrity of evidence becomes very difficult in cloud environments where data may be moved, replicated, or accessed across several virtualized resources on a dynamic basis [7]. To guarantee that every action taken on the evidence is accurately documented and verifiable, the framework emphasizes the necessity of secure logging, traceability, and accountability procedures. These steps are essential for maintaining the admissibility of digital evidence in court and legal procedures, as well as for building confidence in forensic conclusions. The framework also notes that one major worry with cloud-based forensic tools is the possibility of illegal data exposure and alteration. Cloud environments are more vulnerable to external cyberattacks and insider threats due to multi-tenancy, shared resources, and

remote access. The framework recommends the use of digital signature systems and cryptographic technologies like Public Key Infrastructure (PKI) to reduce these concerns. Digital signatures provide for data integrity verification and proof of origin confirmation, while PKI facilitates secure authentication, key distribution, and access verification [8].

Outlier and anomaly detection are crucial for improving the security of digital forensic systems, especially in cloud computing settings, according to recent studies. Finding unusual patterns of behavior that can lead to illegal attempts, data manipulation, or other harmful activity aimed at digital evidence requires the use of outlier detection tools. Detecting sophisticated or previously undiscovered attack patterns is typically a challenge for traditional rule-based security procedures in highly dynamic and distributed cloud infrastructures. Consequently, anomaly detection has become an essential part of enhancing proactive threat detection and forensic preparedness [9]. The use of machine learning techniques has been widely suggested as an effective approach for monitoring network traffic, system logs, and user activities in real time. Machine learning models can analyze large volumes of data generated within cloud environments to establish baseline behavior patterns and identify deviations that may signal potential security breaches. By continuously learning from historical and real-time data, these techniques can adapt to evolving threat landscapes and improve detection accuracy over time. This capability is particularly valuable in cloud-based systems, where workloads, user behavior, and resource configurations frequently change. The application of machine learning techniques has been extensively recommended as a successful method for real-time monitoring of user activity, system logs, and network traffic [10]. Large amounts of data produced in cloud environments can be analyzed by machine learning algorithms to create baseline behavior patterns and spot variations that might indicate possible security breaches. These methods can adjust to changing threat environments and gradually increase detection accuracy by continuously learning from both historical and real-time data. In cloud-based systems, where user behavior, workloads, and resource configurations are constantly changing, this functionality is very beneficial. Additionally, early detection of suspicious activity that can jeopardize the confidentiality and integrity of digital evidence is made possible by machine learning based anomaly detection. Unusual data transfer volumes, odd access frequency, or sudden shifts in storage habits, for instance, can be identified as possible signs of evidence manipulation or infiltration. By identifying these irregularities early on, forensic systems can start the right reaction processes, such as limiting access, isolating evidence, or creating alerts, reducing possible harm, and maintaining the accuracy of forensic data. These observations are in line with the suggested forensic model's incorporation of machine learning methods for security monitoring and anomaly identification in real time. The approach improves its capacity to protect digital evidence from internal threats as well as external attacks by integrating clever anomaly detection algorithms. In addition to enhancing overall system resilience, this proactive security technique helps to maintain a reliable chain of custody. As a result, in contemporary cloud-based forensic investigations, the use of machine learning-driven anomaly detection greatly enhances the efficacy, dependability, and admissibility of digital evidence.

A hybrid cryptographic approach that integrates symmetric and asymmetric encryption algorithms has been suggested to maximize their respective benefits and minimize their drawbacks. This integrated approach works especially well in settings such as cloud-based digital forensic systems, where massive amounts of sensitive data must be handled securely and effectively. This strategy seeks to strike a compromise between robust security guarantees and high performance by combining the two encryption paradigms. The minimal processing overhead and computational efficiency of symmetric encryption make it the preferred method for encrypting large amounts of data. Large datasets that are frequently encountered in forensic investigations can be handled with ease, thanks to algorithms such as the advanced encryption standard (AES), which allows for quick encryption and decryption processes. Symmetric encryption guarantees that digital evidence can be safely transferred and stored without materially affecting the scalability or performance of the system. This efficiency is particularly crucial in cloud systems, where forensic data volumes can grow quickly and necessitate real-time or near-real-time processing. However, symmetric encryption alone makes safe key

distribution and administration more difficult, especially in dispersed and multi-tenant cloud infrastructures. Asymmetric encryption methods are used to handle and safeguard cryptographic keys to overcome these difficulties. Public key based systems enable access control, authentication, and secure key exchange, eliminating the need for parties to directly exchange secret keys. The method adds an extra degree of security against key compromise and unwanted access by encrypting symmetric keys using asymmetric encryption. By guaranteeing that the keys required for decryption are safely stored even if encrypted data are intercepted, the combination of symmetric and asymmetric encryption improves overall system security. Authorized forensic investigators can securely share evidence and increase resistance to cryptographic attacks using this layered security paradigm. Furthermore, by providing strong access control, accountability, and non-repudiation procedures, hybrid encryption systems can improve adherence to security and regulatory requirements. Therefore, in contemporary cloud-based forensic systems, the combination of symmetric and asymmetric encryption offers a workable and efficient option for safe, scalable, and reliable digital evidence management in the cloud.

METHODOLOGY

User (Forensic Investigator) Modules

Login

- Ensures only authorized personnel can access the system, preventing unauthorized access.
- Logs login times and user activity to maintain audit trails, supporting investigation integrity.

Register

- Collects key information for investigators to ensure proper identification and role assignment.
- It determines permissions and ensures that only authorized users have access to relevant system modules and data.

Upload Data

- It maintains metadata, such as timestamps and source information, ensuring the traceability and authenticity of the evidence.
- Files are categorized and tagged for easy retrieval, ensuring that no evidence is misplaced or overlooked.

View and Collect Evidence

- It provides investigators access to digital evidence for examination, ensuring that they can efficiently proceed with the analysis.
- It facilitates the organization of evidence into case-specific files, aiding systematic and thorough investigations.

View Evidence Status

- Monitors the location and custody of evidence, ensuring that it is handled according to the protocol. It notifies investigators of delays or potential issues with evidence handling, ensuring timely action.

Authenticate Evidence

- It uses an SBVM to confirm the authenticity of the evidence and prevent tampering.
- Ensures the evidence's timeline is immutable and verifiable, supporting its legal admissibility.

Access Encrypted Evidence

- Provides investigators with tools to decrypt encrypted evidence while ensuring compliance with access policies.
- Only authorized users can decrypt sensitive evidence, with an audit trail of who accessed it.

Generate Reports

- Compiles evidence findings into comprehensive reports for legal or investigative review.
- Tailor reports to different case requirements, ensuring flexibility and detail in final documentation.

Logout

- Securely logs out users to prevent unauthorized access after the investigation session is complete.
- Ensures that all data and activities are properly ended, maintaining system integrity and protecting sensitive information.

Admin Modules

Login

- Admins log into the system using their credentials.

View Users

- Admin views details of all registered users' data.
- It provides a comprehensive view of all registered users, including their roles, permissions, and activity logs, enabling administrators to manage system access effectively.

Manage Evidence

- Admins oversee the collection, encryption, and storage of digital evidence.
- Admins can track the entire lifecycle of evidence, from collection to storage, to ensure proper handling and security.

Monitor Encryption and Key Generation

- The admins supervise encryption and key generation processes.
- It ensures the proper generation, distribution, and storage of encryption keys, safeguarding sensitive data from compromise.

Logout

- Admins can log out of the system to secure their session and personal data.

CONCLUSION

In conclusion, the proposed Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) offers a significant advancement in digital forensic security by addressing the vulnerabilities inherent in traditional centralized storage systems. Through the use of decentralized data, an SBVM for authentication, and MHE for encryption, this architecture ensures the confidentiality, integrity, and authenticity of digital evidence throughout its lifecycle. By leveraging the EEO model for optimal key generation, the system enhances key management security, making it resilient to cyber threats and attacks. The architecture is specifically tailored for cloud forensics in an IaaS platform, providing scalable, reliable, and secure storage solutions for handling large volumes of evidence. Simulations demonstrate that DFA-AOKGE outperforms existing methods, offering improved security, performance, and reliability compared to existing methods. This approach represents a critical step forward in addressing the evolving challenges of cloud-based digital forensics, paving the way for more secure, efficient, and trustworthy forensic investigations in the digital age. Numerous cloud forensic solutions currently in use still rely on architecture for centralized evidence storage. Centralized models create single points of failure by design, which can seriously impair system availability and reliability, even though they make management and control easier. Centralized storage systems are particularly susceptible to data loss and extended downtime in the event of cyberattacks, hardware malfunctions, or service interruptions. Additionally, as the amount of forensic data increases, centralized methods become less effective at scaling, which restricts their use in expansive, dispersed cloud systems. These restrictions make it more difficult to

offer continuous and safe access to digital evidence in a dynamic cloud infrastructure and lower fault tolerance. By adopting such an architecture, organizations can ensure that digital evidence remains protected, authentic, and admissible in legal proceedings.

REFERENCES

1. Bachiphale PM, Zulpe NS. Optimal multisecret image sharing using lightweight visual signcryptography scheme with optimal key generation for gray/color images. Int J Image Graph. 2025;25(03):2550017. doi:10.1142/S0219467825500172.
2. Kumar G, Saha R, Lal C, Conti M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Gener Comput Syst. 2021;120:13–25. doi:10.1016/j.future.2021.02.016.
3. Raji L, Ramya ST. Secure forensic data transmission system in cloud database using fuzzy based butterfly optimization and modified ECC. Trans Emerg Telecommun Technol. 2022;33:e4558. doi:10.1002/ett.4558.
4. Abdel-Ghaffar EA, Daoudi M. Personal authentication and cryptographic key generation based on electroencephalographic signals. J King Saud Univ Comput Inf Sci. 2023;35(5):101541. doi:10.1016/j.jksuci.2023.03.019.
5. Velmurugadass P, Dhanasekaran S, Shasi Anand SS, Vasudevan V. Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Mater Today Proc. 2021;37:2653–2659. doi:10.1016/j.matpr.2020.08.519.
6. Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Syst. 2022;39(10):e13126. doi:10.1111/exsy.13126.
7. Nasreen S, Mir AH. Enhancing cloud forensic investigation system in distributed cloud computing using DK-CP-ECC algorithm and EK-ANFIS. J Mob Multimed. 2023;19(3):679–706. doi:10.13052/jmm1550-4646.1933.
8. Du J, Raza SH, Ahmad M, Alam I, Dar SH, Habib MA. Digital forensics as advanced ransomware pre-attack detection algorithm for endpoint data protection. Secur Commun Netw. 2022;2022:1424638. doi:10.1155/2022/1424638.
9. Razaque A, Aloqaily M, Almiani M, Jararweh Y, Srivastava G. Efficient and reliable forensics using intelligent edge computing. Future Gener Comput Syst. 2021;118:230–239. doi:10.1016/j.future.2021.01.012.
10. Kashif M, Mehfuz S, Shakeel I, Ahmad S. Employing an ECC-based hybrid data encryption method to improve multitenancy security in cloud computing. In: Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON); 2023. p. 79–83. doi:10.1109/REEDCON57544.2023.10150684.

