International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 32 Issue 01 – JANUARY 2026.

Improving Digital Forensic Security: A Secure Storage Model with Authentication and Optimal Key Generation Based Encryption

Priyadarshini[#1], Vijalaxmi[#2]

CSE, VISVESVARAYA TECHNOLOGICAL UNIVERSITY CENTER FOR PG STUDIES, KALABURAGI 585105, INDIA

CSE, VISVESVARAYA TECHNOLOGICAL UNIVERSITY CENTER FOR PG STUDIES, KALABURAGI 585105, INDIA

Abstract

The rapid expansion of cloud computing and Internet of Things (IoT) ecosystems has intensified concerns related to data security, integrity, privacy, and trustworthy digital evidence management. Conventional cloud-based forensic and security frameworks rely heavily on centralized architectures and traditional cryptographic techniques, which introduce single-point failures, limited transparency, and increased vulnerability to sophisticated cyber threats. Furthermore, existing encryption and authentication mechanisms struggle to provide robust protection in resource-constrained IoT environments while simultaneously addressing user privacy and regulatory compliance.

To overcome these limitations, this research proposes a novel decentralized digital forensic framework named DFA-AOKGE (Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption). The proposed architecture integrates blockchain-based decentralized data distribution to eliminate centralized control and ensure tamper-resistant evidence preservation. Advanced cryptographic mechanisms, including Edwards-curve Digital Signature Algorithm (EdDSA) and Identity-Based Cryptography (IBC), are employed to strengthen authentication and access control. A Secure Biometric Verification Module (SBVM) is incorporated to enhance user authentication while maintaining biometric privacy. Additionally, an Efficient Entropy-based Optimization (EEO) technique is introduced for optimal secret key generation, improving cryptographic strength and resistance to attacks.

Index terms — Decentralized Digital Forensics, Blockchain Technology, Cloud–IoT Security, EdDSA, Identity-Based Cryptography, Biometric Authentication, Optimal Key Generation, Homomorphic Encryption, Data Integrity, Privacy Preservation.

I. INTRODUCTION

The widespread adoption of cloud computing and the Internet of Things (IoT) has transformed modern digital infrastructures by enabling scalable data storage, real-time analytics, and interconnected smart systems. These technologies are increasingly deployed across critical domains such as healthcare, smart cities, finance, and law enforcement, where large volumes of sensitive data are generated, transmitted, and stored continuously. While cloud–IoT integration offers significant operational advantages, it also introduces complex security, privacy, and digital forensic challenges that existing centralized architectures struggle to address effectively.

Digital forensics plays a vital role in investigating cyber incidents, preserving electronic evidence, and ensuring accountability in distributed computing environments. However, traditional digital forensic frameworks largely rely on centralized evidence collection and storage mechanisms, making them vulnerable to single-point failures, data tampering, unauthorized access, and insider threats. In cloud-based systems, forensic data is often controlled by third-party service providers, raising concerns regarding data ownership, integrity verification, and trustworthiness of collected evidence. These issues become even more critical in IoT environments, where devices are resource-constrained, widely distributed, and frequently targeted by sophisticated cyberattacks.

II. LITERATURE REVIEW

Recent advancements in cloud computing and Internet of Things (IoT) technologies have significantly increased the complexity of digital forensic investigations due to data distribution, multi-tenancy, and lack of direct control over evidence sources. Early studies on cloud forensics highlighted critical challenges such as evidence volatility, dependency on cloud service providers, and the absence of standardized mechanisms for maintaining chain of custody in distributed environments. Similarly, IoT forensic research has emphasized issues related to heterogeneous device architectures, constrained resources, and insecure data transmission, which collectively undermine reliable evidence preservation.

To address security concerns in cloud-based systems, conventional cryptographic techniques such as AES and DSA have been widely adopted. However, multiple studies report that traditional key management schemes relying on centralized authorities introduce single-point failures and increase exposure to insider and external attacks. These

limitations become more pronounced in IoT environments, where secure key distribution and computational efficiency are critical. As a result, researchers have explored elliptic curve cryptography and identity-based cryptographic schemes to reduce key management overhead while improving authentication efficiency.

Blockchain technology has emerged as a promising solution for enhancing data integrity and transparency in distributed systems. Several researchers have demonstrated that blockchain-based logging mechanisms can provide tamper-proof audit trails for digital evidence and event records. By decentralizing trust, blockchain eliminates reliance on centralized forensic authorities and improves accountability. Nevertheless, existing blockchain-assisted forensic frameworks often focus solely on evidence immutability and lack integrated authentication models, privacy-aware biometric handling, and efficient encryption mechanisms for cloud storage.

Biometric authentication has gained increasing attention for strengthening access control in secure systems due to its ability to uniquely identify users. Studies indicate that biometric-based authentication significantly reduces impersonation and credential theft risks. However, researchers also highlight critical privacy concerns, as compromised biometric data cannot be revoked or replaced. Current solutions often store biometric templates in centralized repositories or apply weak protection mechanisms, making them unsuitable for high-assurance forensic applications.

III. Existing System

In the rapidly evolving landscape of cloud computing and the Internet of Things (IoT), the need for secure, efficient, and privacy-preserving systems has become paramount. As organizations increasingly rely on cloud-based solutions for data storage and processing, they encounter significant challenges concerning data integrity, security, and centralized evidence gathering. Traditional cryptographic methods, while instrumental in enhancing security, often fall short in addressing the complexities introduced by centralization and single-point vulnerabilities.

One of the primary issues is the centralization of evidence collection and preservation. Current systems frequently depend on centralized authorities to manage and secure user data. This centralization not only creates a single point of failure but also increases the risk of unauthorized access and data breaches. In the event of a security compromise, the repercussions can be severe, leading to data loss, financial damage, and erosion of user trust. Furthermore, the centralized model often hinders the accountability of data handling practices, making it challenging to track and verify data provenance.

IV. Proposed System

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.

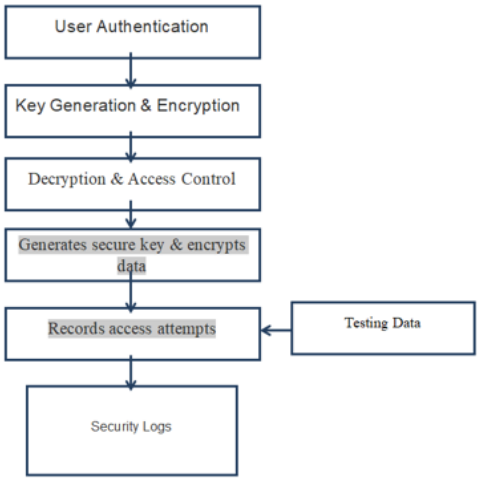

Fig 1: Data Flow Diagram

A. *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.

V. Methodology

A. *Knowledge Base Construction:*

Data Collection: Aggregate query-call records from KCC data servers and the Open Government Data Platform India from the past eight years, ensuring compliance with data

usage regulations.

Data Processing: Clean and structure the collected data to create a comprehensive knowledge base that includes farmer queries, locations, and expert responses.

B. Response-Retrieval Model Development:

Model Design: Develop a response-retrieval model capable of processing varied inputs, including misspelled words and regional language variations.

Algorithm Implementation: Utilize machine learning techniques for effective query matching and retrieval.

1) Advantages:

AgriResponse System: Introduce a user-friendly platform for farmers and helpline operators to access plant protection information.

Error-Tolerant Mechanisms: Implement spelling correction and fuzzy matching to enhance user experience and query processing.

Multiple Answer Support: Allow for the provision of various solutions to a single query, reflecting regional agricultural practices.

National-Level Efficiency: Ensure the system is tested and optimized for use across diverse regions of India.

Public Accessibility: Make the knowledge base, model codes, and question bank publicly accessible to facilitate reproducibility and further research.

Multilingual Support: Address the challenges of multilingual data by incorporating strategies for handling language diversity and translation errors.

Reliable Metrics: Establish robust performance metrics for evaluating the effectiveness of the AgriResponse system.

C. Copyright Considerations:

Data Usage Compliance: Ensure that all data collected from KCC servers and public platforms adhere to copyright and data protection regulations.

Open Source Licensing: Consider using an open-source license for the code and resources developed, promoting sharing and collaborative improvement while protecting intellectual property.

Attribution Practices: Clearly document and attribute all sources of data and code to maintain transparency and ethical research practices.

D. Expected Outcomes:

Functional AgriResponse System: A fully operational system that meets the needs of farmers for plant protection queries.

Enhanced User Engagement: Increased usage and satisfaction among farmers and helpline operators due to the system's responsiveness and accuracy.

Contribution to Agricultural Research: A publicly available framework that encourages future research and development in agricultural information systems.

E. Future Research Directions:

System Evaluation: Conduct extensive user testing to assess the effectiveness of the AgriResponse system and identify areas for improvement.

Scalability Studies: Investigate the scalability of the system to other regions and agricultural domains.

Integration with Other Technologies: Explore opportunities for integrating AgriResponse with mobile applications and AI-driven chatbots for broader accessibility.

VI. MODULE DESCRIPTION

Enhanced Knowledge Base: A comprehensive knowledge base constructed from eight years of call-log records, capable of answering diverse plant protection-related questions from farmers across India.

Effective Query-Response System: A functional text-based query-response generation system that allows farmers to receive timely and relevant information regarding agricultural practices and plant protection.

Improved Accessibility: Increased accessibility to agricultural knowledge for farmers, enabling them to make informed decisions and enhance their crop yields.

Robust Response-Retrieval Models: Development and implementation of three response-retrieval models that effectively handle approximate matching and spatial-based searching, optimizing the retrieval of answers based on user queries.

Comprehensive Validation: Performance validation of the framework using a diverse question bank of 755 queries related to 151 crops, ensuring its applicability across various agricultural contexts in India.

Performance Metrics Assessment: Evaluation of the retrieval models based on three key metrics:

Accuracy Percentage: Measuring the correctness of retrieved responses.

Crop-weighted Performance Score: Evaluating the effectiveness of responses based on the significance of different crops.

Average Response-Retrieval Time: Assessing the efficiency of the system in providing timely answers.

VII. CONCLUSION

This research presented **DFA-AOKGE**, a decentralized digital forensic framework designed to address critical security, integrity, and privacy challenges in cloud and IoT environments. The study identified fundamental limitations of traditional centralized forensic architectures, including single-point failures, weak accountability, inefficient key management, and inadequate privacy protection for sensitive forensic and biometric data. These shortcomings significantly hinder reliable evidence preservation and trustworthy forensic investigations in modern distributed systems.

To overcome these challenges, the proposed framework integrates blockchain-based decentralized data management with advanced cryptographic mechanisms such as EdDSA and Identity-Based Cryptography to strengthen authentication and access control. The inclusion of a Secure Biometric Verification Module ensures reliable identity validation while preserving user privacy. Furthermore, the Efficient Entropy-based Optimization technique enhances secret key generation, and the adoption of multi-key homomorphic encryption enables privacy-preserving computation on encrypted forensic data stored in the cloud.

The decentralized nature of DFA-AOKGE ensures tamper resistance, transparent auditing, and verifiable data

provenance, thereby improving trust among stakeholders such as users, service providers, and regulatory authorities. Security analysis and architectural evaluation demonstrate that the proposed framework offers improved resilience against data tampering, unauthorized access, and insider threats compared to existing centralized approaches.

REFERENCES

[1] R. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," *Digital Investigation*, vol. 10, no. 4, pp. 325–333, 2013.
[2] S. Zawoad and R. Hasan, "FAIoT: Towards building a forensics-aware eco system for the Internet of Things," *IEEE International Conference on Services Computing*, pp. 279–284, 2015.
[3] A. Singh, K. Chatterjee, and S. Chakraborty, "A survey on cloud key management," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2509–2527, 2017.
[4] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology (CRYPTO)*, pp. 47–53, 1984.
[5] D. J. Bernstein et al., "High-speed high-security signatures," *Journal of Cryptographic Engineering*, vol. 2, no. 2, pp. 77–89, 2012.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[7] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.
[8] C. Gentry, "Fully homomorphic encryption using ideal lattices," *ACM Symposium on Theory of Computing*, pp. 169–178, 2009.
[9] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," *ACM Symposium on Theory of Computing*, pp. 1219–1234, 2012.
[10] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, pp. 1–25, 2011.