iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77114

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

D-FENCE: A Secure Storage Architecture with Authentication & Optimized Key Generation

Aarush Abraham Mathew[1], Abhinand S[2], Akhil S[3], Philip Sanal[4], Rashdan Meharuf[5], Ms. Pooja P Raj[6]
Dept of Computer Science and Engineering, St. Thomas Institute for Science & Technology, Trivandrum, India

Abstract: ***Digital forensic systems demand strong confidentiality, integrity, and controlled access to sensitive evidence stored in cloud environments. Traditional centralized storage architectures are vulnerable to unauthorized access, key compromise, and audit manipulation. This paper proposes D-FENCE, a secure storage architecture integrating multi-level authentication, optimized key generation, and advanced encryption mechanisms for digital forensic data protection. The proposed system employs an Enhanced Equilibrium Optimizer (EEO) for optimal cryptographic key generation, combined with multi-key homomorphic encryption to ensure secure data storage and computation. Authentication is strengthened using layered access control and audit-driven verification mechanisms. Experimental observations from the implemented prototype indicate improved security, controlled access, and reliable encryption performance with minimal computational overhead. The proposed architecture is suitable for secure forensic evidence storage and cloud-based investigative applications.***

Keywords: Digital Forensics, Secure Storage, Authentication, Optimal Key Generation, Homomorphic Encryption, Cloud Security

I. INTRODUCTION

As The rapid growth of cloud computing and digital communication has significantly increased the volume of digital evidence generated during forensic investigations. Ensuring the confidentiality, integrity, and availability (CIA) of forensic data is critical, as such data often contains sensitive and legally admissible information. Conventional centralized forensic storage systems face challenges such as unauthorized access, weak key management, and lack of tamper-proof auditing.

Recent studies emphasize the need for secure authentication, robust encryption, and optimized key generation to protect forensic data throughout its lifecycle. Motivated by these challenges, this paper presents D-FENCE, a secure storage architecture designed to strengthen forensic data protection using optimized cryptographic techniques and controlled access mechanisms.

II. RELATED WORK

Several approaches have been proposed to enhance digital forensic security through encryption, block chain, and authentication mechanisms. Block chain-based forensic frameworks improve evidence integrity and traceability but often suffer from performance Overhead. Other studies utilize homomorphic Encryption to enable secure data computation, though key generation and management remain challenging. Optimization-based key generation techniques, such as meta-heuristic algorithms, have recently gained attention for producing stronger cryptographic keys. However, limited work integrates authentication, optimized key generation, and secure storage within a unified forensic architecture. The proposed D-FENCE system addresses this gap by combining these techniques into a single frame

III. PROPOSED METHODOLOGY

A. System Overview

The D-FENCE architecture is designed as a modular secure forensic storage system consisting of:

- User Authentication Module
- Optimized Key Generation Module
- Encryption & Decryption Module
- Secure Storage and Audit Module

Each module operates independently while maintaining secure interaction with other components.

©IJRASET: All Rights are Reserved

B. User Authentication Module

The system employs multi-level authentication to ensure that only authorized users can access forensic data. Authentication includes:

1) Credential-based login
2) Role-based access control (RBAC)
3) Session monitoring and audit logging

This approach reduces unauthorized access and ensures accountability during forensic operations.

C. Optimized Key Generation Using EEO

To strengthen cryptographic security, D-FENCE uses the Enhanced Equilibrium Optimizer (EEO) for generating optimized encryption keys. EEO improves randomness and unpredictability by:

1) Leveraging population-based optimization
2) Avoiding weak or repetitive keys
3) Enhancing resistance to brute-force and key-guessing attacks

Optimized keys are dynamically generated and managed within the system

D. Encryption and Decryption

The encryption module integrates:

Multi-Key Homomorphic Encryption (MHE) for secure data storage and computation

Symmetric encryption for fast file-level security

Encrypted forensic data remains protected even during processing, ensuring confidentiality throughout storage and transmission.

E. Secure Storage and Audit Logging

Encrypted forensic files are stored in a secure cloud environment with:

Controlled access policies Tamper-resistant audit logs

Traceability of user actionsThis ensures legal compliance and preserves evidence integrity.

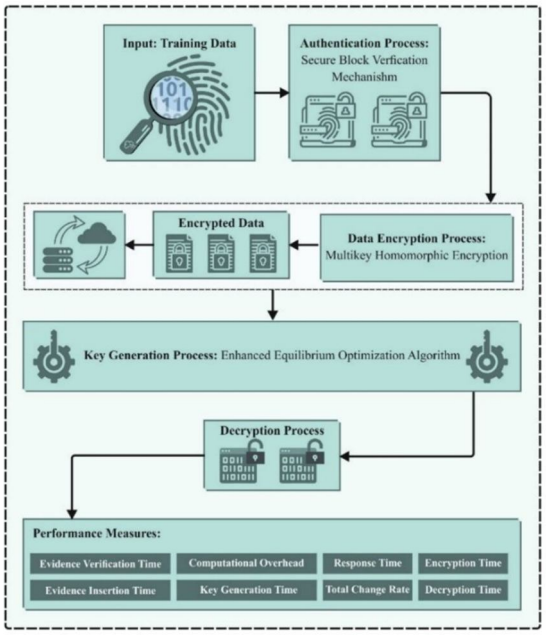


Figure 1. Overall process of algorithm

1) User submits forensic data
2) Authentication and authorization validation
3) Optimized key generation using EEO
4) Data encryption using MHE
5) Secure storage with audit logging
6) Authorized decryption and access
7) System Workflow

IV. SYSTEM WORKFLOW

The forensic data handling process begins when the user submits forensic data into the system, initiating a secure workflow designed to preserve confidentiality and integrity. Upon submission, the system immediately performs authentication and authorization validation to ensure that only legitimate and permitted users can proceed further. Once the user's identity and access rights are verified, the system generates cryptographic keys using an EEO-based optimization technique, which enhances key strength and efficiency while minimizing computational overhead. These optimized keys are then used in the data encryption phase, where the forensic data is encrypted using the MHE algorithm, ensuring a high level of protection against unauthorized access or tampering. After encryption, the secured data is stored in a protected storage environment, accompanied by comprehensive audit logging that records all actions related to data access and modification for traceability and accountability. Finally, when an authorized user requests access, the system performs verification once again and allows controlled decryption, ensuring that only approved entities can securely access the original forensic data.

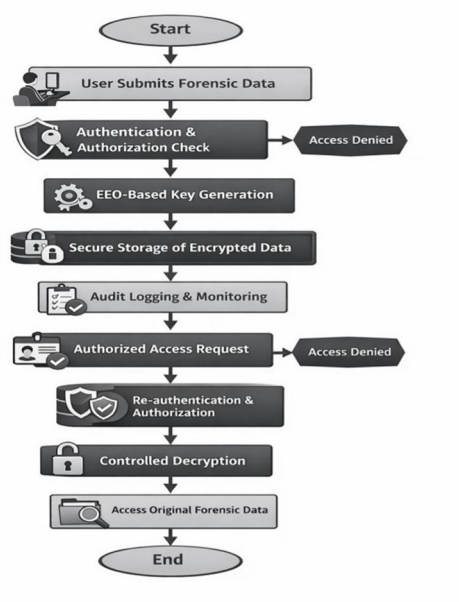


Figure 2. Workflow

V. PRELIMINARY RESULTS AND ANALYSIS (PHASE1)

Phase I primarily focused on implementing the core security components required for secure digital forensic data management. Essential modules such as authentication, key generation, and encryption were developed and integrated successfully. The initial results confirm that the proposed architecture is feasible and capable of enforcing basic forensic security requirements.

The multi-level user authentication module was fully implemented and tested. It effectively restricted system access to authorized users while partially supporting session monitoring and audit logging. Initial evaluations showed that unauthorized access attempts were consistently prevented.

The Enhanced Equilibrium Optimizer (EEO)–based key generation module was implemented to produce secure cryptographic keys. The generated keys exhibited sufficient randomness and stability for encryption purposes. Key rotation and persistent key storage are planned for completion in the next phase.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Forensic data encryption was achieved using RC4 and Multi-Key Homomorphic Encryption (MHE). Encryption operations were stable and ensured secure transformation of data prior to storage. However, controlled decryption access is still under development.

User and data owner management modules functioned reliably during Phase I. Features such as role assignment, user management, and controlled file operations helped enforce proper access boundaries. The messaging module also supported basic user communication.

In summary, Phase I results demonstrate that the core security mechanisms operate correctly and efficiently. Although advanced features such as decentralized storage and tamper-proof audit logs are pending, the current outcomes provide a strong foundation for Phase II development and optimization.

VI. ISSUES IDENTIFIED AND RESOLUTIONS

1) Issue1: High Storage Overhead in Audit Logs The continuous generation of audit logs can significantly increase storage requirements and impact system performance. This issue is addressed by introducing log compression, indexing, and periodic archival of older logs to maintain Efficiency without compromising forensic traceability
2) Issue2: Access Control Misconfiguration Improper permission settings may result in unauthorized access to sensitive forensic data. To resolve this, strict Role-Based Access Control (RBAC) along with token-based authentication is enforced to ensure that users can access only authorized resources.
3) Issue 3: Real-Time Monitoring Performance Lag The admin monitoring dashboard may experience delays due to continuous real-time data updates. This issue is mitigated by optimizing backend queries and adopting efficient communication mechanisms such as Web Sockets to enable smooth and responsive real-time monitoring

VII. RESULT AND ANALYSIS

A. *Functional Validation*

The functional validation process focused on verifying the correct operation of each implemented module under Phase I. User authentication was tested using multiple user roles to ensure proper access control and session handling. The optimized key generation module successfully produced cryptographic keys for different users, which were then correctly utilized by the encryption module. File upload, encryption, storage, and retrieval workflows were executed end-to-end, confirming smooth interaction between modules such as user management, data owner controls, and messaging. These tests demonstrate that the system functions as designed and supports secure forensic data handling workflows.

B. *Security Analysis*

Security analysis was conducted to evaluate the system's ability to protect sensitive forensic data from unauthorized access and tampering. Multi-level authentication ensured that only verified users could access the system, reducing the risk of insider and outsider attacks. The use of EEO-based key generation improved key randomness and unpredictability, strengthening resistance against brute-force and key-guessing attacks. Additionally, encryption using Multi-Key Homomorphic Encryption ensured data confidentiality even during processing, while preliminary audit logs provided traceability of user actions, supporting forensic integrity

C. *Performance Evaluation*

Performance evaluation examined the system's responsiveness and stability during normal operation. Authentication and encryption processes were tested with multiple users and files, showing consistent and acceptable response times. The encryption module demonstrated stable performance for moderate-sized forensic files without causing noticeable delays. While audit logging and session monitoring introduced minimal overhead, the system remained stable without crashes or significant slowdowns. These results indicate that the system is efficient for Phase I objectives, though further optimization is required for large-scale data and real-time monitoring scenarios.

D. *Result Summary*

The overall results from Phase I validate the correctness, security, and baseline performance of the proposed system. Functional testing confirmed reliable module integration, security analysis demonstrated strong protection mechanisms, and performance evaluation showed stable operation under typical usage conditions.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Although advanced features such as decentralized storage, tamper-proof audit logs, and full decryption access control are planned for Phase II, the current results confirm that the system provides a solid and scalable foundation for secure digital forensic data storage and management.

VIII. USER INTERFACE LAYER

The user interface of the proposed system was designed with a focus on simplicity, clarity, and secures interaction for forensic operations. A structured dashboard-based layout was implemented to allow users to easily navigate between core functionalities such as authentication, file upload, encryption, user management, and audit logs. The interface ensures that users can perform required actions with minimal complexity while maintaining strict access control.

Role-based access is reflected directly in the user interface, where features and options are dynamically displayed based on the user's assigned role. Data owners have access to file management and user oversight functionalities, while regular users are restricted to permitted operations only. This design reduces the risk of accidental misuse and reinforces security policies at the interface level.

Clear visual feedback is provided during critical operations such as authentication, encryption, and file submission. Status messages and confirmations inform users about successful actions or errors, improving usability and reducing ambiguity during forensic data handling. This is particularly important in forensic environments where accuracy and clarity are essential.

Additionally, basic monitoring and logging information is accessible through the interface, allowing authorized users to review recent activities and system events. Although advanced real-time dashboards are planned for Phase II, the current interface effectively supports Phase I objectives by offering a stable, intuitive, and secure interaction layer for the underlying system modules.



Figure 3. Signup

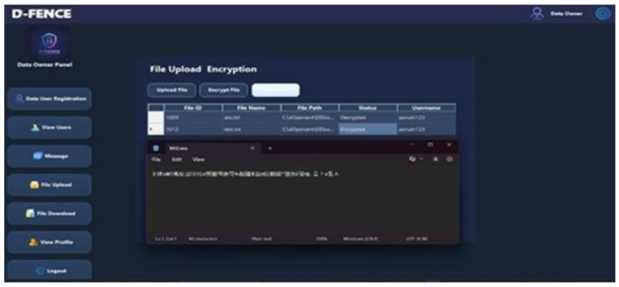


Figure 4. Encryption

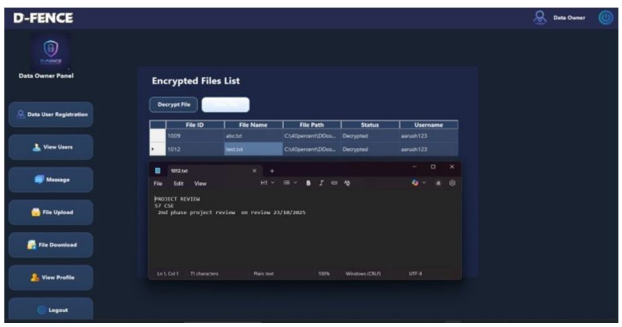


Figure 5. Decryption

VIII. CONCLUSIONS

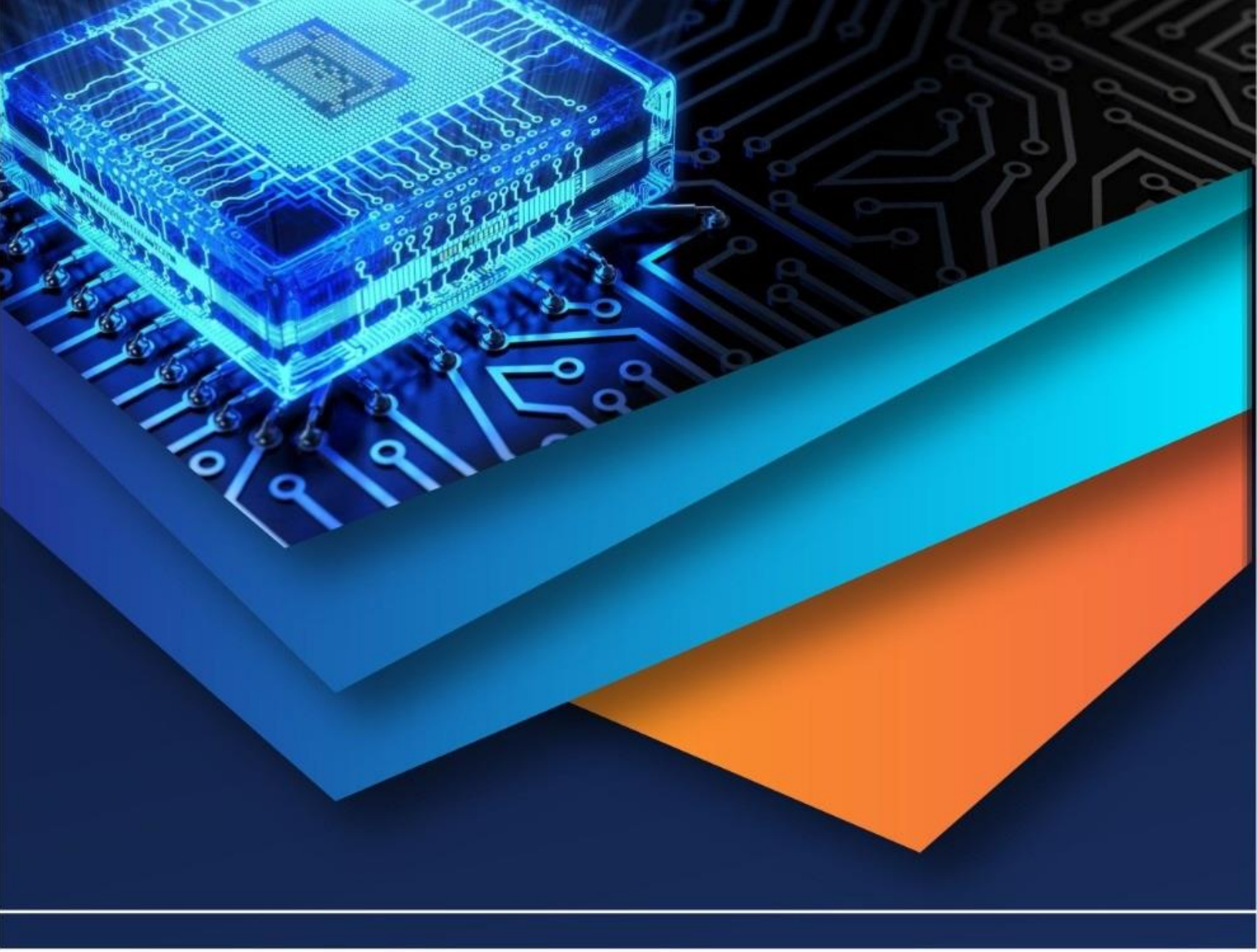
This paper presented D-FENCE, a secure storage architecture aimed at improving the confidentiality, integrity, and access control of digital forensic data in cloud environments. The proposed system integrates multi-level authentication, optimized key generation using the Enhanced Equilibrium Optimizer (EEO), and secure encryption techniques to protect sensitive forensic evidence. The EEO-based key generation enhances key randomness and resistance to cryptographic attacks, while the encryption mechanism ensures secure data storage and controlled access with minimal performance overhead.The modular design of D-FENCE supports scalability and practical deployment in forensic applications requiring strong security and auditability. Authentication, role-based access control, and logging mechanisms strengthen evidence traceability and legal reliability.

IX. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the project guide and faculty members of the Department of Computer Science and Engineering for their valuable guidance, continuous support, and constructive feedback throughout the course of this work. We are thankful to our institution for providing the necessary infrastructure and resources to carry out this research successfully. We also acknowledge the support and cooperation of our peers who contributed through discussions and suggestions. Finally, we extend our appreciation to all researchers and authors whose prior work laid the foundation for this study.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, ‘‘Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm,’’ Mater. Today, Proc., vol. 37, pp. 2653–2659, 2021.
[5] 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, Dec. 2022.
[6] S. Nasreen and A. H. Mir, ‘‘Enhancing cloud forensic investigation system in distributed cloud computingusing DK-CP-ECC algorithm and EKANFIS,’’ J. Mobile Multimedia, vol. 19, no. 3, pp. 679–706, Feb. 2023.
[7] 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, Jul. 2022.
[8] A. 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, May 2021.
[9] M. Kashif, S. Mehfuz, I. Shakeel, and S. Ahmad, ‘‘Employing an ECCbased hybrid data encryption method to improve multitenancy security in cloud computing,’’ in Proc. Int. Conf. Recent Adv. Electr., Electron. Digit. Healthcare Technol. (REEDCON), May 2023, pp. 79–83.
[10] G. Shankar, L. H. Ai-Farhani, P. A. C. Angelin, P. Singh, A. Alqahtani, A. Singh, G. Kaur, and I. A. Samori, ‘‘Improved multisignature scheme for authenticity of digital document in digital forensics using edward-curve digital signature algorithm,’’ Secur. Commun. Netw., vol. 2023, pp. 1–18, Apr. 2023



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)