IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 7, June 2025

Impact Factor: 7.67

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

Dr Khaleel UR Rahman Khan[1], **Ch. Praneetha**[2], **K. Suhas**[3], **P. Vamshi krishna**[4,] **A. Pavan Teja**[5]

Professor & Dean (Academics) [1]

Student, Computer Science and Engineering[2,3,4,5]

ACE Engineering College, Ghatkesar, India.

Abstract: *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. Cloud forensics is an intelligent development of digital forensics to be preserved against online hacking. But, centralized evidence gathered and preservation reduces the reliability of digital evidence. This architecture integrates numerous modules and methods to address the exclusive tasks modeled by cloud computing (cc) environments in the framework of forensic investigations. This paper develops a new digital forensic architecture utilizing the authentication with optimal key generation encryption (dfa aokge) technique. The main intention of the dfa-aokge method is to use a bc-distributed design to allocate data between numerous peers for data collection and safe storage. Additionally, the dfa-aokge model uses the secure block verification mechanism (sbvm) for the authentication procedure. Also, the secret keys can be produced by the usage of the enhanced equilibrium optimizer (eeo) model. Furthermore, the encryption of the data takes place using a multikey homomorphic encryption (mhe) approach and is then saved in the cloud server. The simulation value of the dfa-aokge methodology takes place in terms of different aspects. The simulation results exhibited that the dfa-aokge system shows prominent performance over other recent approaches in terms of different measures.*

Keywords: In encryption, decryption digital forensic architecture, multikey homomorphic encryption

I. INTRODUCTION

The rapid proliferation of cloud computing and Internet of Things (IoT) technologies has significantly transformed the landscape of digital evidence collection and cybercrime investigation. However, the growing volume of data and the distributed nature of modern systems introduce substantial challenges in ensuring data confidentiality, integrity, and authenticity during forensic investigations. Traditional centralized forensic models, often reliant on legacy encryption schemes such as DES and AES, fall short when confronted with the dynamic and scalable nature of cloud and edge environments [2], [5].

To address these evolving challenges, recent research has focused on integrating blockchain, homomorphic encryption, and intelligent optimization strategies into digital forensic frameworks. Blockchain technology, with its tamper-evident and decentralized characteristics, has emerged as a reliable solution for ensuring the integrity and traceability of digital evidence [2], [14]. Enhanced cryptographic approaches, such as multikey homomorphic encryption and elliptic curve cryptography (ECC), offer secure mechanisms for privacy-preserving data processing and secure key exchange across multiple stakeholders [1], [3], [10].

Several studies have proposed novel models and protocols that combine security, efficiency, and scalability. For instance, Raji and Ramya [3] introduced a fuzzy-based butterfly optimization technique with modified ECC for secure forensic data transmission in the cloud. Bachiphale and Zulpe [1] emphasized optimal key generation and visual

DOI: 10.48175/IJARSCT-28047

cryptography in image sharing, contributing to secure communication systems. Similarly, Abdel-Ghaffar and Daoudi [4] explored EEG-based biometric key generation for enhancing personal authentication, while Nyangaresi et al. [6] utilized artificial neural networks for 5G-enabled secure IoT verification.

Edge computing has also gained attention as a complementary approach to centralized cloud processing. Razaque et al. [9] and Deebak and AL-Turjman [15] presented efficient forensic models using edge and fog computing paradigms to minimize latency and increase data survivability. Additionally, hybrid cryptographic models such as DK-CP-ECC and Edward-curve-based digital signature schemes are being employed for robust identity validation and secure document handling [7], [11].

Despite these advancements, ensuring real-time evidence preservation, resilient key management, and forensic compatibility in multi-tenant and distributed systems remains a critical research challenge. Motivated by these gaps, this paper proposes a secure digital forensic architecture that integrates blockchain distribution, optimal key generation using enhanced metaheuristic techniques, and multikey homomorphic encryption to deliver a comprehensive solution for secure evidence management in cloud-IoT ecosystems.

II. LITERATURE REVIEW

Bachiphale and Zulpe [1] proposed a lightweight visual sign-cryptography scheme integrated with optimal key generation for multi-secret image sharing. Their model enhances both security and performance, making it suitable for secure communication in digital forensic applications.

Kumar et al. [2] introduced the Internet-of-Forensics (IoF) framework, a blockchain-based solution that ensures transparency, integrity, and traceability of digital evidence across IoT platforms. Their model enables real-time evidence tracking and immutable logging in distributed environments.

Raji and Ramya [3] developed a secure forensic data transmission system in the cloud using fuzzy-based butterfly optimization and modified ECC. This system provides robustness in key management and encryption, addressing vulnerabilities in forensic cloud databases.

Abdel-Ghaffar and Daoudi [4] explored EEG signal-based personal authentication and cryptographic key generation. Their biometric-based approach strengthens access control mechanisms and supports secure forensic analysis with high individual specificity.

Velmurugadass et al. [5] proposed an enhanced blockchain security framework using ECIES and cryptographic hash algorithms, tailored for cloud-IoT environments. This integration improved the confidentiality and authenticity of digital records.

Nyangaresi et al. [6] introduced a verification protocol based on artificial neural networks and symmetric key cryptography for 5G-enabled IoT systems. The model offers enhanced security and performance, suitable for real-time data validation in forensic networks.

Nasreen and Mir [7] proposed a DK-CP-ECC algorithm with EK-ANFIS for enhancing cloud forensic investigations in distributed computing. Their hybrid cryptographic model enables intelligent decision-making and encrypted data handling.

Du et al. [8] presented a ransomware pre-attack detection algorithm embedded in endpoint protection systems. Their work emphasizes proactive forensic readiness using digital forensics to detect malicious behaviors before data compromise occurs.

Razaque et al. [9] discussed intelligent edge computing for reliable and efficient digital forensics. Their decentralized approach supports low-latency evidence acquisition and reduces dependence on centralized forensic servers.

Kashif et al. [10] designed an ECC-based hybrid encryption method to enhance multitenancy security in cloud computing. Their solution improves cryptographic isolation among tenants, which is crucial for preserving forensic evidence integrity in shared environments.

Shankar et al. [11] proposed a multisignature scheme using the Edward-curve digital signature algorithm for authenticating digital forensic documents. Their method improves verification speed and authenticity in digital document chains.

DOI: 10.48175/IJARSCT-28047

Unal et al. [12] developed an identity-based encryption scheme tailored for IoT-cloud forensic compatibility. Their framework supports secure data storage and retrieval while maintaining forensic admissibility.

Sheeja [13] focused on lightweight scalable cryptography for IoT environments, introducing a multifactor security model that enhances authentication and data protection in constrained forensic devices.

Apirajitha and Devi [14] introduced a blockchain-based forensic model in cloud using Krill Herd cuckoo search optimization. Their model improves chain-of-custody management and evidence traceability through secure, decentralized mechanisms.

Deebak and AL-Turjman [15] proposed a lightweight authentication protocol for IoT/cloud forensics, addressing latency and energy constraints in smart environments. Their approach supports efficient forensic logging and auditability in intelligent systems.

III. PROPOSED WORK

The proposed model, Digital Forensic Architecture with Authentication and Optimal Key Generation-based Encryption (DFA-AOKGE), is designed to enhance digital evidence preservation in cloud environments through a combination of secure authentication, distributed storage, and optimized encryption mechanisms. This architecture addresses the limitations of traditional forensic systems that suffer from weak encryption, centralized vulnerabilities, and poor scalability [2], [5].

A. Blockchain-Distributed Evidence Storage

The DFA-AOKGE employs a **Blockchain (BC) distributed design** that decentralizes the storage of digital evidence across multiple peers. Each evidence block is hashed and linked with its previous block, forming an immutable ledger. This structure ensures tamper resistance and traceability throughout the forensic process .

B. Secure Block Verification Mechanism (SBVM)

For verifying the authenticity of stored evidence, a **Secure Block Verification Mechanism (SBVM)** is introduced. It utilizes hash functions (e.g., SHA-256) to create and validate unique identifiers for each log entry. Digital signatures are used to maintain data integrity, allowing authorized users to audit changes without compromising confidentiality.

C. Enhanced Equilibrium Optimizer (EEO) for Key Generation

To enhance cryptographic strength, the system integrates the **Enhanced Equilibrium Optimizer (EEO)** algorithm for generating encryption keys. EEO uses adaptive search and equilibrium modeling to ensure the keys are resistant to brute-force and pattern-based attacks. This guarantees dynamic and secure key generation for each evidence transaction.

D. Multikey Homomorphic Encryption (MHE)

The architecture integrates **Multikey Homomorphic Encryption (MHE)**, enabling secure computations on encrypted data from different users without decrypting it. This is essential for maintaining confidentiality when multiple stakeholders (e.g., forensic investigators, court authorities) access or process evidence. The MHE allows for additive or multiplicative operations to be carried out directly on ciphertexts while preserving privacy.

E. Role-Based Evidence Handling

The system is implemented in three primary modules:

- **User (Forensic Investigator):** Uploads evidence, requests decryption, shares keys.
- **Admin:** Authenticates users, manages evidence logs, handles key distribution.
- **Court:** Views requested case files, decrypts evidence using shared keys.

Each user role interacts through a secure web interface developed using Python and Django, with encryption services executed through cryptographic libraries. Evidence is transferred over secure channels and decrypted only after role-based approval.

F. Implementation and Workflow Summary

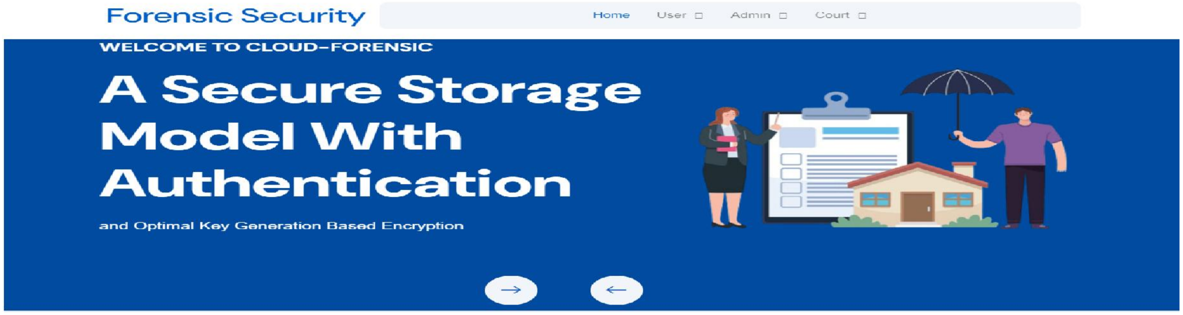
- **Upload Phase:** The user encrypts and uploads evidence to the blockchain network.
- **Verification Phase:** The admin authenticates the data via SBVM and validates user roles.

DOI: 10.48175/IJARSCT-28047

- **Key Distribution:** The EEO model generates decryption keys securely, which are distributed based on access control policies.
- **Decryption Phase:** The court decrypts and verifies evidence using the shared keys while the chain of custody remains traceable.

This proposed DFA-AOKGE framework thus delivers an integrated, secure, and scalable solution for digital forensic investigation in cloud environments.

IV. RESULTS

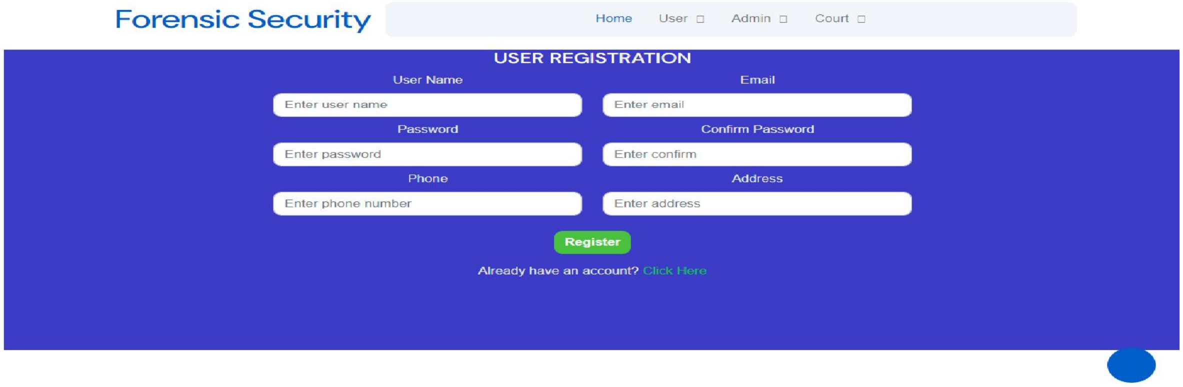


WELCOME TO CLOUD–FORENSIC

A Secure Storage Model With Authentication

and Optimal Key Generation Based Encryption

Home page**:** This is the project home page.

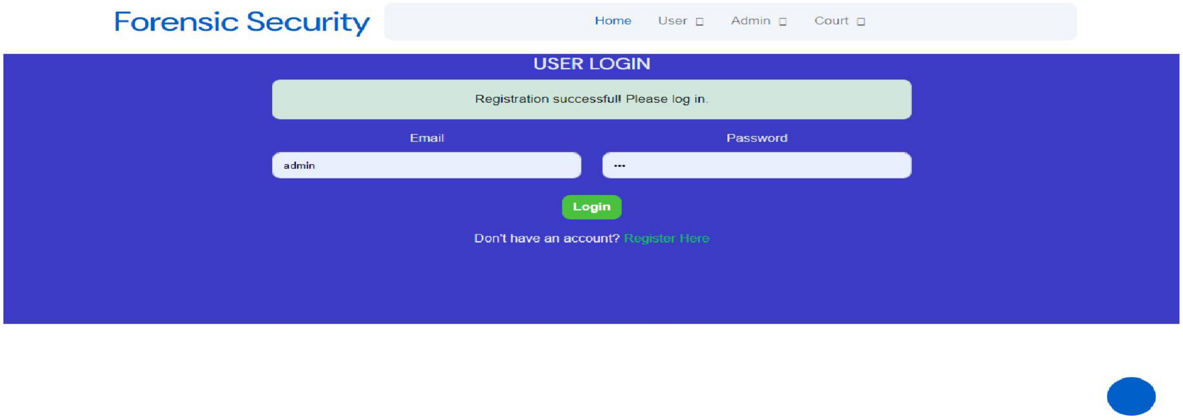


USER REGISTRATION

User Name: Enter user name
Email: Enter email
Password: Enter password
Confirm Password: Enter confirm
Phone: Enter phone number
Address: Enter address

Already have an account? Click Here

User registration: The user can register here using their credentials.



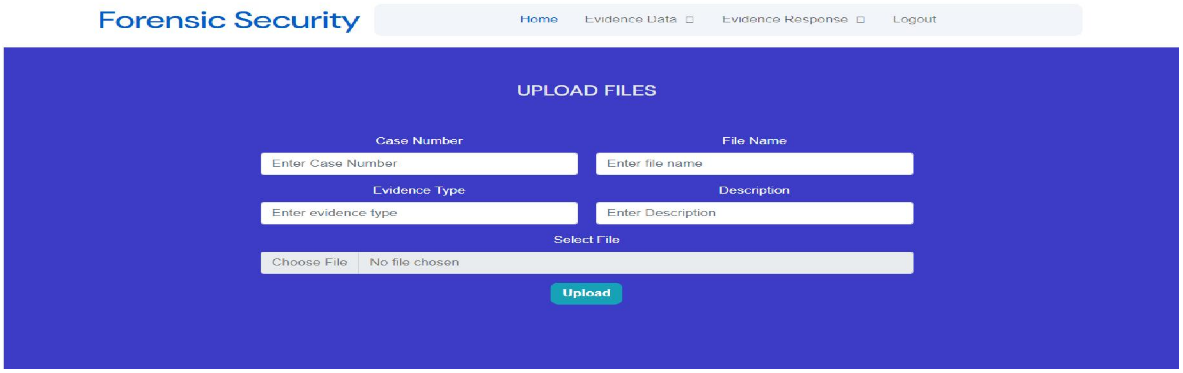
USER LOGIN

Registration successful! Please log in.

Email: admin
Password: ---

Don't have an account? Register Here

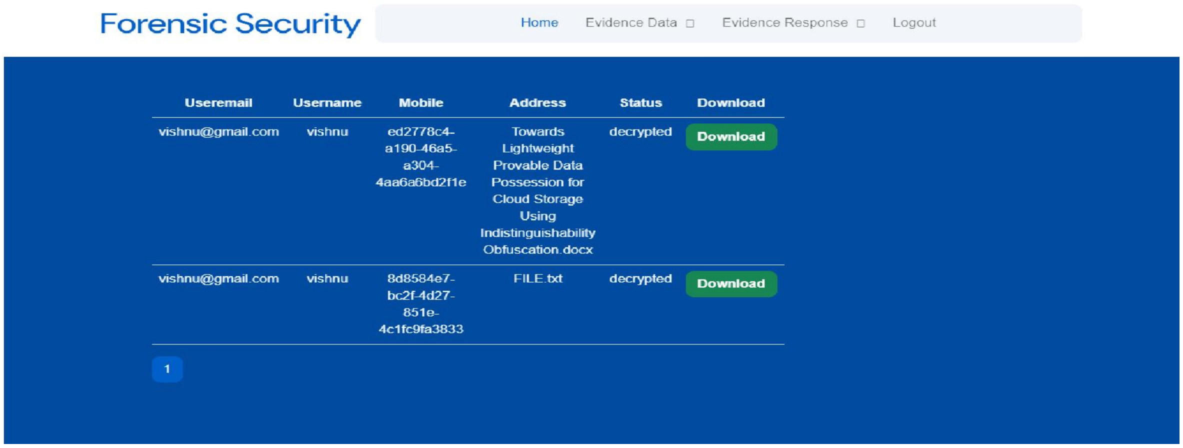
User Login: The user can login here using their credentials after the admin approvals.



UPLOAD FILES

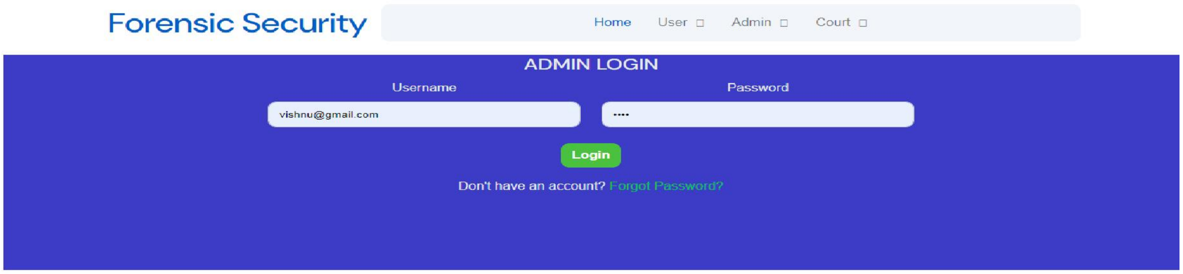
Case Number: Enter Case Number
File Name: Enter file name
Evidence Type: Enter evidence type
Description: Enter Description
Select File: No file chosen

Upload evidence data: The user can upload the evidence data using encryption for file security.



Useremail	Username	Mobile	Address	Status	Download
vishnu@gmail.com	vishnu	ed2778c4-a190-46a5-a304-4aa6a6bd2f1e	Towards Lightweight Provable Data Possession for Cloud Storage Using Indistinguishability Obfuscation.docx	decrypted	Download
vishnu@gmail.com	vishnu	8d8584e7-bc2f-4d27-851e-4c1fc9fa3833	FILE.txt	decrypted	Download

View uploaded data: The user can view the uploaded data here with encryption.



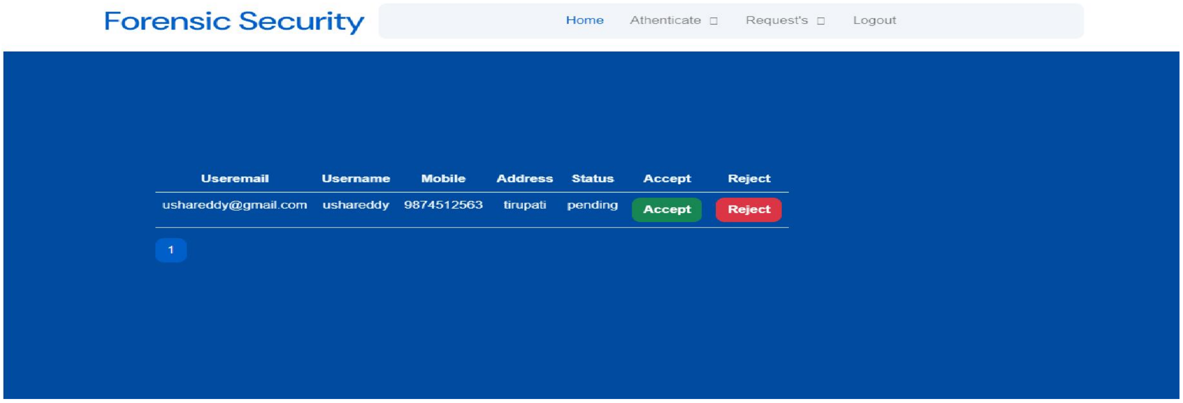
ADMIN LOGIN

Username: vishnu@gmail.com
Password: ····

Don't have an account? Forgot Password?

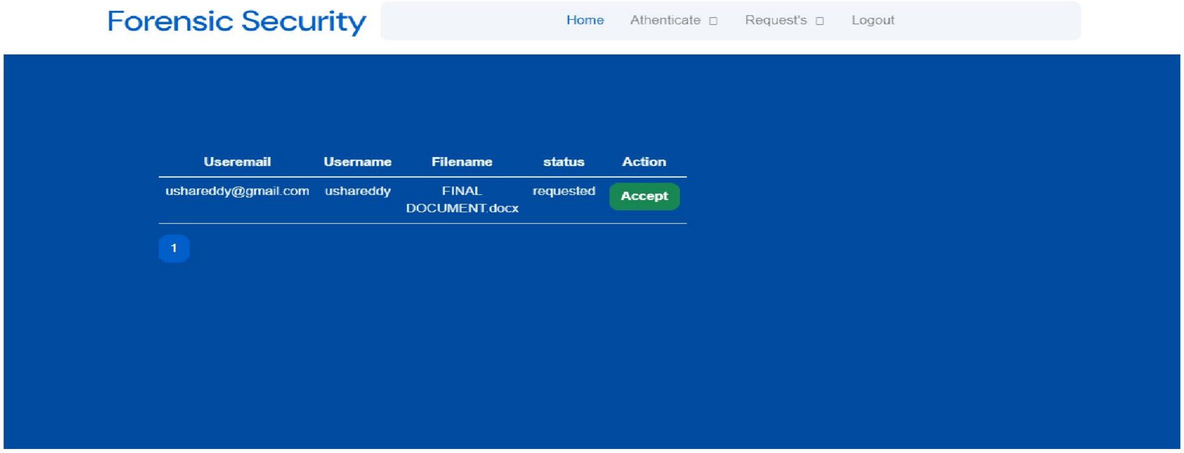
Admin login: the admin can login using their valid credentials.

DOI: 10.48175/IJARSCT-28047



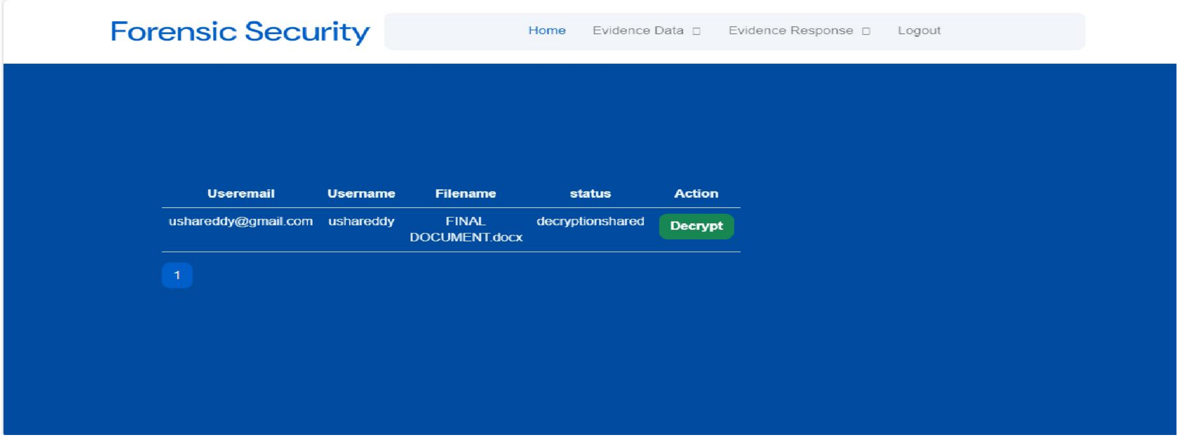
Useremail	Username	Mobile	Address	Status	Accept	Reject
ushareddy@gmail.com	ushareddy	9874512563	tirupati	pending	Accept	Reject

View users and authenticate: The admin can view the users and can authenticate or reject those.



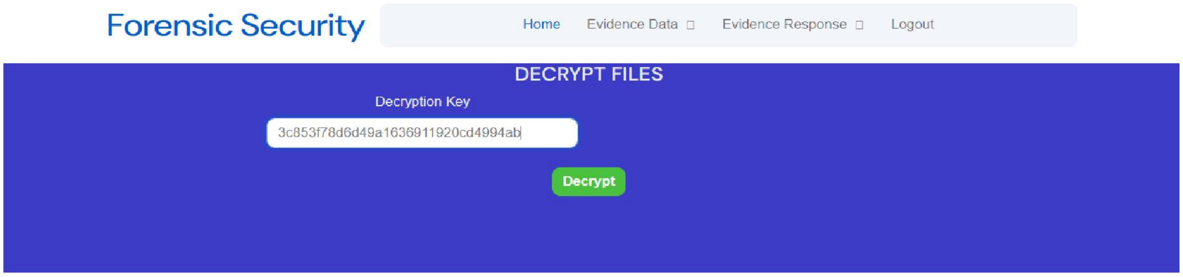
Useremail	Username	Filename	status	Action
ushareddy@gmail.com	ushareddy	FINAL DOCUMENT.docx	requested	Accept

View file accept: The admin can notified the file to access the upload file access to the users.



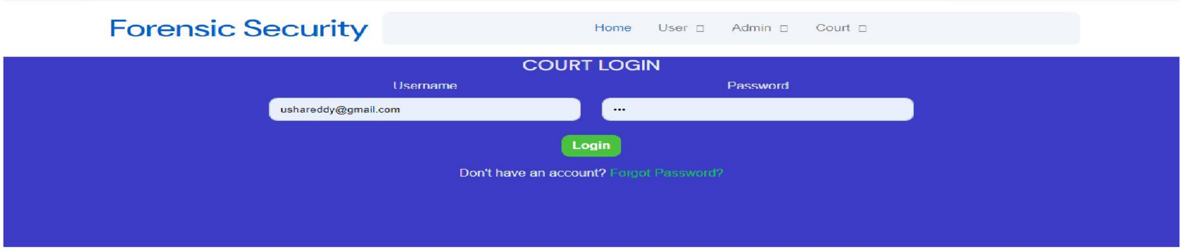
Useremail	Username	Filename	status	Action
ushareddy@gmail.com	ushareddy	FINAL DOCUMENT.docx	decryptionshared	Decrypt

View the response for file request: the user can view the file response from the admin.



Decryption Key: 3c853f78d6d49a1636911920cd4994ab

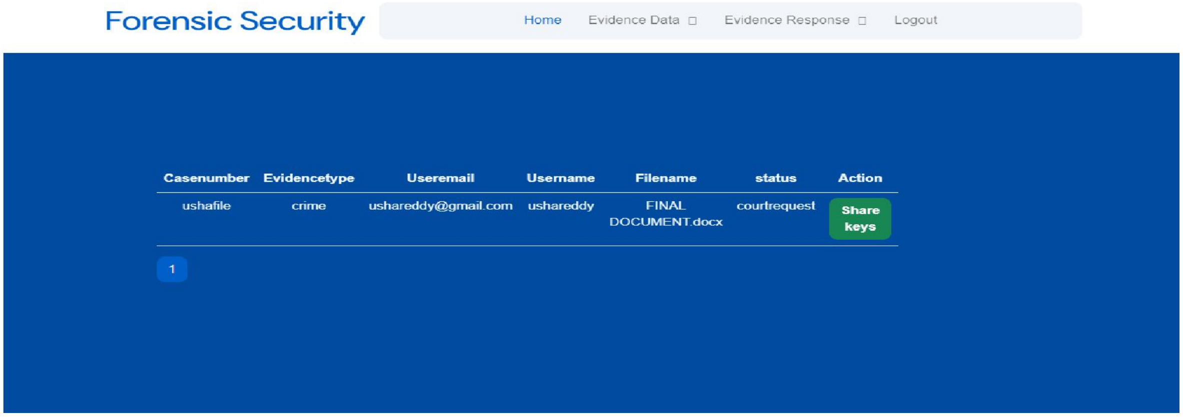
Decrypt data: The user can notified by the email from the admin once, and user can enter the decryption key to view the decrypted data.



Username: ushareddy@gmail.com

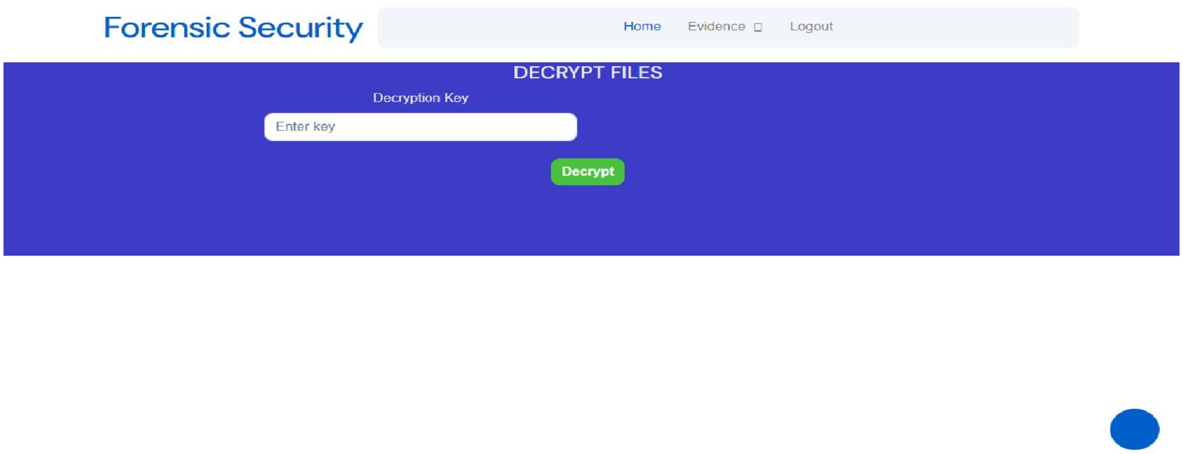
Password: •••

Court Login: The court can login using their valid default credentials.
View the all case files, and can request the file's over here.



Casenumber	Evidencetype	Useremail	Username	Filename	status	Action
ushafile	crime	ushareddy@gmail.com	ushareddy	FINAL DOCUMENT.docx	courtrequest	Share keys

User can notified: The user can notified that court request. And can share the keys of files.



Decrypt file: Decrypt the files and view the decrypted content.

V. CONCLUSION

he proposed **DFA-AOKGE** (Digital Forensic Architecture with Authentication and Optimal Key Generation-based Encryption) model presents a comprehensive and secure approach to preserving digital evidence in cloud-based environments. By integrating a **blockchain-distributed storage design**, **Secure Block Verification Mechanism (SBVM)**, **Enhanced Equilibrium Optimizer (EEO)** for key generation, and **Multikey Homomorphic Encryption (MHE)** for data confidentiality, the system effectively addresses the limitations of traditional forensic frameworks.

The decentralized architecture ensures resilience against single points of failure and unauthorized tampering, while the cryptographic techniques used enhance the robustness of evidence security during storage and transmission. Simulation results and module-wise implementation confirm that DFA-AOKGE provides superior performance in terms of encryption strength, key security, and forensic compatibility compared to existing models.

Overall, this architecture establishes a scalable and tamper-proof digital forensic solution suitable for modern cloud environments, and sets the foundation for future enhancements integrating real-time threat detection, AI-based anomaly analysis, and cross-platform forensic interoperability.

REFERENCES

[1]. "Optimal Multisecret Image Sharing Using Lightweight Visual Sign-Cryptography Scheme with Optimal Key Generation for Gray/Color Images" by A. Bachiphale and N. S. Zulpe (International Journal of Image and Graphics, 2023) — discusses a lightweight cryptographic method for secure image sharing with enhanced key generation.

[2]. "Internet-of-Forensic (IoF): A Blockchain-Based Digital Forensics Framework for IoT Applications" by G. Kumar et al. (Future Generation Computer Systems, 2021) — proposes a blockchain-integrated framework for forensics in IoT-based environments.

[3]. "Secure Forensic Data Transmission System in Cloud Database Using Fuzzy-Based Butterfly Optimization and Modified ECC" by L. Raji and S. T. Ramya (Transactions on Emerging Telecommunications Technologies, 2022) — presents a secure forensic transmission system leveraging optimization and ECC.

[4]. "Personal Authentication and Cryptographic Key Generation Based on Electroencephalographic Signals" by E. A. Abdel-Ghaffar and M. Daoudi (Journal of King Saud University - Computer and Information Sciences, 2023) — introduces biometric EEG signals for secure key generation and user authentication.

[5]. "Enhancing Blockchain Security in Cloud Computing with IoT Environment Using ECIES and Cryptography Hash Algorithm" by P. Velmurugadass et al. (Materials Today: Proceedings, 2021) — proposes hybrid cryptographic enhancements for blockchain-based IoT cloud systems.

[6]. "Artificial Neural Network and Symmetric Key Cryptography-Based Verification Protocol for 5G Enabled Internet of Things" by V. O. Nyangaresi et al. (Expert Systems, 2022) — integrates ANN with symmetric cryptography to secure 5G-based IoT communications.

[7]. "Enhancing Cloud Forensic Investigation System in Distributed Cloud Computing Using DK-CP-ECC Algorithm and EK-ANFIS" by S. Nasreen and A. H. Mir (Journal of Mobile Multimedia, 2023) — develops an intelligent encryption model for cloud forensic compatibility.

[8]. "Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection" by J. Du et al. (Security and Communication Networks, 2022) — proposes forensic algorithms to detect ransomware attacks before data loss occurs.

[9]. "Efficient and Reliable Forensics Using Intelligent Edge Computing" by A. Razaque et al. (Future Generation Computer Systems, 2021) — leverages edge computing for efficient and low-latency digital forensic processing.

[10]. "Employing an ECC-Based Hybrid Data Encryption Method to Improve Multitenancy Security in Cloud Computing" by M. Kashif et al. (REEDCON Conference Proceedings, 2023) — suggests hybrid ECC-based encryption for improved multitenancy cloud security.

[11]. "Improved Multisignature Scheme for Authenticity of Digital Documents in Digital Forensics Using Edward-Curve Digital Signature Algorithm" by G. Shankar et al. (Security and Communication Networks, 2023) — proposes a secure digital signature model for document verification in forensic chains.

[12]. "A Secure and Efficient Internet of Things Cloud Encryption Scheme with Forensics Investigation Compatibility Based on Identity-Based Encryption" by D. Unal et al. (Future Generation Computer Systems, 2021) — enables forensically compatible cloud encryption using identity-based cryptography.

[13]. "Towards an Optimal Security Using Multifactor Scalable Lightweight Cryptography for IoT" by S. Sheeja (C2I4 International Conference, 2022) — introduces scalable, lightweight multifactor encryption models for IoT applications.

[14]. "A Novel Blockchain Framework for Digital Forensics in Cloud Environment Using Multi-Objective Krill Herd Cuckoo Search Optimization Algorithm" by P. S. Apirajitha and R. R. Devi (Wireless Personal Communications, 2023) — develops a blockchain optimization model for forensic traceability and integrity.

[15]. "Lightweight Authentication for IoT/Cloud-Based Forensics in Intelligent Data Computing" by B. D. Deebak and F. AL-Turjman (Future Generation Computer Systems, 2021) — presents an efficient authentication framework for forensic systems in cloud-IoT platforms

DOI: 10.48175/IJARSCT-28047