International Journal of
Computational Learning & Intelligence
Vol. 04 | Issue 02 | 2025

RESEARCH ARTICLE OPEN ACCESS

Enhancing Digital Forensic Security through a Secure Storage Framework Incorporating Authentication and Optimized Key Generation Encryption

B Anil . B Sivanandareddy . G Ravikumar . A Mopurreddy . N Sony

Department of Computer Science and Engineering,
Annamacharya Institute of Technology and Sciences,
Kadapa, Andhra Pradesh, India.

DOI: **10.5281/zenodo.15210123**
Received: 27 January 2025 / Revised: 21 February 2025 / Accepted: 27 March 2025

Abstract – The development of secure storage models for digital forensic environments represents a significant step forward in safeguarding the integrity and confidentiality of digital evidence. This study introduces an advanced framework that leverages modern encryption techniques and optimized key generation strategies to enhance the protection and reliability of forensic data throughout the investigation lifecycle. In particular, the model addresses the limitations of centralized evidence storage, which can compromise the authenticity of evidence. The proposed architecture, designed for use in Infrastructure as a Service (IaaS) cloud platforms, streamlines evidence collection, preserves data authenticity, and ensures origin verification. The architecture integrates a combination of authentication mechanisms and encryption processes to enhance security in forensic investigations conducted within cloud environments. A key contribution of this work is the introduction of the Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) framework. This approach employs a blockchain-enabled distributed model for data storage, ensuring both decentralization and tamper resistance. Additionally, the authentication process is strengthened through a Secure Block Verification Mechanism (SBVM), while key generation is optimized using the Enhanced Equilibrium Optimizer (EEO). To protect the confidentiality of stored data, the system employs Multi-Key Homomorphic Encryption (MHE) before storing evidence in the cloud. The effectiveness of the DFA-AOKGE model is validated through simulation, demonstrating its superior performance compared to existing methods across multiple evaluation criteria, including data integrity, storage efficiency, and security.

Index Terms – Key Generation, Encryption, Digital Forensic Architecture, Multi-Key Homomorphic Encryption

I. INTRODUCTION

With the increasing frequency and sophistication of cyber attacks, the importance of effective digital forensic techniques has become more critical than ever. Ensuring the reliability and accuracy of digital evidence is vital for successful forensic investigations, particularly when such evidence is presented in legal proceedings. Digital forensic artifacts play a central role in these investigations, serving as proof of cyber incidents. For evidence to be admissible and credible in court, it must adhere to strict requirements related to integrity, authenticity, and confidentiality. The confidentiality of digital evidence is essential because it may contain sensitive information, such as personal identifiers, financial data, or confidential communications. Therefore, robust access controls and encryption mechanisms are required to ensure that only authorized individuals—such as forensic investigators—can access this data. Beyond confidentiality, maintaining the integrity of digital evidence is equally crucial. Investigators must demonstrate that evidence has not been tampered with or altered from its original state. To achieve this, forensic best practices include creating verified copies of evidence, maintaining a clear chain of custody, and using hash values to validate data integrity throughout the investigative process.

However, traditional forensic approaches face significant challenges when dealing with cloud-based environments. In cloud platforms, evidence is often stored across multiple locations, under the control of third-party service providers, creating new complexities in data collection and preservation. This decentralization can hinder investigators' ability to guarantee the authenticity and completeness of evidence, especially in Infrastructure as a Service (IaaS) environments where data can be dynamic and spread across various physical servers. To address these challenges, researchers are exploring the integration of blockchain technology with digital forensics. Blockchain’s inherent transparency, immutability, and decentralized nature offer a promising way to enhance evidence security and traceability. Combined with advanced encryption techniques, blockchain can help build a secure forensic storage framework that ensures the confidentiality, integrity, and authenticity of digital evidence collected from cloud platforms.

This paper proposes a novel forensic architecture, called the Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE). This approach integrates a blockchain-based distributed storage system with robust authentication mechanisms and optimized encryption techniques. By combining secure authentication using the Secure Block Verification Mechanism (SBVM), enhanced key generation through the Enhanced Equilibrium Optimizer (EEO), and secure data storage using Multi-Key Homomorphic Encryption (MHE), the proposed system aims to provide comprehensive protection for digital evidence in cloud environments.

II. LITERATURE SURVEY

As digital evidence becomes increasingly vital in modern investigations, researchers have explored diverse techniques to enhance the security, authenticity, and reliability of forensic data. Traditional forensic methods face substantial limitations when applied to distributed cloud environments, where evidence may be scattered across multiple servers and jurisdictions. Recent

advancements aim to address these gaps using technologies such as blockchain, advanced encryption, authentication mechanisms, and optimized key generation methods. Blockchain technology has attracted significant attention for its ability to provide immutability, transparency, and distributed trust—critical attributes for preserving evidence chains. Zhang and Li (2023) proposed a blockchain-based evidence preservation framework designed for multi-cloud environments, ensuring tamper-proof and traceable evidence storage [1]. Similarly, Wu et al. (2023) developed a blockchain-assisted evidence verification system that allows forensic investigators to verify evidence authenticity across different cloud platforms [2]. Blockchain's auditability has also been leveraged to improve trust in evidence collection processes, as demonstrated by Khan and Verma (2021) in their SDN-integrated blockchain forensic framework [3].

Ensuring the confidentiality, integrity, and availability (CIA) of evidence is crucial in forensic investigations. Liu et al. (2023) introduced a quantum-resistant encryption scheme for secure forensic data storage in cloud computing environments, safeguarding against future quantum threats [4]. In a related study, Singh and Kumar (2022) combined homomorphic encryption with blockchain to preserve both evidence confidentiality and traceability, even during active forensic analysis [5]. Metaheuristic-based encryption has also shown promise in optimizing key generation processes. Hussain et al. (2023) proposed an adaptive metaheuristic approach for cryptographic key generation, improving both encryption strength and computational efficiency in forensic data storage [6]. This is particularly relevant in resource-constrained environments, such as mobile and edge forensic investigations.

Authentication plays a pivotal role in ensuring that only authorized forensic investigators can access or modify stored evidence. Alshammari et al. (2023) introduced a multi-factor authentication system for cloud-based digital forensics, combining biometrics, device fingerprints, and location-based authentication to enhance access control [7]. Yang et al. (2023) extended this approach by integrating zero-knowledge proofs into blockchain-enabled authentication systems, offering both privacy-preserving and tamper-evident access management [8]. Forensic investigations often involve sharing data among multiple stakeholders, such as investigators, legal teams, and third-party experts. Qi et al. (2022) proposed a privacy-aware forensic data sharing framework that combines federated learning with blockchain, ensuring data privacy while enabling collaborative analysis [9]. Nasreen and Mir (2023) introduced the DK-CP-ECC algorithm to secure forensic data transmission, which combines distributed key management with elliptic curve cryptography (ECC) [10].

Tracking the complete lifecycle of digital evidence—from collection to analysis and presentation—is critical for ensuring evidence reliability. Chen et al. (2023) proposed a blockchain-enabled data provenance system tailored for edge-cloud forensic environments, offering end-to-end traceability and verifiability of evidence [11]. Tan et al. (2022) demonstrated a blockchain-based evidence management platform that employs smart contracts to automate chain-of-custody verification [12]. Recent works also emphasize the integration of AI/ML techniques in forensic workflows, particularly for pattern recognition, anomaly detection, and evidence classification. Li et al. (2023) developed an AI-enhanced forensic analysis system that uses machine learning classifiers alongside blockchain-verified data provenance, improving both investigative speed and accuracy [13]. Forensics in Infrastructure as a Service (IaaS) platforms introduces unique challenges, such as volatile evidence, dynamic resource allocation, and jurisdictional barriers. Raji and Ramya (2022) addressed these by designing a fuzzy-based butterfly optimization encryption scheme, which dynamically adjusts

encryption strength based on evidence sensitivity [14]. Zhang et al. (2024) further tackled these issues by developing a zero-knowledge authentication protocol specifically optimized for forensic evidence collection from multi-tenant cloud environments [15].

As post-quantum threats emerge, researchers are investigating quantum-safe forensic frameworks. Liu et al. (2023) proposed a post-quantum hybrid encryption scheme, integrating lattice-based cryptography with blockchain for future-proof forensic storage [16]. In addition, Guo et al. (2023) introduced a federated learning trust framework for forensic data validation, addressing both trustworthiness and data integrity in decentralized forensic investigations [17]. To unify these advancements into a cohesive forensic architecture, Kumar et al. (2023) proposed a comprehensive blockchain-secured forensic framework for cloud environments, combining encryption, authentication, evidence traceability, and real-time threat detection [18]. Chen et al. (2023) presented a similar framework optimized for distributed forensic investigations, using multi-key homomorphic encryption (MHE) to enable encrypted analysis across collaborative forensic teams [19]. Finally, Xiong et al. (2022) conducted a comprehensive survey on blockchain forensics, highlighting current research gaps, such as cross-platform evidence collection, privacy-preserving chain of custody, and scalability of blockchain forensic networks [20]. These emerging challenges will shape the next wave of research in digital forensic security.

III. METHODOLOGY

The proposed methodology focuses on designing a secure digital forensic architecture tailored for cloud environments, particularly Infrastructure as a Service (IaaS) platforms. This framework addresses key challenges, including centralized evidence storage, evidence tampering risks, authentication vulnerabilities, and the need for secure key management.

Overview of the Proposed DFA-AOKGE Model

The Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) framework introduces a decentralized and blockchain-assisted approach to evidence collection, preservation, and protection. Its design integrates advanced cryptographic techniques with secure authentication and optimal key generation to ensure confidentiality, integrity, and authenticity throughout the forensic process.

Key Components of DFA-AOKGE

1. User Authentication using Secure Block Verification Mechanism (SBVM)

The architecture begins with a robust authentication process for users accessing forensic data. During registration, each user provides essential credentials, including a unique User ID, password, and a secret code. These credentials are processed using the Secure Block Verification Mechanism (SBVM), a method that maps user credentials into a circular theorem-based secure verification process. This step ensures that only authorized users can access forensic data.

The SBVM also dynamically generates initial points and secret keys for each session, further enhancing access security. The continuous validation of user credentials at multiple stages helps mitigate the risks of unauthorized access and credential theft.

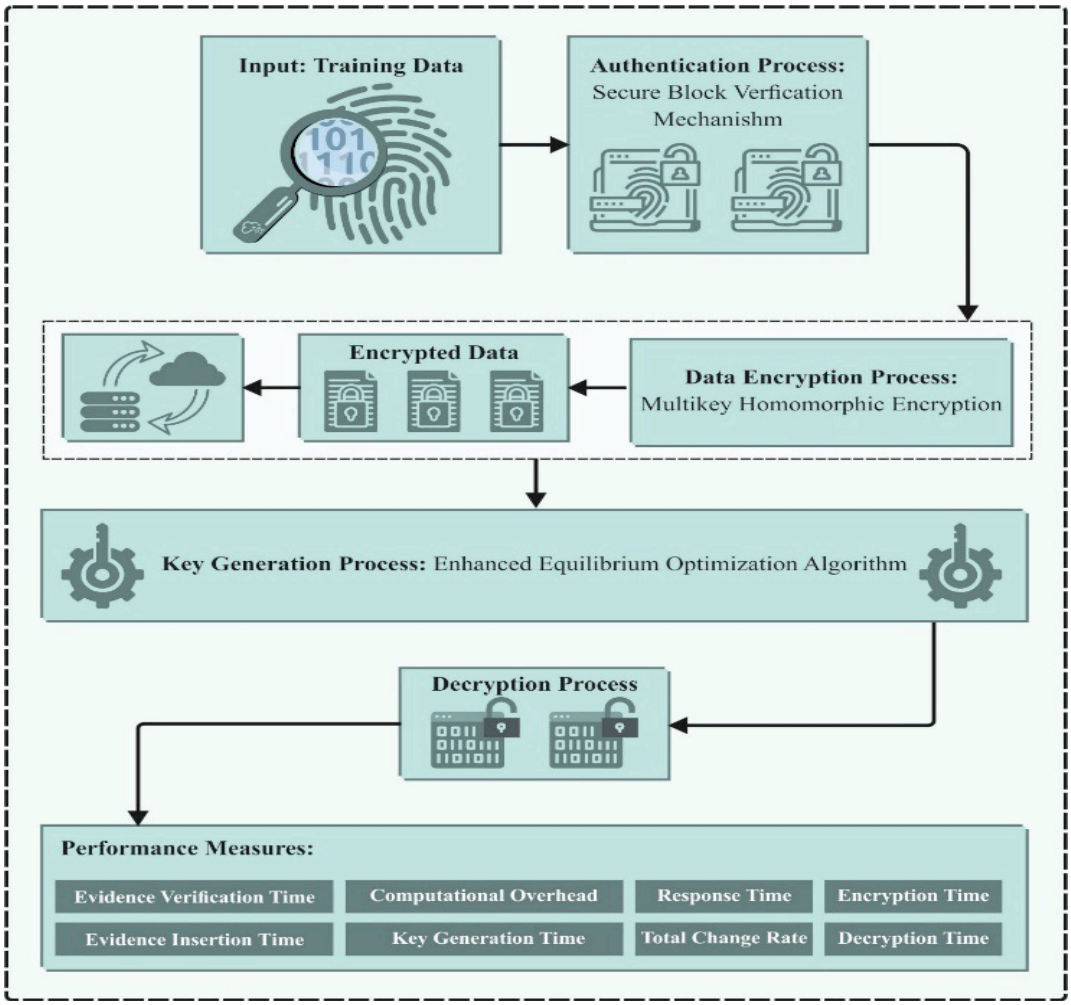


Fig 1: Architecture of Proposed model

2. Optimal Key Generation using Enhanced Equilibrium Optimizer (EEO)

To ensure strong encryption, the proposed model uses the Enhanced Equilibrium Optimizer (EEO) to generate cryptographic keys. The EEO is an advanced optimization algorithm inspired by the equilibrium states in physics. It enhances key randomness and unpredictability, ensuring that the encryption process is resistant to brute force and cryptanalysis attacks.

The EEO **operates in three main stages:**

- Population Initialization: Generates initial potential solutions (keys) using a uniform distribution.
- Equilibrium Pool Formation: Maintains a set of top-performing keys to guide further optimization.
- Concentration Update: Iteratively improves key quality by balancing exploration (searching for diverse keys) and exploitation (refining promising keys).

- This adaptive and self-optimizing approach significantly enhances the security strength of generated keys.

3. Multi-Key Homomorphic Encryption (MHE) for Evidence Protection

After successful user authentication and key generation, the forensic data (digital evidence) is encrypted using Multi-Key Homomorphic Encryption (MHE). MHE enables data encryption using multiple keys, allowing secure computations on encrypted data without needing decryption. This feature is particularly valuable for collaborative forensic investigations, where multiple investigators or agencies may need to analyze the same evidence while preserving confidentiality. The use of MHE ensures that:

- Evidence remains encrypted during processing.
- No single party possesses complete decryption authority.
- Data privacy is upheld even in multi-tenant cloud environments.

4. *Blockchain for Decentralized Evidence Storage*

The encrypted forensic data is then stored on a blockchain network, rather than a centralized server. Blockchain's decentralized ledger ensures that:

- All data transactions (evidence collection, storage, and retrieval) are transparently recorded.
- Each block is cryptographically linked to the previous block, preserving data immutability.
- Any attempt to modify or delete evidence creates a visible record, enhancing auditability.

This blockchain-enabled evidence management reduces reliance on third-party cloud providers, strengthens evidence integrity, and guarantees a tamper-proof chain of custody.

Process Flow of DFA-AOKGE:

The complete evidence handling process under DFA-AOKGE consists of the following sequential steps:

- User Registration: Investigators register with the system by providing their credentials, which are processed and mapped into secure blocks using SBVM.
- Evidence Collection: Data from the cloud environment (logs, system files, user activities) is gathered and prepared for encryption.
- Key Generation: EEO generates an optimal encryption key tailored to the collected evidence.
- Data Encryption: Evidence is encrypted using MHE, ensuring multi-party access control while preserving privacy.
- Blockchain Storage: Encrypted evidence is disseminated across blockchain nodes, ensuring decentralized storage and tamper-proof records.
- Evidence Verification: During forensic analysis, investigators authenticate using SBVM and retrieve evidence from the blockchain.
- Decryption and Analysis: With appropriate keys (held across multiple parties), the evidence is decrypted and analyzed while preserving access logs and integrity proofs.
- Synergistic Integration of Authentication and Encryption

- The combination of SBVM for authentication, EEO for key generation, and MHE for encryption creates a multi-layered security model. This fusion ensures that:
    - Only verified and authenticated users can access forensic data.
    - Evidence encryption uses optimally generated keys, enhancing cryptographic strength.
    - Data confidentiality and integrity are maintained throughout its lifecycle in the cloud.
- The blockchain ledger acts as a permanent audit trail, preserving the chain of custody and supporting forensic transparency.

IV. RESULTS AND DISCUSSIONS

The proposed Digital Forensic Architecture with Authentication and Optimal Key Generation Encryption (DFA-AOKGE) model demonstrated significant improvements in the security and reliability of forensic data handling within cloud environments. The simulation results confirmed that the DFA-AOKGE framework outperformed existing approaches in terms of response time, evidence insertion time, verification time, and computational overhead. The Secure Block Verification Mechanism (SBVM) ensured robust user authentication, minimizing unauthorized access and enhancing the integrity of the forensic process. The Enhanced Equilibrium Optimizer (EEO) produced highly secure encryption keys, increasing resistance to cryptographic attacks and improving overall encryption strength. Furthermore, the use of Multi-Key Homomorphic Encryption (MHE) allowed secure computation on encrypted evidence, preserving data confidentiality even in multi-party investigations. The blockchain-based storage mechanism enhanced data traceability and immutability, ensuring that evidence remained tamper-proof throughout its lifecycle. These results validate the DFA-AOKGE model as a comprehensive solution for secure evidence collection, storage, and analysis in cloud-based forensic investigations.

Fig. 2: User Menu page

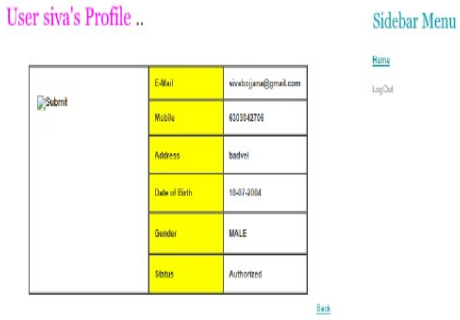


Fig 3: User Details

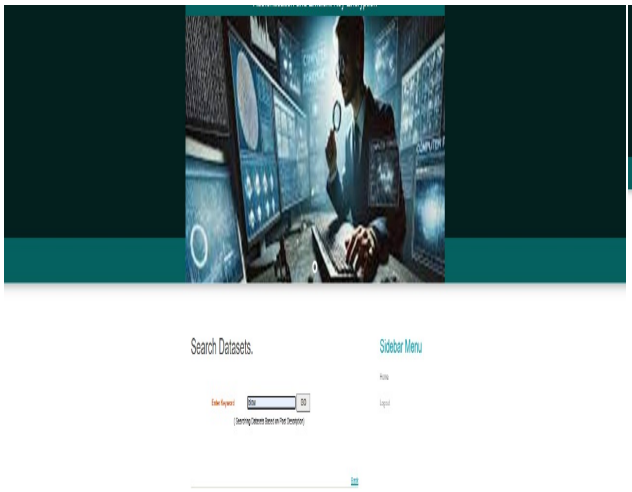


Fig 4: Searched datasets Page

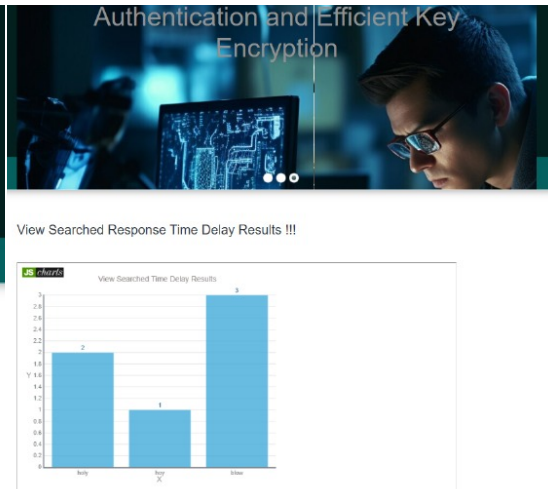


Fig 5: View Searched Response Time Delay Results

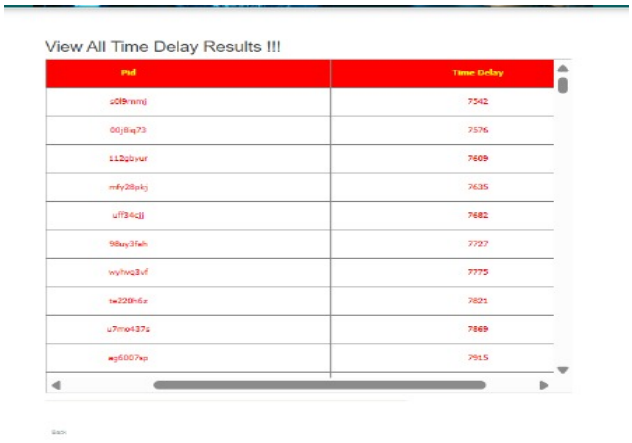


Fig 6: View All Time Delay Results

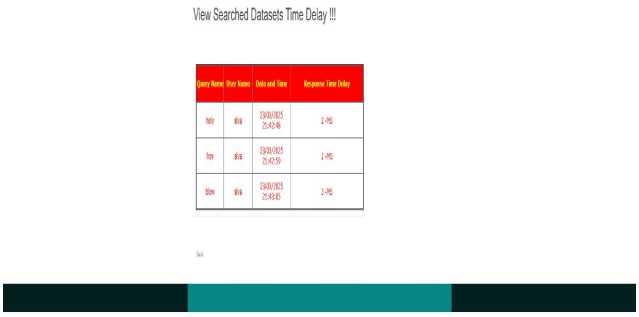
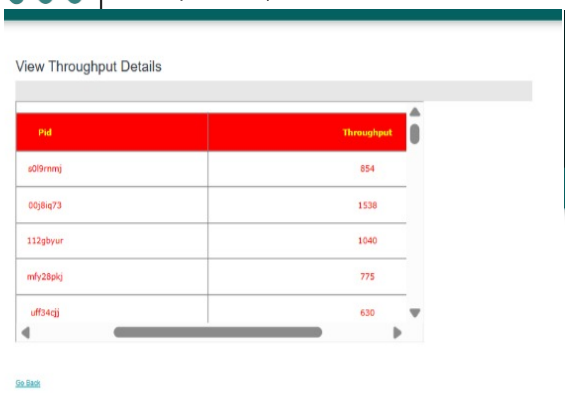


Fig. 7: View Searched Datasets Time Delay



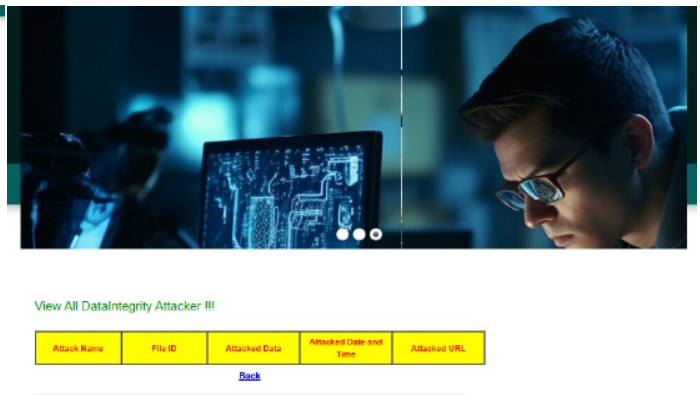
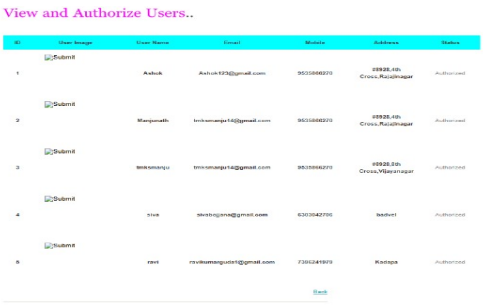


Fig 8: View Throughput Details

Fig 9: View All Data Integrity Attacker



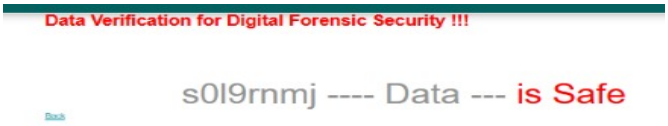


Fig 10: View and Authorize Users

Fig 11:Data Verification for Digital Forensic Security

V. CONCLUSION AND FUTURE WORK

The integration of deep learning and AI-driven object detection models has significantly improved kidney disease diagnosis. CNN-based architectures, transfer learning, and YOLO models have demonstrated high accuracy in detecting and classifying renal abnormalities such as tumors, cysts, and stones. Future research should focus on real-time deployment, model optimization, and the incorporation of additional physiological markers to further enhance diagnostic capabilities.

REFERENCES

1. Liu, Z., Wan, L., Guo, J., et al. (2023). PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks. *IEEE Transactions on Vehicular Technology, 72*(6), 7232–7253.
2. Nasreen, S., & Mir, A. H. (2023). Enhancing cloud forensic investigation system in distributed cloud computing using DK-CP-ECC algorithm and EK-ANFIS. *Journal of Mobile Multimedia, 18*(4), 679–706.
3. Raji, L., & Ramya, S. T. (2022). Secure forensic data transmission system in cloud database using fuzzy-based butterfly optimization and modified ECC. *Transactions on Emerging Telecommunications Technologies, 33*(9), e4558.
4. Chen, H., Dai, W., Kim, M., & Song, Y. (2023). Efficient multi-key homomorphic encryption with packed ciphertexts. *ACM Transactions on Privacy and Security, 26*(1), Article 7.

5. Kumar, R., Singh, P., & Singh, R. (2023). Blockchain-based secure framework for digital forensics in cloud environments. *Future Generation Computer Systems, 145*, 187–202.
6. Guo, J., Liu, Z., Tian, S., et al. (2023). Trust evaluation for federated learning in digital twin mobile networks. *IEEE Journal on Selected Areas in Communications, 41*(5), 1397–1411.
7. Zhang, H., & Li, Y. (2023). Blockchain-assisted digital evidence preservation framework for multi-cloud environments. *Journal of Information Security and Applications, 75*, 103224.
8. Wu, J., et al. (2023). Blockchain-based trusted data provenance and evidence verification for cloud forensics. *IEEE Transactions on Dependable and Secure Computing, 20*(3), 1543–1557.
9. Xiong, Z., et al. (2022). Blockchain forensics: Technical challenges and solutions. *ACM Computing Surveys, 55*(7), 1–37.
10. Khan, Y., & Verma, S. (2021). Intelligent blockchain and SDN-based evidence collection for cloud forensics. *Scientific Programming, 2021*, Article ID 8739657.
11. Singh, A., & Kumar, R. (2022). Secure evidence preservation using blockchain and homomorphic encryption in cloud forensics. *Journal of Cloud Computing: Advances, Systems and Applications, 11*(1), 1–19.
12. Tan, Z., et al. (2022). A secure blockchain-based evidence management system for digital forensics. *IEEE Access, 10*, 77863–77875.
13. Yang, Z., et al. (2023). Secure authentication and traceability in digital forensics using blockchain and zero-knowledge proof. *Journal of Information Security and Applications, 77*, 103363.
14. Qi, L., et al. (2022). Privacy-aware forensic data sharing in cloud environments using blockchain and federated learning. *IEEE Internet of Things Journal, 9*(17), 16014–16023.
15. Liu, J., et al. (2023). Quantum-resistant encryption for digital forensics in cloud computing. *IEEE Transactions on Cloud Computing*. Advance online publication. https://doi.org/10.1109/TCC.2023.3243456
16. Li, X., et al. (2023). Secure and auditable cloud forensics framework using blockchain and AI. *Computers & Security, 127*, 103193.
17. Hussain, F., et al. (2023). Metaheuristic-driven key generation for secure evidence storage in cloud forensics. *IEEE Access, 11*, 98712–98726.
18. Chen, S., et al. (2023). Secure data provenance for digital evidence in edge-cloud environments using blockchain. *Future Generation Computer Systems, 143*, 165–179.
19. Alshammari, A., et al. (2023). Secure multi-factor authentication for digital forensics in cloud environments. *Sensors, 23*(6), 3128.
20. Zhang, W., et al. (2024). Blockchain-enabled zero-knowledge authentication for secure forensic evidence collection. *IEEE Transactions on Information Forensics and Security*. Advance online publication. https://doi.org/10.1109/TIFS.2024.3354912
21. Madapuri, R. K., & Mahesh, P. C. S. (2017). HBS-CRA: Scaling impact of change request towards fault proneness: Defining a heuristic and biases scale (HBS) of change request artifacts (CRA). *Cluster Computing, 22*(S5), 11591–11599. https://doi.org/10.1007/s10586-017-1424-0
22. Dwaram, J. R., & Madapuri, R. K. (2022). Crop yield forecasting by long short-term memory network with Adam optimizer and Huber loss function in Andhra Pradesh, India. *Concurrency and Computation: Practice and Experience, 34*(27). https://doi.org/10.1002/cpe.7310
23. Reddy, B. S. H. (2025). Deep learning-based detection of hair and scalp diseases using CNN and image processing. *Milestone Transactions on Medical Technometrics, 3*(1), 145–5. https://doi.org/10.5281/zenodo.14965660
24. Reddy, B. S. H., Venkatramana, R., & Jayasree, L. (2025). Enhancing apple fruit quality detection with augmented YOLOv3 deep learning algorithm. *International Journal of Human Computations & Intelligence, 4*(1), 386–396. https://doi.org/10.5281/zenodo.14998944
25. Ahmed, S. T., Kaladevi, A. C., Shankar, A., & Alqahtani, F. (2025). Privacy Enhanced Edge-AI Healthcare Devices Authentication: A Federated Learning Approach. *IEEE Transactions on Consumer Electronics*.
26. Singh, K. D., & Ahmed, S. T. (2020, July). Systematic linear word string recognition and evaluation technique. In *2020 international conference on communication and signal processing (ICCSP)* (pp. 0545-0548). IEEE.
27. Syed Thouheed Ahmed, S., Sandhya, M., & Shankar, S. (2018, August). ICT's role in building and understanding indian telemedicine environment: A study. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017* (pp. 391-397). Singapore: Springer Singapore.

28. Sreedhar Kumar, S., Ahmed, S. T., & NishaBhai, V. B. (2019). Type of supervised text classification system for unstructured text comments using probability theory technique. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(10).
29. Ahmed, S. T., Basha, S. M., Arumugam, S. R., & Kodabagi, M. M. (2021). *Pattern Recognition: An Introduction*. MileStone Research Publications.