Advanced Security in Digital Forensics: Authenticated Storage with Key Based Encryption

R.Ajay[1], Syed Mohammad Shoaib[2], S Indra Sai[3], P. Sonith[4],Mr.O G Suresh Kumar[5], Mr.Pandreti Praveen[6], Dr. R Karunia Krishnapriya[7], Mr. V.Shaik Mohammad Shahil[8], Mr.N.Vijaya Kumar[9]
[1,2,3,4] B.Tech Student, [5,6,8,9] Assistance Professor, [7]Associate Professor,
Department of CSE, Sreenivasa Institute of Technology and Management Studies, Chittoor.

***Abstract*— The digital forensics industry requires comprehensive solutions to protect digital evidence faces major challenges. The cloud forensics discipline protects digital evidence through modern techniques that lose credibility when all evidence is stored in one location. This paper presents a novel approach to digital forensic architecture, titled "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption." Our system brings together SBVM and EEO for security creation while meeting both reliability and strong encryption standards. Our system selects ECC encryption because this technology offers strong security protection. Following encryption the data travels to secure storage spaces on our cloud platform. Our solution delivers higher security outcomes than current practices plus enhances dependability and efficiency for forensic work in cloud settings.**

***Keywords*- Digital forensics, cloud forensics, secure block verification mechanism, optimal key generation, enhanced equilibrium optimizer, Elliptic Curve Cryptography, data encryption, cloud storage, digital evidence security, forensics architecture, performance metrics.**

I. INTRODUCTION

Our digital transformation era saw cloud computing become popular because it changed how people and companies handle and access digital data. Cloud adoption now affects digital forensics practices because it creates new problems when protecting digital evidence. In cloud environments, where data is distributed across various locations, frequently updated, and subject to various online threats such as hacking, data tampering, and unauthorized access, the need for robust security and integrity mechanisms has never been more critical. Traditional digital forensic methods, which are typically designed for centralized storage systems, struggle to address these issues in the cloud due to the inherent complexity and dynamic nature of cloud infrastructure. The lack of efficient mechanisms for evidence authentication, secure storage, and reliable retrieval further compounds these challenges.

To address these growing concerns, this project presents an innovative forensic architecture called "Advanced Security in Digital Forensics: Authenticated Storage with Key- Based Encryption." This new approach combines the strengths of modern cryptographic and optimization technologies to create a secure and efficient framework for managing digital evidence in cloud environments. One of the key features of the proposed architecture is the Secure

Block Verification Mechanism (SBVM), which is designed to authenticate evidence blocks by verifying their integrity and ensuring they have not been tampered with during storage or transfer. SBVM operates by using hash-based methods and digital signatures to ensure the authenticity of each data block, making it resistant to alterations, whether malicious or accidental.

A major challenge in digital forensics is the management of cryptographic keys. For this reason, the architecture introduces an Enhanced Equilibrium Optimizer (EEO) model for generating secret keys used in encryption processes. The EEO model optimizes the key generation process by considering multiple factors such as security strength, computational efficiency, and resource consumption. This allows for the creation of highly secure yet computationally efficient keys, which are crucial for maintaining the performance of cloud-based systems without sacrificing security.

Our proposal uses ECC encryption to strengthen the security of stored data. ECC solves security problems effectively using shorter keys which decreases the hardware resources needed compared to RSA. ECC suits cloud computing because cloud

systems typically run on constrained resources with high performance needs. The cloud system safely stores encrypted data so that authorized persons have access to the evidence and unauthorized persons cannot.

Our design benefits from easy expansion capacity. Our system handles huge digital evidence collections effectively while staying fast. Cloud storage lets the system handle more forensic data while keeping excellent performance which supports today's bigger distributed law enforcement work.

Adding cloud storage helps us easily access evidence correctly while keeping our data safe. Officials can gather and examine digital evidence quickly which makes their work faster and increases digital investigation outcomes. Fast evidence access helps investigators complete their work quickly because time-sensitive cases require fast responses for successful digital forensics.

Our project uses modern technology while fixing historic evidence inspection problems to develop a practical secure digital forensics system. The system helps forensic investigators of all backgrounds keep their digital evidence secure while preserving evidence authenticity and simplifying evidence storage or retrieval operations. This advanced architecture responds to cloud challenge growth to offer digital forensics tools that protect evidence quality and make investigators work faster and more effective

A. Objective Of The Study

The objective of this research is to develop an advanced digital forensic architecture, titled "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption," to address the challenges of securing and preserving digital evidence in cloud environments. This architecture aims to enhance security and reliability by incorporating a Secure Block Verification Mechanism (SBVM) for robust authentication, utilizing an Enhanced Equilibrium Optimizer (EEO) model for efficient key generation, and employing Elliptic Curve Cryptography (ECC) for strong data encryption. By achieving these goals, the proposed model seeks to outperform existing approaches in ensuring the integrity, confidentiality, and accessibility of digital evidence while enhancing the efficiency and reliability of cloud-based forensic investigations.

B. Scope of the Study

This research focuses on developing a secure and efficient digital forensic architecture tailored for cloud environments, addressing challenges in evidence integrity, authentication, and storage. It incorporates a Secure Block Verification Mechanism (SBVM) for authentication, an Enhanced Equilibrium Optimizer (EEO) for key generation, and Elliptic Curve Cryptography (ECC) for encryption. Designed for scalability and adaptability, the architecture aims to support secure and reliable evidence management for forensic investigations, providing improved performance and practical applicability in cloud-based scenarios.

C. Problem statement

The field of digital forensics faces significant challenges in ensuring the security, integrity, and reliability of digital evidence, particularly in cloud environments where centralized evidence collection and storage are vulnerable to online threats and unauthorized access. Existing approaches often lack robust mechanisms for authentication, efficient encryption, and secure key management, leading to compromised evidence integrity and reliability. This highlights the need for a novel forensic architecture that can effectively address these limitations by providing enhanced security, reliable authentication, and efficient data management to safeguard digital evidence in cloud-based forensic investigations.

II. RELATED WORK

[1] Biedermann, A., & Taroni, F. (2018) The role of forensic science in the criminal justice system: A reflection on the concept of evidence and the challenges of advancing towards new paradigms.This study emphasizes the transformative role of forensic science in strengthening the criminal justice system. By examining the evolving nature of forensic evidence, the research underscores the limitations of traditional paradigms in addressing the complexity of modern evidence interpretation. The study advocates for the integration of forensic methods with broader scientific principles to improve evidence credibility and reliability. It also highlights the need for interdisciplinary

collaboration and the adoption of innovative technologies to overcome challenges in forensic analysis, interpretation, and presentation in courtrooms.

[2] Dykstra, J., & Sherman, A. T. (2013) Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. This research introduces FROST, a specialized suite of digital forensic tools developed for the OpenStack cloud platform, addressing challenges unique to virtualized infrastructures. The study demonstrates how FROST facilitates secure, scalable, and efficient forensic investigations within cloud environments. Key contributions include methods for the collection, preservation, and analysis of data in a virtualized setting while maintaining chain-of-custody integrity. The implementation of FROST showcases its utility in reducing complexities associated with data volatility, multi-tenancy, and remote storage, ultimately setting a benchmark for future forensic tools in cloud ecosystems.

[3] Stallings, W. (2016) Cryptography and network security: Principles and practice. This comprehensive text serves as a cornerstone for understanding cryptographic methods and network security principles. It provides an in- depth exploration of encryption techniques, authentication protocols, and secure communication mechanisms. These principles are crucial for implementing robust digital forensic processes and protecting sensitive data. The book also delves into key management strategies, digital signatures, and public key infrastructures, offering practical insights for securing forensic evidence, ensuring data integrity, and safeguarding systems from cyber threats.

[4] Wang, L., Zhang, Z., & Hung, P. C. K. (2012) Cloud computing security: Fundamentals, mechanisms, and applications. This research outlines the foundational principles and security mechanisms necessary for safeguarding cloud computing environments. It offers a detailed analysis of the unique challenges posed by cloud ecosystems, including data breaches, unauthorized access, and regulatory compliance. The study provides actionable solutions for secure application development in the cloud, such as encryption, access control, and intrusion detection systems. These mechanisms play a vital role in forensic investigations within cloud environments by ensuring secure data acquisition, storage, and analysis while maintaining evidence integrity.

[5] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2010) Toward secure and dependable storage services in cloud computing. This study proposes a robust framework for enhancing the security and dependability of cloud storage services. By focusing on key aspects like data integrity, confidentiality, and availability, the research addresses critical challenges faced by cloud storage systems. The proposed mechanisms, including dynamic data auditing and distributed storage verification, mitigate risks related to data tampering and loss. These advancements are instrumental for forensic investigations, ensuring that stored evidence remains trustworthy, tamper- proof, and readily accessible during legal proceedings.

III. PROPOSED CLOUD-BASED SECURE FINGERPRINT AUTHENTICATION AND FILE MANAGEMENT SYSTEM

The proposed system enhances cloud forensics by incorporating authenticated storage and key-based encryption. It uses a secure block verification mechanism (SBVM) to ensure evidence integrity, while secret keys are generated using an Enhanced Equilibrium Optimizer (EEO) model. Data is encrypted with Elliptic Curve Cryptography (ECC) and securely stored on the cloud, ensuring both security and privacy. Simulation results show that this approach outperforms existing methods in terms of security, reliability, and efficiency.

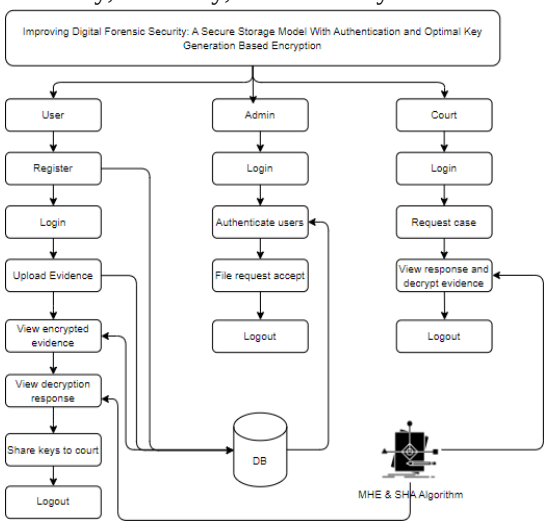


Fig 1: Flow chart of Advanced Security In Digital Forensics: Authenticated Storage With Key Based Encryption

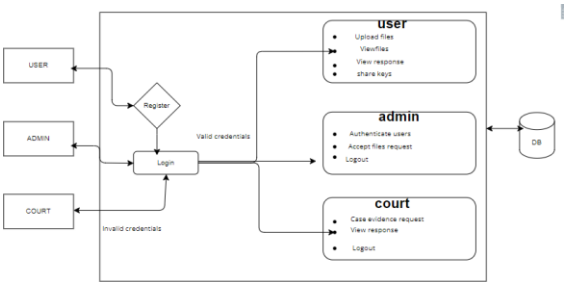


Fig 2: Flow chart of Advanced Security In Digital Forensics: Authenticated Storage With Key Based Encryption

A. Methods

ECC technology develops safe encryption styles through elliptic curves that need less computing power. The ECC system protects data at strength levels similar to RSA but needs only compact encryption keys. Due to their short keys ECC offers faster processing on small devices in both mobile and Internet of Things functions. Thanks to ECDLP and elliptic curve algebra your data stays protected within the Elliptic Curve Cryptography system platform. Organizations use ECC security tools because these tools shield internet services from data theft using SSL/TLS certificates and digital signing methods.

B. ECC shows top-level scalability while maintaining excellent system speed. To achieve an equivalent level of protection ECC uses a 256-bit key which requires far less processing and usage space than RSA's 3072- bit key. ECC offers this high efficiency that makes it ideal for Bitcoin use because the network depends on ECC for protecting digital transactions and user signatures. ECC helps build many cryptographic tools by letting users use it for public-key encryption digital signatures and key exchange both in symmetric and asymmetric systems. ECC stays important for secure communication as people need better protection without higher processing costs.

C. Advantages

The following are the advantages of our Cloud-Based Secure Fingerprint Authentication and File Management System:

- Smaller Key Sizes: Offers equivalent security to RSA with much smaller key sizes.
- Efficient Computation: Faster encryption/decryption with less computational overhead.
- Low Resource Consumption: Uses less memory, bandwidth, and power, ideal for resource-constrained devices.
- High Security: Strong protection based on the difficult elliptic curve discrete logarithm problem (ECDLP).
- Scalable: Provides adjustable security levels with smaller keys.

IV. MODULES AND ITS IMPLEMENTATION

User:

1. Login: Investigators log into the system using their credentials.
2. Register: Users can register with providing the required information.
3. Request to admin for share data: The case user should be take a permission from the admin to share the evidence information to the court.
4. View Decryption key response from admin: The admin should be share the decryption key's to the user for decrypt the data
5. Upload Evidence Data: The case user can able to share the evidence information with the encryption format with the decryption key to the requested court.
6. Share to court: Now The user can share the evidence information to the court.
7. Logout: The user should be logout.

Admin Modules:

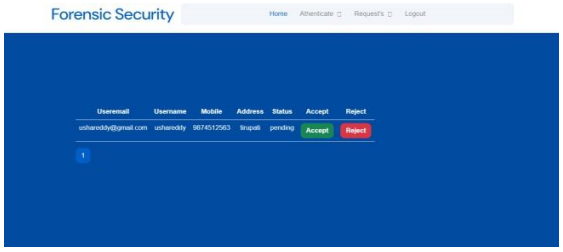
1. Login: Admins log into the system using their credentials.
2. View Users: Admins view details of all registered users.
3. Manage Evidence: Admins oversee the evidence data collection, and storages of that digital evidence.
4. Monitor Encryption and Key Generation: Admins supervise encryption and key generation processes to the users.
5. Logout: Admin can Logout.

Court Module:

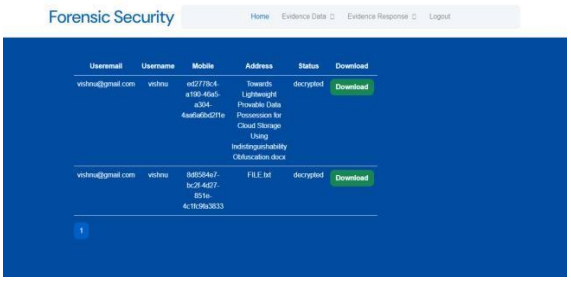
1. Login: Court can login using default credentials.
2. View the case numbers: the court can view the case numbers and can request for file access from evidences.
3. View response: The court can view the evidence response for decryption key from the case users.
4. Logout: the court can logout successfully.

V. RESULTS

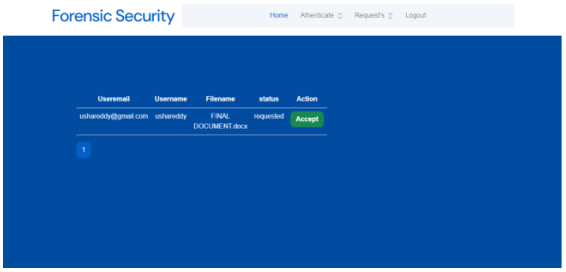
View users and authenticate: The admin can view the users and can authenticate or reject those.



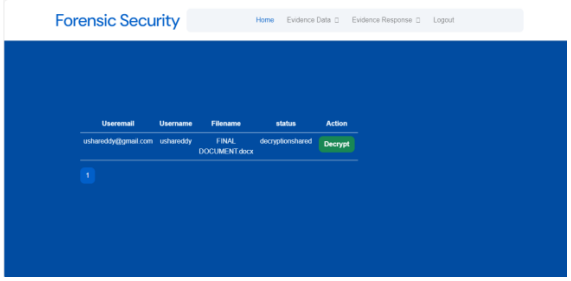
View uploaded data: The user can view the uploaded data here with encryption.



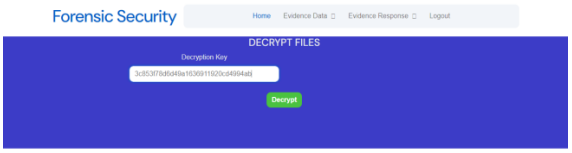
View file accept: The admin can notified the file to access the upload file access to the users.



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



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.



VI. CONCLUSION

In conclusion, the proposed "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption" architecture provides a robust solution to the challenges of securing digital evidence in cloud environments. By integrating secure block verification, key-based encryption using an Enhanced Equilibrium Optimizer model for key generation, and Elliptic Curve Cryptography for data encryption, this approach ensures both the integrity and confidentiality of digital evidence. The simulation results validate its superior performance, demonstrating improved security, reliability, and efficiency compared to existing methods, making it a promising advancement for digital forensics in cloud-based settings.

VII. FUTURE ENHANCEMENT

Future enhancements to the proposed architecture could involve incorporating advanced machine learning techniques for real-time threat detection and dynamic adaptation to evolving cyberattacks, further improving the system's security. Additionally, integrating decentralized storage solutions, such as blockchain, could enhance evidence integrity and transparency by providing an immutable ledger of data access and modifications. Exploring lightweight cryptographic algorithms optimized for cloud environments could also improve performance without compromising security. Furthermore, the system could be extended to support multi-cloud environments, ensuring scalability and broader applicability across diverse forensic scenarios, thereby strengthening the resilience of digital forensics in complex cloud ecosystems.

VIII. REFERENCES

[1] Biedermann, A., & Taroni, F. (2018). The role of forensic science in the criminal justice system: A reflection on the concept of evidence and the challenges of advancing towards new paradigms. Forensic Science International, 289, 112–123. https://doi.org/10.1016/j.forsciint.2018.04.003

[2] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digital Investigation, 10(1), S87–S95.

https://doi.org/10.1016/j.diin.2013.06.008

[3] Stallings, W. (2016). Cryptography and network security: Principles and practice. Pearson Education.

[4] Wang, L., Zhang, Z., & Hung, P. C. K. (2012). Cloud computing security: Fundamentals, mechanisms, and applications. Advances in Information Security, 95, 1–34. https://doi.org/10.1007/978-1-4419-9445-4_1

[5] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2010). Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220–232. https://doi.org/10.1109/TSC.2011.24

[6] Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, 268–275. https://doi.org/10.1109/CLOUD.2010.41

[7] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342

[8] Miller, J. B., & Paruchuri, V. (2020). Cloud-based digital forensic frameworks: Challenges and opportunities. Journal of Cybersecurity and Privacy, 2(3), 255–270. https://doi.org/10.3390/jcp2030016

[9] Kaur, P., & Singh, M. (2017). A review on the role of cryptography in the field of cloud forensics. International Journal of Computer Science and Information Security, 15(2), 90–95.

[10] Harris, S. (2019). Cloud forensic techniques and their implementation in securing digital evidence. Journal of Digital Forensics Practice, 11(4), 256–265. https://doi.org/10.1080/15567281.2019.1652783