Twin Route Forensics: Investigative Framework for Restoring Altered Text in Digital Forensics Using Cryptography

[1]Dr. Y. Chitti Babu,[2]Vardhanapu Surya Prakash,[3]Tata Rajeswari,[4]Viswanadhapalli Chandu

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

Digital text evidence plays a critical role in cybercrime investigations; however, such data is highly vulnerable to unauthorized modification and tampering, which affects its credibility during forensic analysis. Most existing encryption-based systems focus primarily on data confidentiality and fail to verify whether the stored content has been altered. This paper presents TwinRoute Forensics, a secure investigative framework designed to protect, verify, and restore digital text evidence using cryptographic techniques. The system integrates user authentication, Advanced Encryption Standard (AES) encryption, and SHA-256 hash-based integrity verification to ensure that only original and unaltered evidence can be accessed and restored. Text data is encrypted, stored with a unique record identifier, and verified for integrity before controlled decryption. The proposed system enhances forensic reliability, strengthens chain-of-custody compliance, and ensures trustworthiness of digital evidence in cyber investigations.

KeyWords: ***Digital Forensics, AES Encryption, SHA-256, Text Integrity, Cyber Security, Evidence Verification, Cryptography***

INTRODUCTION

Digital forensics has become an essential domain in cybercrime investigations, where digital text evidence such as emails, chat logs, documents, and system logs plays a vital role. Ensuring the authenticity and integrity of such evidence is critical, as even minor alterations can invalidate legal proceedings and forensic conclusions. Traditional systems primarily focus on encrypting data to protect confidentiality but often overlook integrity verification before decryption. The increasing frequency of cyber-attacks and digital fraud highlights the need for forensic systems that

not only secure evidence but also verify its originality. Without proper integrity checks, encrypted evidence may still be tampered with, leading to unreliable forensic outcomes. To address these challenges, Twin Route Forensics introduces a secure and reliable framework that combines authentication, encryption, and hash-based verification. The system ensures that text evidence can only be restored after successful integrity validation, thereby improving the credibility and reliability of digital forensic investigations.

LITERATURE SURVEY

Several studies have focused on securing digital data using cryptographic techniques. Stallings (2020) discussed the importance of AES encryption and SHA-based hashing for ensuring data confidentiality and integrity, but highlighted the absence of forensic-oriented validation mechanisms. Schneier (2019) emphasized cryptographic hashing for tamper detection but did not address controlled restoration of altered data. Kahate (2018) explored authentication-based security models for textual data, yet lacked a forensic workflow for evidence recovery. Other studies proposed secure storage systems but failed to integrate integrity verification before decryption, making them unsuitable for forensic applications.The proposed work differs by incorporating pre-decryption integrity verification and forensic-controlled restoration, ensuring only authentic evidence is accessed.

RELATED WORK

Previous research in digital security focused on encryption algorithms, authentication mechanisms, and secure databases. Most systems rely on symmetric encryption and access control to protect data. However, these approaches typically decrypt data without validating whether it has been altered.

TwinRoute Forensics adopts a forensic-driven development approach using cryptographic algorithms integrated into a web-based framework. The workflow includes secure user authentication, encrypted storage, integrity verification using SHA-256, and controlled decryption, which ensures forensic reliability and trust.

EXISTING SYSTEM

Existing digital text protection systems primarily rely on basic user authentication and encryption techniques to secure sensitive information. In these systems, text data is encrypted during storage and directly decrypted upon user request without performing any integrity verification. Although encryption ensures data confidentiality, it does not guarantee that the stored evidence has remained

unaltered. As a result, these systems are unable to detect unauthorized modifications or tampering of digital text evidence. The absence of forensic compliance mechanisms reduces the reliability and trustworthiness of such systems, making them unsuitable for legal and forensic investigations where evidence authenticity is critical.

PROPOSED SYSTEM

The proposed system introduces a forensic-grade framework specifically designed to protect, verify, and restore digital text evidence with high reliability. Each submitted text input is encrypted using the Advanced Encryption Standard (AES) algorithm and simultaneously processed with the SHA-256 hashing algorithm to generate a unique integrity value before storage. A distinct record identifier is assigned to every evidence entry to ensure traceability. During evidence retrieval, the system performs integrity verification by comparing the newly generated hash value with the stored hash. Controlled decryption is permitted only when the integrity of the data is successfully validated. This approach ensures that tampered or altered evidence is never restored, thereby preserving forensic authenticity and strengthening the chain of custody.

SYSTEM ARCHITECTURE

The system architecture is composed of multiple interconnected modules that work together to ensure secure evidence handling. The user authentication module verifies authorized access to the system, while the encryption and hashing module secures text evidence by applying cryptographic algorithms. Encrypted data and corresponding hash values are then stored securely through the storage module. During retrieval, the verification and decryption module validates data integrity before allowing controlled decryption. The overall data flow begins with user input, followed by encryption and hashing, secure database storage, integrity verification, and final restoration of original evidence. The architectural design ensures confidentiality, integrity, and forensic reliability throughout the evidence lifecycle, as illustrated in the system architecture diagram

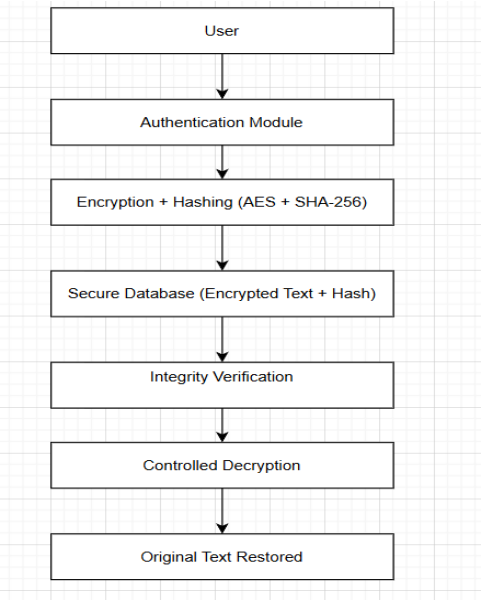

Fig 1: System Architecture

METHODOLOGY DESCRIPTION

Client Side: The client interface allows users to securely submit, retrieve, and verify text evidence through authentication-based access.

API Request / API Response: The system uses RESTful APIs for secure communication, employing HTTP methods and JSON-based data exchange.

Server Side: Backend logic handles encryption, hashing, verification, and access control using secure cryptographic libraries.

Store / Retrieve: Encrypted data and hash values are stored and retrieved securely using record identifiers.

Database: The database stores encrypted text, hash values, and metadata, ensuring confidentiality and integrity.

RESULTS AND DISCUSSION

The system was tested with multiple text inputs to evaluate integrity verification and restoration accuracy.

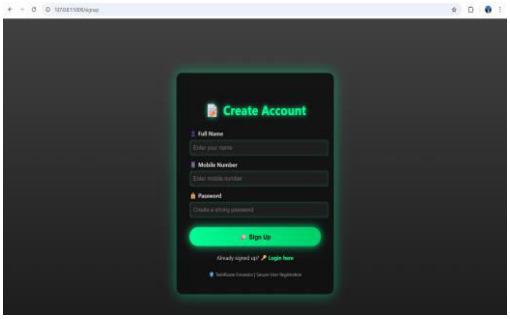

Fig 2: Signup page

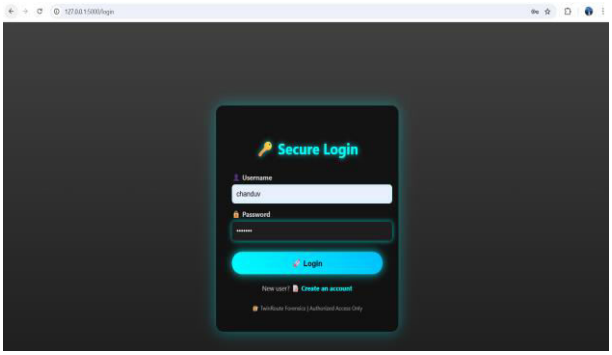

Fig 3: Login page

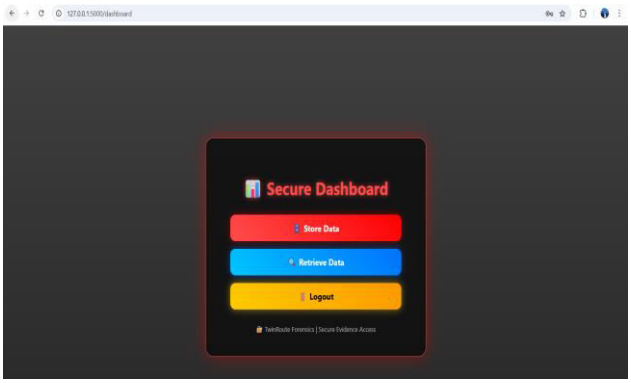

Fig 4: Dashboard

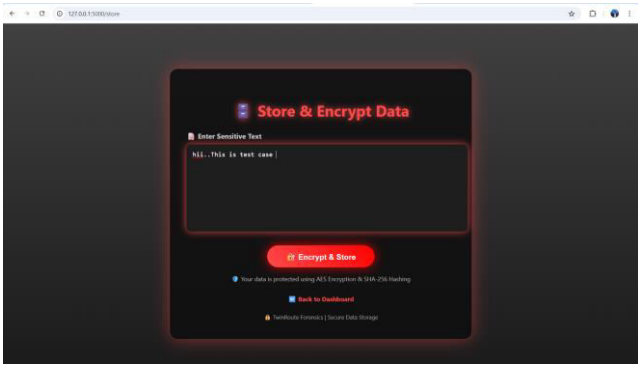

Fig 5: Encrypt data

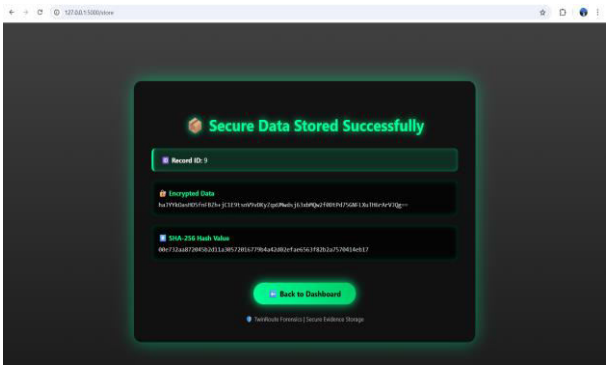

Fig 6:Stored data

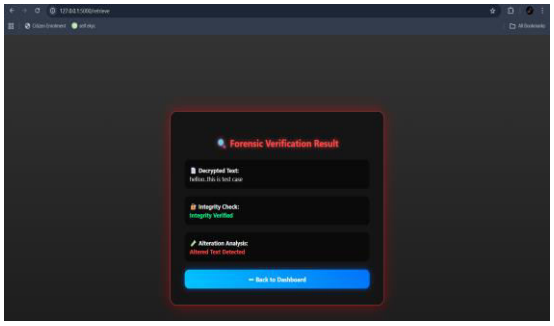

Fig7: Fetch Encrypted

The results confirm that tampered data is detected and blocked, while authentic data is successfully restored. Performance analysis shows efficient encryption and verification with minimal overhead.

CONCLUSION

This paper presented TwinRoute Forensics, a secure investigative framework for restoring altered text in digital forensics. By integrating AES encryption, SHA-256 integrity verification, and controlled decryption, the system ensures confidentiality, authenticity, and tamper resistance. The proposed approach significantly enhances forensic reliability and strengthens digital evidence trustworthiness.

FUTURE SCOPE

The proposed TwinRoute Forensics framework can be further enhanced by integrating advanced technologies to improve scalability, security, and forensic intelligence. One potential extension is the incorporation of blockchain-based audit trails to maintain an immutable and transparent record of evidence storage, access, and verification activities, chain-of-custody compliance. Artificial intelligence and machine learning techniques can also be employed to automatically detect anomalies or suspicious modifications in encrypted text evidence, enabling proactive tamper detection. Additionally, deploying the system in a secure cloud environment would allow scalable storage, remote investigator access, and collaborative forensic analysis across multiple jurisdictions. Future improvements may also include support for multi-format digital evidence, advanced access control policies, and automated forensic reporting, making the framework more robust and adaptable to real-world cybercrime investigation scenarios.

REFERENCES

[1 Kesavulu, O. S. C., & Harini, P. (2013). Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium. *Int. J. Latest Trends Eng. Technol*, *2*(4), 469-478.

[2] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. New York, NY, USA: Wiley, 2019.

[3] A. Kahate, *Cryptography and Network Security*, 3rd ed. New Delhi, India: McGraw-Hill, 2018.

[4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the*

Internet, 3rd ed. London, U.K.: Academic Press, 2019.

[5] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2022.

[6] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHA-256)," FIPS PUB 180-4, 2021.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2018.

[8] M. Kahn, J. Smith, and R. Brown, "Integrity verification techniques in digital forensics," *IEEE Access*, vol. 8, pp. 145672–145681, 2020.

[9] D. Quick and K. R. Choo, "Forensic analysis of encrypted data: Challenges and solutions," *Digital Investigation*, vol. 22, pp. 45–56, 2019.

[10] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*, 4th ed. Boston, MA, USA: Addison-Wesley, 2018.

[11] I. Sommerville, *Software Engineering*, 10th ed. Boston, MA, USA: Pearson, 2020.

[12] R. S. Pressman and B. R. Maxim, *Software Engineering: A Practitioner's Approach*, 9th ed. New York, NY, USA: McGraw-Hill, 2019.

[13] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication 800-86, 2021.

[14] M. Rogers and S. Seigfried-Spellar, "Digital forensic evidence reliability and integrity," *Journal of Digital Forensics, Security and Law*, vol. 14, no. 2, pp. 1–12, 2019.

[15] H. Kaur and R. Singh, "Secure text data storage using cryptographic techniques," *International Journal of Computer Applications*, vol. 176, no. 9, pp. 18–24, 2018.

[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2020.

[17] S. Behl and R. Behl, *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford, U.K.: Oxford Univ. Press, 2017.

[18] A. Patel and D. Shah, "Secure authentication and integrity verification in web-based systems," *International Journal of Information Security*, vol. 19, no. 3, pp. 325–334, 2020.

[19] OWASP Foundation, "OWASP Top 10 – Web Application Security Risks," 2022. [Online]. Available: https://owasp.org

[20] IEEE Computer Society, "Digital forensics and evidence integrity standards," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 72–79, 2020.