Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

A Secure Digital Forensic Framework for Text Evidence Authentication and Integrity Validation

[1]M Vardhan, [2]B Kartheek, [3]B Jaya Prakash

[1,2,3]Department of Computer Science Engineering (Cyber Security), GATES Institute of Technology, Gooty, Andhra Pradesh, India

Abstract: Digital forensics has become a fundamental component of cybercrime investigations, where digital text evidence, including emails, chat records, documents, and system logs, plays a crucial role in identifying and prosecuting malicious activities. Preserving the authenticity and integrity of such evidence is essential, as even slight modifications can compromise forensic analysis and affect legal admissibility. Although conventional security mechanisms primarily emphasize data encryption to maintain confidentiality, they often lack robust methods for verifying data integrity before the decryption process. The growing incidence of cyber-attacks, digital tampering, and online fraud has created a demand for forensic frameworks capable of both protecting and authenticating digital evidence. In the absence of effective integrity verification, encrypted data may still be altered, resulting in unreliable forensic outcomes and reduced evidential value. To overcome these limitations, the proposed Twin Route Forensics framework integrates user authentication, secure encryption, and hash-based integrity verification into a unified system. The framework ensures that digital text evidence is decrypted and restored only after successful validation of its authenticity, thereby preventing unauthorized modifications and preserving data reliability. By combining confidentiality with pre-decryption integrity checking, the proposed approach enhances the security, trustworthiness, and evidential value of digital text data. The system provides a robust solution for modern digital forensic investigations and contributes to the development of more secure and dependable cybercrime investigation processes.

Keywords: Digital Forensics, Digital Evidence, Text Evidence Authentication, Data Integrity Verification, Cryptography, Hash Functions, Cybercrime Investigation, Data Encryption, Digital Evidence Preservation, Information Security.

I. 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.

Furthermore, the framework enhances the security of digital evidence by implementing a dual verification process that detects unauthorized modifications before evidence reconstruction. This approach strengthens forensic reliability by ensuring that only verified and untampered data is pro-cessed during investigation.

Growth of Cybercrime and Digital Evidence

The rapid expansion of digital communication and cloud-based services has significantly increased the volume of electronic data generated every day. As a result, cybercriminals exploit these technologies to conduct activities such as identity theft, financial fraud, data breaches, and unauthorized system access. In many of these cases, digital text records serve as crucial evidence for identifying suspects and reconstructing events. Therefore, maintaining the security and reliability of

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

digital evidence has become a fundamental requirement in modern forensic investigations.

Authentication in Digital Forensic Systems

Authentication is an essential component of digital forensic frameworks because it ensures that only authorized individuals can access sensitive evidence. Strong authentication mechanisms protect confidential information from unauthorized viewing or modification and help maintain the chain of custody during investigations. By restricting access to verified users, forensic systems can reduce the risk of evidence tampering and enhance the overall security of the investigation process.

Importance of Data Integrity

Data integrity is one of the core principles of digital forensics, as the accuracy and originality of evidence directly affect investigative outcomes. Any unauthorized alteration, whether intentional or accidental, can reduce the credibility of digital evidence and lead to incorrect conclusions. Implementing effective integrity verification methods allows investigators to confirm that evidence remains unchanged from the time it is collected until it is presented for analysis or legal review.

Secure Storage and Transmission of Evidence

Digital evidence is often transferred between investigators, forensic laboratories, and legal authorities during an investigation. This process creates opportunities for unauthorized access or data manipulation if appropriate security measures are not implemented. Secure storage and encrypted transmission mechanisms help protect evidence from external threats while preserving its confidentiality and authenticity throughout the investigation lifecycle.

Advantages of Hash-Based Verification

Hash-based verification techniques provide an efficient and reliable method for detecting modifications in digital files. A unique hash value is generated for each evidence file, and this value acts as a digital fingerprint. If the content of the file changes, even by a single character, the generated hash value will differ from the original. This capability enables forensic investigators to quickly identify tampered evidence and maintain the integrity of digital investigations.

Applications of Secure Digital Forensic Frameworks

Secure digital forensic frameworks can be applied across various sectors, including law enforcement, banking, healthcare, corporate organizations, and government institutions. These systems assist investigators in protecting confidential records and verifying the authenticity of electronic evidence. The adoption of advanced forensic security mechanisms contributes to more transparent investigations and strengthens public trust in digital justice systems.

Reliability of the Proposed Twin Route Forensics Framework

The proposed Twin Route Forensics framework combines authentication, encryption, and integrity verification to provide a comprehensive solution for protecting digital text evidence. By validating data integrity before the decryption process, the framework minimizes the possibility of processing altered or maliciously modified files. This approach enhances the reliability of forensic analysis and supports the development of secure and trustworthy cybercrime investigation systems.

Future developments of the proposed framework may include the integration of artificial intelligence for automated evidence classification, blockchain technology for decentralized evidence storage, and cloud-based forensic services for remote accessibility. These enhancements can further improve the efficiency, scalability, and security of digital forensic systems, enabling them to address the evolving challenges of cybercrime investigations.

II. RELATED WORK

Previous research in digital security has primarily focused on encryption algorithms, authentication mechanisms, and secure database systems to protect sensitive information. Most existing systems rely on symmetric encryption techniques and access control policies to ensure confidentiality and restrict unauthorized access. However, these approaches often decrypt the stored data directly without first verifying whether the data has been modified or tampered with.

Recent studies in digital forensics emphasize the importance of data integrity and authenticity when handling digital evidence in cybercrime investigations. Cryptographic hash functions such as SHA-256 are widely used to detect

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

unauthorized changes in stored data and maintain the integrity of digital records.

The proposed TwinRoute Forensics Framework adopts a forensic-driven development approach that integrates cryptographic algorithms into a web-based system. The framework incorporates secure user authentication, encrypted data storage, integrity verification using SHA-256 hashing, and controlled decryption. By verifying data integrity before decryption, the system enhances forensic reliability and ensures the trustworthiness of digital text evidence in investigative environments.

Recent advancements in cybersecurity research highlight the importance of combining encryption, hashing, and authentication mechanisms within a unified framework to strengthen data protection and forensic reliability. Despite these developments, many existing systems still lack a pre-decrintegrity verification process, which may lead to the processing of compromised or tampered data. The TwinRoute Forensics Framework addresses this limitation by introducing a dual-route security pro-cess that verifies the integrity of digital text evidence before allowing decryption and access, thereby improving trust in forensic analysis.

III. 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 never restored, thereby preserving forensic authenticity and strengthening the chain of custody.

IV. SYSTEM ARCHITECTURE

The system architecture is composed of multiple inter-connected 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.

Importance of Digital Forensics

With the rapid growth of information technology and internet-based communication, digital devices have become a primary source of evidence in cybercrime investigations. Emails, instant messages, digital documents, and system logs often contain critical information that can assist forensic experts in identifying malicious activities and reconstructing criminal events. As cyber threats continue to evolve, digital forensics plays an increasingly important role in ensuring that electronic evidence is collected, preserved, and analyzed according to legal and technical standards.

Challenges in Digital Evidence Protection

One of the major challenges in digital forensic investigations is maintaining the authenticity and integrity of digital evidence throughout its lifecycle. Electronic data can be easily modified, copied, or deleted without leaving visible traces, making it vulnerable to tampering and unauthorized access. Even a minor alteration in a digital file may compromise its evidential value and affect the outcome of legal proceedings. Therefore, reliable mechanisms for protecting and validating digital evidence are essential for establishing trust in forensic investigations.

Role of Cryptography in Digital Forensics

Cryptographic techniques have become fundamental tools for securing digital evidence against unauthorized disclosure and manipulation. Encryption algorithms ensure the confidentiality of sensitive information by preventing unauthorized users from

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

accessing protected data. However, encryption alone cannot guarantee that the stored evidence has remained unchanged. For this reason, modern forensic systems increasingly combine cryptographic methods with integrity verification techniques to provide comprehensive protection for digital evidence.

Hash-Based Integrity Verification

Hash functions are widely used in digital forensics to verify the originality of electronic data. A cryptographic hash generates a unique digital fingerprint for a file, and any modification to the content results in a completely different hash value. By comparing the original and current hash values, investigators can quickly determine whether evidence has been altered. This approach strengthens the reliability of forensic analysis and supports the admissibility of digital evidence in judicial processes.

Need for Integrated Security Frameworks

Modern cybercrime investigations require forensic frameworks that combine authentication, encryption, and integrity verification into a unified security model. Integrating these mechanisms helps prevent unauthorized access while ensuring that evidence remains unchanged during storage and transmission. Such frameworks not only improve the reliability of forensic outcomes but also reduce the possibility of human error and strengthen confidence in digital investigations.

Future Scope of Digital Forensic Systems

Advancements in cybersecurity and digital communication technologies continue to create new challenges for forensic investigators. Future digital forensic systems are expected to incorporate artificial intelligence, blockchain technology, and advanced cryptographic techniques to enhance evidence management and verification. These innovations can improve automation, reduce investigation time, and provide more secure methods for preserving digital evidence, ultimately supporting more effective cybercrime detection and prosecution.

The architectural design ensures confidentiality, integrity, and forensic reliability throughout the evidence lifecycle, as illustrated in the system architecture diagram.

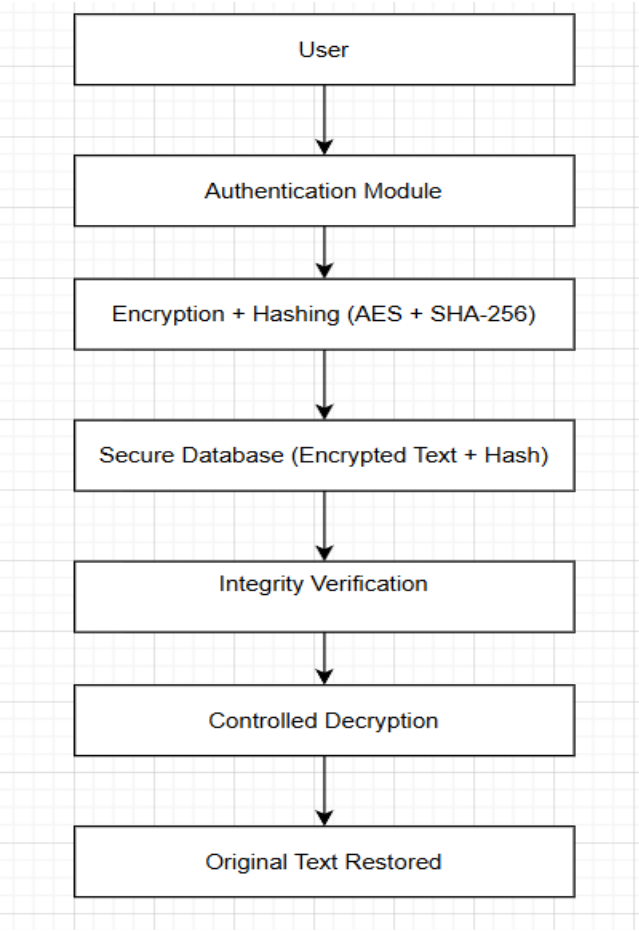


Figure 1: System Architecture

V. 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 REST-ful 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

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

metadata, ensuring confidentiality and integrity.

VI. IMPLEMENTATION

Cryptograpic Mechanisms Used

1. AES-256 Encryption

The proposed CryptoTrace framework utilizes the Advanced Encryption Standard (AES-256) algorithm to en-sure secure storage of digital text evidence. AES-256 is a symmetric key encryption algorithm that uses a 256-bit key to encrypt plaintext data into ciphertext. In the pro-posed system, when a user uploads text evidence, the data is encrypted using AES-256 before being stored in the database. This ensures confidentiality and prevents unauthorized access to sensitive forensic data.

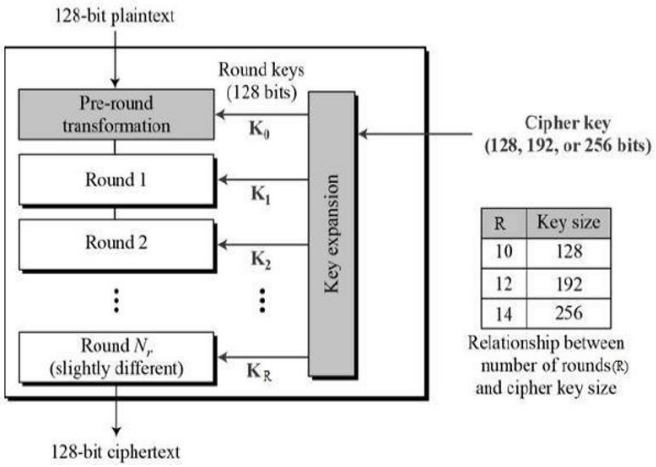


Figure 2: AES in Cryptography

- AES uses Substitution-Permutation Network
- Data is processed in 128-bit blocks
- AES-256 performs 14 encryption rounds

2. SHA-256 Hashing for Integrity Verification

To ensure data integrity, the system employs the SHA-256 hashing algorithm. SHA-256 generates a unique 256-bit hash value for each piece of digital text evidence.

This hash value acts as a digital fingerprint of the original data. During the verification stage, the system recomputes the hash of the stored text and compares it with the original hash value. Any mismatch indicates that the data has been modified or tampered with.

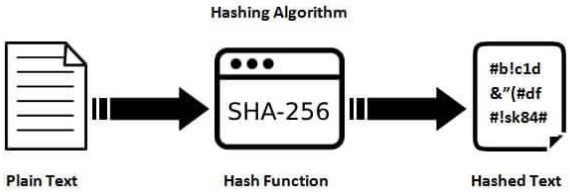


Figure 3: SHA-256 Algorithm

VII. RESULTS

This project is designed to protect and verify the integrity of textual evidence using cryptographic techniques. The system integrates encryption algorithms such as AES for secure data storage and SHA-256 hashing for integrity verification. By combining cryptography with forensic analysis , CryptoTrace enables investigators to Detect and recover manipulated text while maintaining the authenticity of digital evidence.

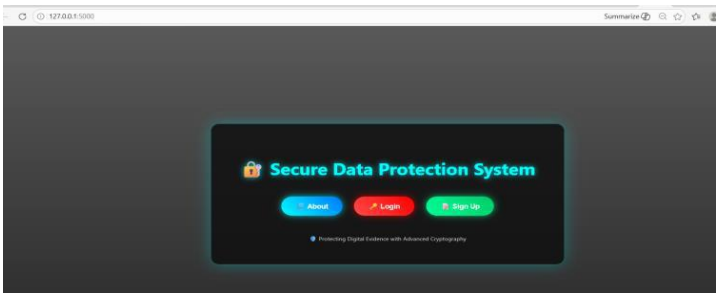


Figure 4: The landing page of cryptotrace

The landing page serves as the entry interface for the CryptoTrace system, providing options such as About, Login, and Sign Up. It acts as the initial access point for forensic analysts to enter the secure platform. The inter-face highlights the system's objective of protecting digital evidence using cryptographic techniques.

Secure Login (role-based access control): The login interface authenticates authorized users before allowing access to forensic operations. Analysts provide credentials that are validated by the system to prevent unauthorized access. This mechanism ensures that only verified investigators can handle sensitive digital evidence.

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

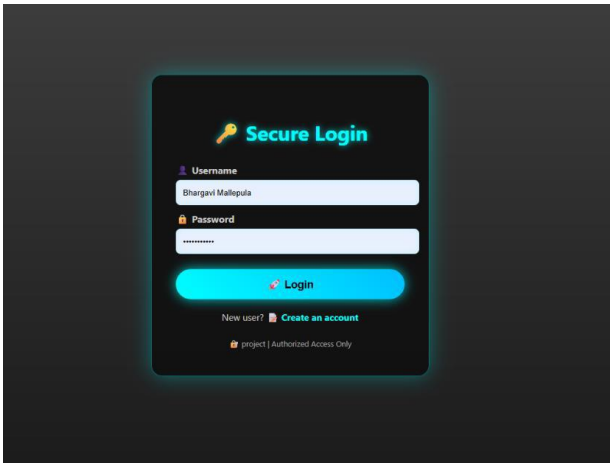
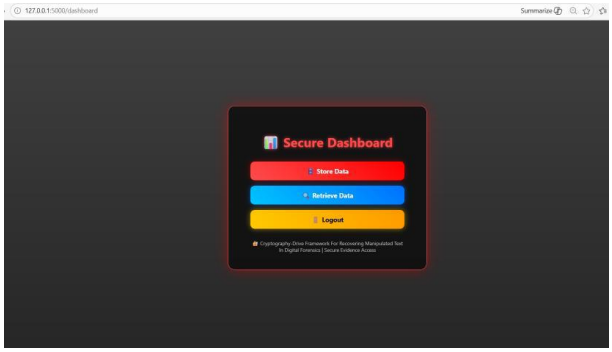


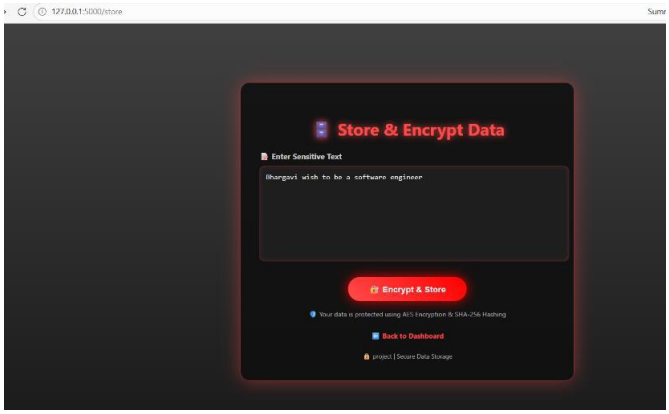
Figure 5: Represents Secure Landing Page

Analyst Dashboard (case operations hub): After authentication, the analyst dashboard provides options such as Store Data and Retrieve Data. These operations correspond to evidence submission and verification processes. The dashboard acts as the central inter-face for managing digital forensic evidence.



The above figure depicts the secure dashboard of our project.

Store and Encrypt Data (evidence ingestion). In this step, the investigator enters the suspected text evidence into the system. The data is encrypted using AES to ensure confidentiality and a SHA-256 hash is generated for integrity verification. The encrypted data and hash value are securely stored in the database. Advancements in cybersecurity and digital communication technologies continue to create new challenges for forensic investigators. Future digital forensic systems are expected to incorporate artificial intelligence, blockchain technology, and advanced cryptographic techniques to enhance evidence management and verification. These innovations can improve automation, reduce investigation time, and provide more secure methods for preserving digital evidence, ultimately supporting more effective cybercrime detection and prosecution.



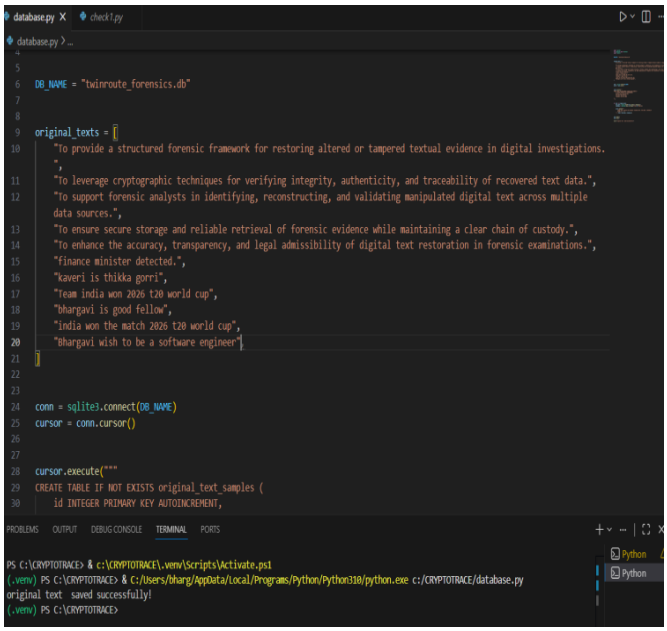


Figure : Represents the original text stores successfully

Storage Confirmation (evidence record created). After encryption, the system generates a unique Record ID along with the ciphertext and SHA-256 hash value. This record acts as a reference for retrieving the stored evidence. The stored hash serves as the integrity finger-print of the original data.

Advancements in cybersecurity and digital communication technologies continue to create new challenges for forensic investigators. Future digital forensic systems are expected to

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

incorporate artificial intelligence, blockchain technology, and advanced cryptographic techniques to enhance evidence management and verification. These innovations can improve automation, reduce investigation time, and provide more secure methods for preserving digital evidence, ultimately supporting more effective cybercrime detection and prosecution.

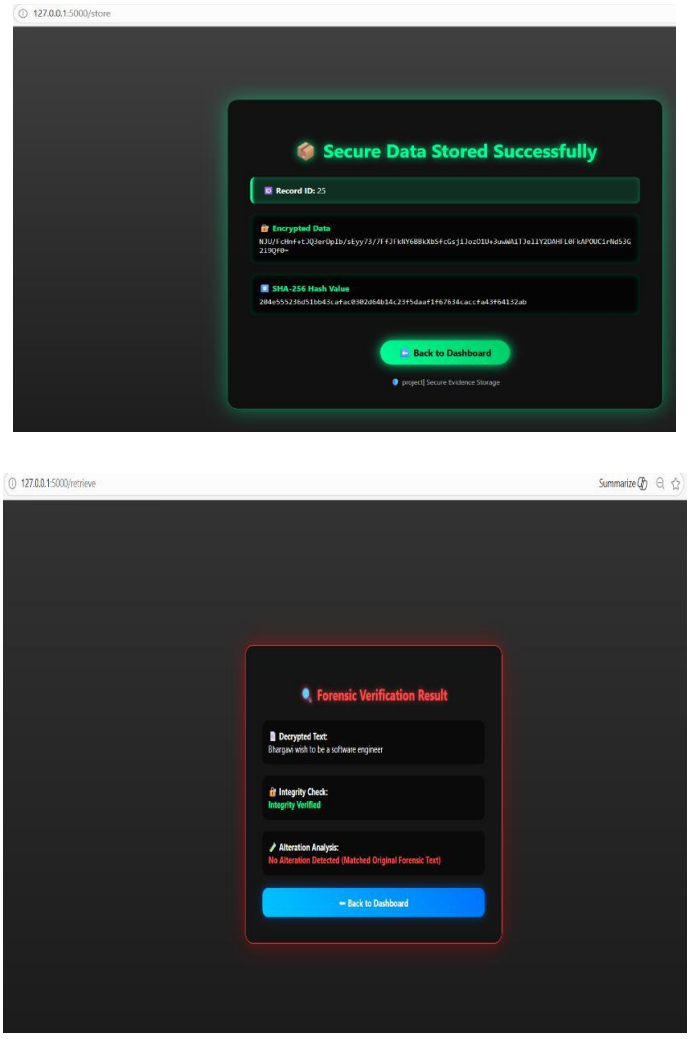


Figure : Represents which stores ID for retrieving the data

Forensic Verification Result (tamper detection). During retrieval, the system decrypts the stored cipher-text and recomputes the SHA-256 hash. The newly generated hash is compared with the stored value to verify data integrity. If both values match, the system confirms that the evidence has not been altered.

Backend Initialization (database setup). The backend initialization process sets up the SQLite database and inserts original text samples used for comparison. A Python script creates the required tables and stores reference texts. This setup supports alteration detection and forensic verification during evidence analysis.

VIII. 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 trust-worthiness.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pear-son, 2020.
[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. Lon-don, 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.

Current Journal of Engineering and Science Research
Volume 3, Issue 5, pp 32-39, May 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.305005
Available Online at https://www.cjesr.com

[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] 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.
[17] OWASP Foundation, "OWASP Top 10 – Web Application Security Risks," 2022. [Online]. Available: https://owasp.org.
[18] IEEE Computer Society, "Digital forensics and evidence integrity standards," IEEE Security & Privacy, vol. 18, no. 4, pp. 72–79, 2020.

Citation of this Article:

M Vardhan, B Kartheek, & B Jaya Prakash. (2026). A Secure Digital Forensic Framework for Text Evidence Authentication and Integrity Validation. *Current Journal of Engineering and Science Research.* 3(5), 32-39. Article DOI: https://doi.org/10.47001/CJESR/2026.305005

***** End of the Article *****