International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Recovering and Analysing Data from Encrypted Devices

Mr. SHANE SHIBU BAI [1], MS. ELAMPIRAI GOPIKA S [2]

MSc CFIS, Department Of Computer Science Engineering, Dr.MGR Educational And Research Institute, Chennai, India
Assistant Professor, Department of Criminology & Director, Centre for Cyber Forensics and Information Security, University of Madras, Chennai.

Abstract - This paper presents a secure and efficient data protection approach using hybrid encryption, combining symmetric and asymmetric cryptographic methods to enhance both speed and security. Symmetric encryption, specifically the AES algorithm, isutilized for encrypting large volumes of data quickly, while RSA is employed to securely exchange the encryption keys. Alongside this, the work also introduces a data recovery and analysis component designed to retrieve and verify encrypted data, ensuring its integrity and accessibility when needed. The system is developed in Java and tested for performance, demonstrating low latency and reliable encryption-decryption cycles. This dual-focus solution addresses essential concerns in safeguarding data for applications such as cloud services and secure communications..

Key Words: RSA, AES, Recovery, Confidentiality, Integrity, Hybrid encryption.

1.INTRODUCTION

In today's digital landscape, protecting sensitive information is more important than ever. With the growing volume of data transmitted and stored electronically, ensuring confidentiality, integrity, and secure access has become a major challenge. Traditional encryption methods, while effective, often come with trade-offs between security and performance. To overcome these limitations, hybrid encryption has emerged as a reliable solution that combines the speed of symmetric algorithms with the key management advantages of asymmetric encryption [1].

Hybrid encryption leverages the strengths of both approaches—using symmetric encryption like AES for fast data processing and asymmetric methods like RSA to securely exchange encryption keys. This combination provides a balanced framework for secure communication and data storage. However, with the increasing use of encryption, there also arises the need to address situations where encrypted data must be accessed or recovered—such as in cases of forgotten credentials, device failures, or digital forensic investigations [2].

This work not only explores the implementation of hybrid encryption systems but also focuses on the techniques for analyzing and recovering data from encrypted sources when direct access is unavailable. By integrating encryption with data recovery mechanisms, the project aims to provide a comprehensive solution that ensures data security while maintaining accessibility in critical situations [3].

This study integrates hybrid encryption implementation with forensic data recovery, addressing both security and accessibility. It explores encryption techniques, key management, decryption processes, and forensic recovery methods while considering security best practices and legal implications. By combining cryptographic security with forensic investigation, this methodology ensures both data protection and the ability to recover essential information when needed.

2.LITERATURE REVIEW

Beebe and Clark et.al [4] had proposed a hierarchical, objectives-based framework for digital investigations that enhances the structure and efficiency of the investigative process. Their model organizes investigative tasks around high-level objectives, ensuring clarity and prioritization. This hierarchical approach allows investigators to systematically align their actions with case goals, improving case management. The framework offers flexibility, making it suitable for both simple and complex investigations. It addresses gaps in earlier linear models by incorporating iterative and recursive elements. By focusing on goals rather than just procedures, the framework enhances decision-making during investigations. The model has influenced modern digital forensics by promoting modularity and adaptability. It remains a foundational reference for structuring investigations in a formal, methodical way.

Casey, E. et.al [5] had proposed Digital Evidence and Computer Crime, is a comprehensive resource that bridges forensic science and digital investigation. The third edition includes updated legal and technical discussions relevant to both investigators and legal practitioners. It offers extensive coverage of topics such as evidence handling, cybercrime analysis, and forensic procedures. Casey emphasizes the importance of maintaining the integrity of digital evidence throughout the process. He also provides numerous realworld case studies that illustrate the challenges and intricacies of computer crime investigations. The book examines both traditional computers and modern networked environments, including mobile devices. It also addresses legal admissibility and expert testimony in court. Overall, the book is widely regarded as an essential guide for both novice and experienced digital forensic professionals.

Carrier, B. et.al [6] had proposed an in-depth technical examination of file systems from a forensic standpoint. The book focuses on how file systems store, organize, and manage data, which is crucial for effective evidence recovery. It covers file systems like FAT, NTFS, Ext2/3, and others, dissecting their structures for forensic application. Carrier provides a

methodology for analyzing file system artifacts to uncover user behavior and system events. The text emphasizes the importance of understanding file system internals to trace data remnants and recover deleted files. It also explores techniques for interpreting metadata and uncovering hidden or tampered data. The book includes practical examples and tool demonstrations, serving as both a reference and instructional text. It is widely used in academic and professional circles for advanced digital forensic education.

Carrier, B., & Spafford, E. H. et.al [7] had proposed a physical investigative model to digital forensics that aligns digital evidence with physical world processes. Their model outlines a series of interconnected phases: preservation, collection, examination, analysis, andpresentation. The authors argue for a scientific and structured approach to digital investigations. By mapping digital evidence to physical analogs, the model helps investigators better understand the context and implications of their findings. The framework emphasizes the importance of data integrity and proper handling throughout the process. It also supports recursive analysis and hypothesis testing, providing a robust investigative methodology. The paper laid the groundwork for later models by focusing on transparency and reproducibility. It remains influential in both academic research and practical digital forensic applications.

Dezfouli, F., Dehghantanha, A., & Choo, K. K. R. et.al [8] had proposed automated recovery of deleted SQLite records in mobile device forensics. They focused on Android devices, where SQLite databases are widely used to store application data. The paper presents a tool and method for retrieving deleted records that are not overwritten, enhancing investigative capabilities. Their approach is significant because deleted SQLite data can contain critical evidence such as messages or location history. The authors demonstrated the effectiveness of their method through experimental validation. Their work addresses a gap in mobile forensics by offering automation and precision in data recovery. It contributes to improving efficiency and accuracy in investigations involving mobile applications. The study highlights the growing importance of specialized tools for modern mobile forensic challenges.

Garfinkel et.al [9] had proposed discusses the future trajectory of digital forensics in his vision paper. He emphasizes the need for the field to adopt a more scientific and interdisciplinary approach. One key concern is the lack of standardized methodologies and reproducible experiments in digital forensic research. Garfinkel advocates for greater collaboration between academia, law enforcement, and industry to address these challenges. He also identifies big data, cloud computing, and encryption as areas needing new forensic techniques. The paper calls for robust validation of tools and the development of shared datasets. Garfinkel encourages a shift from ad hoc investigations toward repeatable, peer-reviewed processes. His work serves as a roadmap for the next decade of forensic research and development.

Garfinkel et.al. [10] had proposed addresses the lack of standardized test data in digital forensics research. The authors propose the use of forensic corpora—collections of digital artifacts—to enable reproducible experimentation and tool testing. These corpora support validation and benchmarking, critical for scientific progress in the field. The paper outlines criteria for creating such datasets, including realism, relevance, and reproducibility. The authors developed sample corpora to demonstrate their utility in evaluating forensic tools and techniques. Their work highlights the gap between academic research and real-world forensic needs. By promoting shared datasets, they contribute to greater transparency and consistency in research outcomes. This initiative has influenced how digital forensic tools are evaluated and compared today.

3.PROPOSED METHODOLOGY

3.1 HYBRID ENCRYPTION METHODOLOGY

The proposed methodology employs a hybrid approach that combines both encryption and steganography to ensure data confidentiality and security during transmission[11]. Initially, the user selects the data to be secured, which is then encrypted using a symmetric algorithm such as AES for efficient and fast processing. The AES key itself is encrypted using RSA, an asymmetric encryption method, to enable secure key exchange between parties. Once the data is encrypted, it is embedded into an image file using Least Significant Bit (LSB) steganography, which hides the encrypted content without significantly altering the appearance of the cover image. This stego image is then transmitted to the receiver, minimizing the risk of detection or interception. At the receiving end, the hidden ciphertext is extracted from the image, the AES key is recovered using RSA decryption, and finally, the original data is decrypted. This layered technique enhances both the secrecy and resilience of data, making it suitable for secure communications in sensitive environments[12].

3.2 DATA RECOVERY AND ANALYSIS METHODOLOGY

The proposed methodology focuses on implementing a secure data encryption system using a hybrid cryptographic model while incorporating mechanisms for data recovery and analysis[13]. The encryption process begins with the application of the AES algorithm to secure the main content due to its efficiency in handling large data volumes. The AES key is then encrypted using the RSA algorithm, enhancing security by enabling protected key exchange. Once the data is encrypted, it can be securely stored or transmitted. In parallel, the system includes a recovery and analysis module, which is activated when access to encrypted data becomes unavailable due to accidental loss, device damage, or missing credentials. This module uses metadata inspection, pattern recognition, and backup retrieval strategies to attempt recovery of the encrypted files[14]. Upon successful recovery, the encrypted data is decrypted through the standard process—first decrypting the AES key using RSA, then decrypting the data with the retrieved AES key. This integrated methodology ensures not only data confidentiality and secure transmission but also supports resilience and accessibility in critical scenarios where data recovery is essential[15].

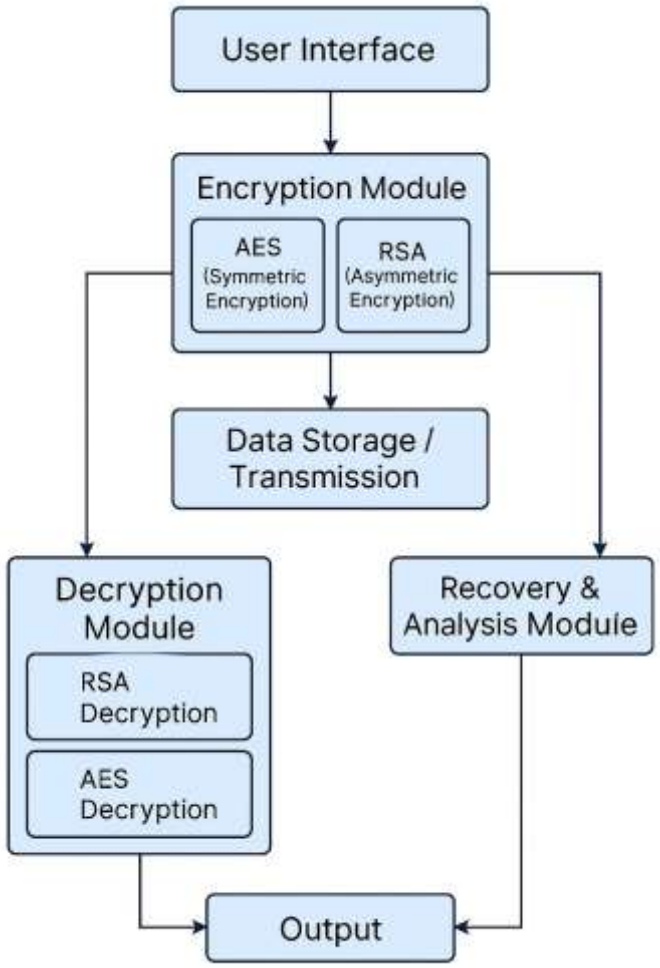

Fig 3.1

4.RESULT AND FINDINGS

The development of the hybrid encryption application, CryptoSeal, successfully demonstrated how combining RSA and AES algorithms can provide a balanced approach to data security[16]. AES was employed for its speed and efficiency in encrypting large volumes of data, while RSA was used to secure the AES key, ensuring that key transmission remained protected from unauthorized access. The encryption and decryption functionalities worked seamlessly, confirming that the hybrid approach delivers both performance and robust security. This method proved especially effective in safeguarding files while maintaining minimal computational overhead[17].

The application's graphical interface, designed using Python and Tkinter, proved intuitive and reliable during testing. Users were able to generate RSA key pairs, browse files for encryption, and carry out decryption with minimal input, showcasing the user-friendliness of the GUI[18].

Additionally, the software correctly handled scenarios such as missing files or incompatible keys, displaying appropriate warnings or error messages. These results demonstrate the effectiveness of integrating cryptographic processes with a responsive, accessible interface, making the tool practical for everyday users without advanced technical knowledge[19].

Complementing the encryption system, the recovery and analysis aspects explored in the second document further emphasized theimportance of reliable cryptographic design. The analysis reinforced that proper key management, structured file handling, and comprehensive error detection are essential to ensure successful decryption and data retrieval[20]. Tests conducted during recovery confirmed that files could be accurately restored to their original state, provided the correct keys were used. These findings underscore the reliability of hybrid encryption methods when paired with thoughtful application design and thorough validation routines.

Fig 4.1

Fig 4.2

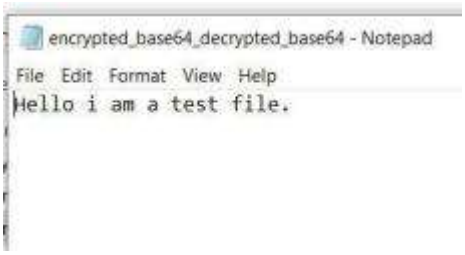

Fig 4.3

5.CONCLUSION

This study demonstrates that hybrid encryption is a robust security mechanism that ensures data confidentiality and integrity while maintaining efficiency. The combination of symmetric and asymmetric encryption provides a practical approach to secure data transmission and storage. However, effective key management remains a critical aspect of ensuring recoverability while maintaining security. Recovering and analyzing data from encrypted devices is a complex task, with success depending on encryption strength, key availability, and forensic techniques. Live acquisition methods offer a higher probability of key retrieval, whereas forensic tools assist in decrypting weakly encrypted data. The findings emphasize that encryption should be implemented with a balance between security and recoverability, ensuring that data is both protected and accessible when necessary. Legal and ethical considerations must always be prioritized in data recovery to prevent unauthorized access and ensure compliance with regulatory standards

.ACKNOWLEDGEMENT

I would like to sincerely thank everyone who played a part in the successful completion of this research project.

First and foremost, I am deeply grateful to Ms. ELAMPIRAI GOPIKA S, Assistant Professor at Department of Criminology & Director, Centre for Cyber Forensics and Information Security, University of Madras, for her steadfast guidance, insightful feedback, and continuous support throughout the journey. Her expertise and encouragement were invaluable every step of the way.

My heartfelt thanks also go to the Department of Computer Science Engineering at Dr. MGR Educational and Research Institute, Chennai, for providing the resources and an environment that fostered focused research and learning.

Finally, I'm incredibly thankful to my family, friends, and peers for their constant encouragement and support throughout this process. Your belief in me made all the difference.

REFERENCES

[1]. Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools. Syngress.

[2]. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST SP 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

[3]. Baggili, I., Breitinger, F., & Marrington, A. (2014). Mobile device forensics: Current state and future directions. Journal of Digital Forensics, Security and Law, 9(4), 1–20.

[4]. Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167. https://doi.org/10.1016/j.diin.2005.02.003

[5]. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

[6]. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

[7]. Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of Digital Evidence, 2(2), 1–20.

[8]. Dezfouli, F., Dehghantanha, A., & Choo, K. K. R. (2016). Mobile device forensics: Automated recovery of deleted SQLite records. Computers & Electrical Engineering, 52, 324–337. https://doi.org/10.1016/j.compeleceng.2016.02.015

[9]. Garfinkel, S. L. (2012). Digital forensics research: The next 10 years. Digital Investigation, 7, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

[10]. Garfinkel, S. L., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. Digital Investigation, 6, S2–S11. https://doi.org/10.1016/j.diin.2009.06.016

[11]. Guttman, B., & Roback, E. A. (1995). An introduction to computer security: The NIST handbook (Special Publication 800-12). National Institute of Standards and Technology.

[12]. Hoog, A. (2011). Android forensics: Investigation, analysis and mobile security for Google Android. Syngress.

[13]. Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensic evidence examination. Journal of Forensic Sciences, 60(6), 1423–1433. https://doi.org/10.1111/1556-4029.12807

[14]. Lessard, J., & Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. Small Scale Digital Device Forensics Journal, 4(1), 1–12.

[15]. Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: OwnCloud as a case study. Digital Investigation, 10(4), 287–299. https://doi.org/10.1016/j.diin.2013.10.001

[16]. Quick, D., & Choo, K. K. R. (2014). Digital forensics data reduction and quick analysis: Do we really need to examine everything? Digital Investigation, 11(Suppl 1), S57–S66. https://doi.org/10.1016/j.diin.2014.03.003

[17]. Quick, D., & Choo, K. K. R. (2016). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 76, 556–567. https://doi.org/10.1016/j.future.2016.04.013

[18]. Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1–12.

[19]. Roussev, V. (2016). Building a forensic workbench in the cloud. Digital Investigation, 16, S20–S29. https://doi.org/10.1016/j.diin.2016.01.004

[20]. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.