WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cryptography-Based Secure File Storage System Using AES

K.Nagaraj[1], Ms. S. Malini[2]

[1]Dept of Computer Applications

[2]Assistant Professor Dept of Computer Applications

[1, 2] Adhiyamaan College of Engineering (Autonomous), Hosur, Tamil Nadu, India

ABSTRACT

Using the Advanced Encryption Standard (AES) set of rules, this paper affords a strong cryptography-based totally steady document storage device meant to make sure data confidentiality and integrity. The system stresses presenting a secure repository for touchy data, such magazine entries, in which information manipulation and unlawful access are essential concerns. We each strongly encrypt and authenticate the stored information using AES in Galois/Counter Mode (GCM), consequently safeguarding it from diverse security concerns. The design emphasizes the need of safe key derivation the usage of features like PBKDF2 to decrease brute-pressure attacks and consists of a secure key control system, which is critical for safeguarding the encryption keys. This system gives an entire solution for people and corporations wishing to protect their valuable digital belongings by means of sturdy cryptographic strategies. The execution info consist of The implementation information—including encryption and decryption processes, key control regulations, and protection concerns—are investigated to illustrate the device's efficacy.

I. INTRODUCTION

Strong security regulations are required inside the virtual age to protect in opposition to facts breaches and illegal get admission to given the wealth of sensitive records. Confidential files, monetary facts, and private journals require secure garage choices making certain integrity and confidentiality. Much of virtual information security depends on cryptography; the Advanced Encryption Standard (AES) has grown to be a broadly used, very safe encryption method. This work seems at building a cryptography-based totally steady report garage device the usage of AES, so satisfying the urgent call for for safe facts repositories. The machine targets to be a trustworthy and regular answer for people and agencies wishing to shield their touchy information.

Stored records protection relies on the effective use of cryptographic techniques and safe key control regulations.
Strong safety functions and a proven track record assist to make AES the number one encryption technique. The system employs AES in Galois/Counter Mode (GCM) to offer both confidentiality and integrity, consequently making sure that encrypted statistics stays safe from unauthorised access and manipulation. Key control—consisting of safe key generation, garage, and derivation—determines the overall security of the device. Key derivation techniques like PBKDF2 assist to reinforce the system against brute-pressure attacks. The layout of the system guarantees an entire security system by thinking about numerous security factors inclusive of side-channel attacks and secure memory management.

II. RELATED WORK

Existing secure file storage solutions often employ AES encryption, but vary in key management and integrity mechanisms. Cloud-based systems like Google Drive and Dropbox offer encryption, but user control over keys is limited. Research explores homomorphic encryption for computations on encrypted data, though it's computationally intensive. Studies on client-side encryption highlight the importance of local key management, using hardware security modules (HSMs) or password-derived keys via PBKDF2. Implementations focusing on journal encryption often use AES-GCM for authenticated encryption. File system encryption tools like VeraCrypt and EncFS provide strong encryption, but may lack user-friendly interfaces. Secure note-taking apps like Standard Notes emphasize end-to-end encryption, but their open-source nature requires careful auditing. Research on secure key distribution and rotation protocols addresses the challenge of managing numerous keys. The use of Argon2 as a key derivation function is increasingly favored over PBKDF2 for its resistance to GPU-based attacks. Secure multiparty computation (SMPC) offers theoretical security for distributed data, but is complex to implement.

III METHODOLOGY

This system employs AES-256 in GCM mode for data encryption, ensuring both confidentiality and integrity. User-specific encryption keys are generated using a cryptographically secure random number generator (CSPRNG). Key derivation from user passwords utilizes PBKDF2 with a unique salt for each user, bolstering resistance to brute-force attacks. Encrypted data, including the IV, tag, and ciphertext, is stored in a secure storage module.

The system implements a modular design, separating encryption, key management, and storage functionalities. Thorough testing of encryption/decryption processes, key management, and error handling ensures system robustness. Security analysis and threat modeling are performed to identify and mitigate potential vulnerabilities.

IV DISCUSSION

The proposed system effectively demonstrates the feasibility of a secure, user-centric file storage solution leveraging AES-GCM. The integration of robust key derivation through PBKDF2 significantly enhances security against password-based attacks. The modular design facilitates future scalability and adaptability to different storage environments. Balancing security with usability remains a key consideration, requiring careful UI/UX design. The system's reliance on client-side encryption provides users with greater control over their data privacy. However, secure key management remains a critical challenge, demanding robust implementation and user education. Future work should explore integration with hardware security modules and advanced key distribution protocols. Thorough security audits and penetration testing are essential for validating the system's resilience against real-world threats.

V CONCLUSION AND FUTURE WORK

This paper presented a secure file storage system utilizing AES-GCM and robust key derivation, providing a strong foundation for data confidentiality and integrity. Future work will focus on integrating hardware security modules (HSMs) for enhanced key protection and exploring advanced key distribution protocols. Implementing secure multi-party computation (SMPC) for collaborative data access without revealing plaintext is another promising avenue. Research into post-quantum cryptographic algorithms is crucial for long-term security in the face of quantum computing advancements. Additionally, thorough security audits and penetration testing will be conducted to validate the system's resilience. User experience improvements, including more intuitive key management interfaces, will be prioritized.

REFERENCES

[1] **National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197, Advanced Encryption Standard (AES).** This standard defines the AES algorithm, which is the core encryption method used in the system.

[2] **National Institute of Standards and Technology (NIST). (2007). NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation:** Galois/Counter Mode (GCM) and GMAC**.**

[3] **National Institute of Standards and Technology (NIST). (2013). NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: General. (Revised).** This document provides guidelines for using PBKDF2, the key derivation function employed in the system.

[4] **Bernstein, D. J. (2015). Argon2: memory-hard functions for password hashing and other applications.** This paper details the Argon2 key derivation function, an alternative to PBKDF2 that offers improved security against certain attacks.

[5] **Ferguson, N., Schneier, B., &Kohno,T.(2010). Cryptography engineering: design principles and practical applications.** This book provides a comprehensive overview of cryptography engineering principles, including secure key management and implementation considerations.

[6] **Rivest, R. L. (1992). The MD5 message-digest algorithm.** Although MD5 is considered insecure for cryptographic hash functions, it helps to understand the historical context of cryptographic hashing, and why stronger algorithms like SHA-256 are needed.

[7] **Housley, R., Polk, W., Ford, W., & Solo, D. (2002). Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.** This reference provides insight into secure key and certificate management, which is important when considering larger scale implementations.