EasyChair Preprint

№ 15720

Securing the File Storage System with Standard Encryption: Secured and Encrypted File's Storage System

Santhosh Kumar Ramidi, Ashish Rathod, Sunkari Hari, Lakshy Patel and Hansa Vaghela

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

January 15, 2025

Securing The File Storage System with Standard Encryption: Secured and Encrypted File's Storage System

1st Ramidi Santhosh Kumar
Department of Computer Science and Engineering
Parul University
Vadodara, India
santhoosh619@gmail.com

2nd Rathod Ashish Kumar VijayKumar
Department of Computer Science and Engineering
Parul University
Vadodara, India
ash.rd2905@gmail.com

3rd Sunkari Hari
Department of Computer Science and Engineering
Parul University
Vadodara, India
sunkarihari7@gmail.com

4th Lakshy Jayeshkumar Patel
Department Of Computer Science And Engineering
Parul University
Vadodara, India
lakshypatel5895@gmail.com

5th Prof. Hansa Vaghela
Department Of Computer Science And Engineering
Parul University
Vadodara, India
vaghelahansa315@gmail.com

***Abstract*— Cloud computing has emerged as a fundamental technology for data storage and services across various sectors, offering scalable resources accessible on demand. Despite its benefits, security remains a critical concern in cloud environments. This paper presents a comprehensive file security model aimed at addressing this challenge. Our approach employs hybrid encryption, combining file splitting and RSA for secure communication between users and servers. Recognizing the limitations of individual cryptographic techniques, we integrate DES and AES algorithms with steganography to bolster data security. Through the use of multithreading, files are divided into three parts and encrypted simultaneously with different algorithms, enhancing efficiency and resilience. Key information, encompassing encryption specifics, is securely embedded into images using LSB steganography. By leveraging AES and DES algorithms, our methodology ensures robust data protection on a single cloud server, providing heightened security and peace of mind for users.**

Keywords—Data Storage, Cloud Computing, Cryptography, AES Algorithm, DES Algorithm

I. INTRODUCTION

In contemporary computing landscapes, where data storage and cloud computing play pivotal roles across various sectors including industries, military installations, and diverse software and hardware enterprises, the challenge of safeguarding sensitive information against cyber threats looms large. With the ever-evolving tactics of malicious actors, ensuring robust data security has become paramount.

Traditional approaches to data protection often prove insufficient against sophisticated cyberattacks. In response, cryptography emerges as a beacon of hope, offering advanced techniques to fortify data against unauthorized access and manipulation. However, relying solely on a single cryptographic algorithm for achieving high-level security in cloud computing environments may fall short of providing comprehensive protection.

To address this concern, we propose the integration of a novel security mechanism leveraging symmetric key cryptography algorithms. Recognizing that both user applications and program infrastructures often coexist within provider premises, we underscore the urgency for a robust file security model tailored to the specific challenges posed by local system environments.

Central to our approach is the adoption of hybrid encryption, wherein files undergo encryption using two distinct algorithms. Complemented by file splitting techniques, this strategy not only bolsters data confidentiality but also ensures secure communication channels between users and servers.

In this research paper, we embark on a comprehensive exploration of the efficacy of hybrid cryptography in enhancing data security within cloud computing paradigms. By elucidating the underlying principles, evaluating performance metrics, and assessing real-world applicability, we aim to offer valuable insights into fortifying data storage infrastructure against prevalent cyber threats. Through empirical validation and theoretical analysis, we seek to contribute to the ongoing discourse on cybersecurity, paving the way for resilient data protection frameworks in an increasingly interconnected digital ecosystem.

II. TERMINOLOGY

A. Encryption:

Cryptography serves as a cornerstone of modern data security, covering a variety of terms essential to understanding the mechanisms and applications. Basically, encryption involves using encryption algorithms to convert plaintext data into ciphertext, making it unreadable to unauthorized persons. Key cryptography concepts include One of the most important ideas in cryptography is the distinction between symmetric and asymmetric encryption. Effective communication between parties is made possible by symmetric encryption, which uses a single common key for both encryption and decryption. Asymmetric cryptography, on the other hand, can employ digital signatures and safe key exchange in addition to mathematically related key pairs—a public key for encryption and a private key for decryption—to improve security. Strength of encryption algorithm is often measured by key length and complexity, with longer keys generally

providing higher levels of security. Additionally, terms such as encryption protocols, including SSL/TLS, and encryption modes, such as ElectronicCodebook (ECB) and CipherBlockChaining (CBC), play an important role in determining how data is securely encrypted and transmitted over a network. Also, encryption standards and rules, such as AES (Advanced Encryption Standard) and GDPR (General Data Protection Regulation), shape encryption practices and compliance requirements in various industries and jurisdictions. Understanding the terminology surrounding encryption is fundamental for implementing effective security measures and safeguarding sensitive information in today's digital landscape.

B. Cryptography

In the realm of cryptography, a multifaceted field at the intersection of mathematics, computer science, and information security, a diverse array of terminology arises, reflecting the complexity and importance of securing digital communications and data. At its core, cryptography involves the development and application of mathematical algorithms and protocols aimed at transforming plaintext information into ciphertext, rendering it unintelligible to unauthorized parties. Key concepts within cryptography include encryption, the process of encoding data using cryptographic algorithms and keys to ensure confidentiality; decryption, the reverse process of converting ciphertext back to plaintext using the appropriate keys; cryptographic keys, which are strings of data utilized for encryption and decryption operations; symmetric encryption, which encrypts and decrypts data using the same key. increased security and flexibility are provided by asymmetric encryption, which uses distinct public and private key pairs for encryption and decryption; cryptographic hash algorithms, To guarantee authenticity and integrity, it creates a fixed-size hash from the input data. Asymmetric cryptography is used by some digital signatures to offer an avenue for confirming the integrity and validity of a digital message or document. Understanding and leveraging these cryptographic concepts are vital for addressing contemporary cybersecurity challenges and advancing secure communication technologies.

C. Advanced Encryption Standard (AES) Algorithm

The Advanced Encryption Standard (AES) algorithm, also known as Rijndael, is a symmetric block cipher selected by the National Institute of Standards and Technology (NIST) in 2001 to replace the existing Data Encryption Standard (DES). AES operates on fixed-size blocks of data, typically 128 bits long, using keys of varying lengths: 128, 192, or 256 bits. The algorithm consists of several key components: low-byte, row shift, column shuffle, and round key addition transformations performed over several rounds depending on the key size. Subbytes involve replacing each status byte with the corresponding byte in the S-box, a predefined lookup table. The row shift function rotates the rows of the state array to provide byte-by-byte distribution. Mix Columns work with state array columns to combine bytes with a linear transformation for further scaling. data. For round keys that are generated from the primary key, Add-Round-Key applies an exclusive OR condition. The key length determines how many rounds there are. A 128-bit key requires 10 rounds, a 192-bit key requires 12 rounds, and a 256-bit key requires 14 rounds. As a result of its high level of security, demonstrated ability to withstand a number of cryptographic assaults, and effective implementation across a broad range of hardware platforms, AES is one of the most commonly used cryptographic algorithms in use today.

AES uses key expansion in addition to the core modifications to create a sequence of round keys from the original key. This procedure entails iterating over a key schedule and determining the round keys needed for each encryption and decryption round by combining byte substitution, rotation, and XOR operations. The strength of the Advanced Encryption Standard's (AES) substitution-permutation network (SPN) structure is the main factor contributing to its security.which provides confusion and diffusion properties essential for cryptographic security. The sub bytes transformation introduces non-linearity by substituting bytes using the S-box, Row shifting and column shuffling operations ensure that the result of a single round depends on all input bytes, making it more resistant to differential and linear cryptographic analysis. Additionally, the round key addition step introduces key material states. providing the encryption with the unique properties of the specific key. The robustness of AES has been extensively evaluated through cryptanalysis efforts, including differential, linear, and algebraic attacks, with no significant weaknesses discovered in the standard version of the algorithm. However, variants such as AES-192 and AES-256 offer increased key length for heightened security against brute-force attacks, accommodating the evolving threat landscape. Overall, AES stands as a cornerstone of modern cryptography, underpinning secure communication, data storage, and privacy protection in numerous applications ranging from banking and e-commerce to government and military systems.

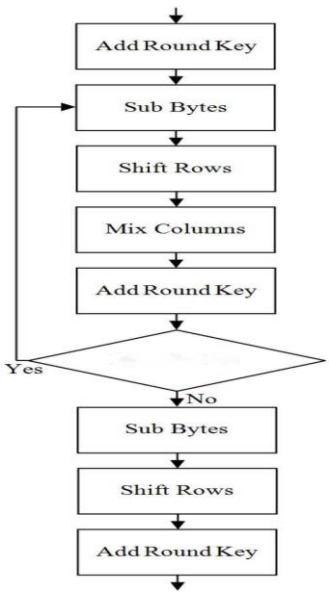

Fig.1. AES Algorithm Work Flow

D. DES Algorithm

3DES also known as Triple DES or TDES, is an improved version of the original DES algorithm designed to eliminate vulnerabile to the brute force attack due to smaller key sizes. 3DES works by sequentially applying the DES algorithm three times to each block of data using three individual keys. It employs a key length of 168 bits, divided into three 56-bit subkeys, providing increased security compared to the original DES while maintaining compatibility with existing systems. The algorithm consists of an encryption phase, where the plaintext undergoes an initial encryption using the first key, followed by a decryption phase using the second key, and finally another encryption phase using the third key. This triple application of DES provides an effective key length of 168 bits, significantly enhancing resistance against brute-force attacks compared to the original 56-bit DES key. Despite its enhanced security, 3DES is slower and less efficient than modern encryption algorithms like AES due to its reliance on multiple iterations of DES. However, it is still commonly used in many applications, particularly to meet with current standards and regulations like the Payment Card Industry Data Security Standard (PCI DSS) or in legacy systems that do not support AES.

Apart from its fundamental functions, 3DES offers many modes of operation, such as Cypher Block Chaining (CBC), Cypher Feedback (CFB), and Electronic Code Book (ECB), which offer supplementary security measures and encrypt data blocks of varying sizes. like information. honesty as well as confidentiality. In the case of encrypting recurring data patterns, for instance, security issues may arise since ECB mode encrypts each data block independently. However, before encryption in CBC mode, every plaintext block is XORed with the preceding ciphertext block. providing randomness that reduces the vulnerabilities present in ECB mode. Moreover, 3DES supports keying options like two-key 3DES (where the first and third subkeys are the same), which balances security with efficiency in scenarios where three unique keys are not feasible. Despite its resilience against brute-force attacks, 3DES is not immune to other cryptographic attacks, and its effectiveness diminishes over time as computing power advances. Consequently, modern encryption standards like AES have largely supplanted 3DES in new implementations due to their superior performance and security properties. Nonetheless, 3DES remains a critical component in various legacy systems and serves as a transitional encryption solution during migration to more robust cryptographic standards. software implementations of 3DES are more flexible and portable, allowing for easier integration into diverse computing environments, but they may suffer from slower processing speeds compared to dedicated hardware solutions. Additionally, 3DES is subject to various security considerations, including key management practices to safeguard against key leakage and exploitation. Effective key management involves securely generating, storing, distributing, and periodically updating encryption keys to prevent unauthorized access to sensitive data. Organizations must also comply with industry regulations and standards governing the use of encryption algorithms such as 3DES. ensuring compliance with data protection laws and safeguarding sensitive information from unauthorized access and disclosure. Despite its age and potential limitations, 3DES continues to play a crucial role in securing data in numerous sectors, underscoring its enduring relevance in contemporary cybersecurity landscapes.

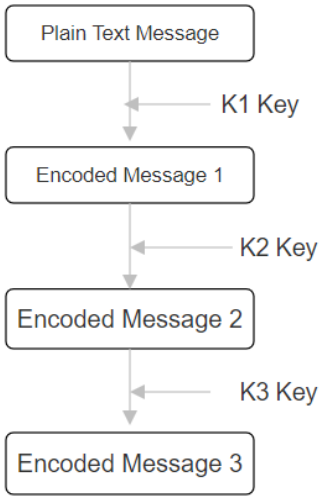

Fig.2. 3DES Algorithm Work Flow

III. Methodology

- The user have to do the registration , if the user already existed, then he/she should login with their credentials like username ,password, and colour code.
- The user while registration, as we included two-layer password protection system, so the user has to give the password also the user has to select three colours as a colour code combination and the user have to remember both password and colour code combination.
- After the user logins with his/her credentials , user have to select the file which he/she wants to store in our file storage system.
- Once the user selects the file, the file will get encrypted by AES and 3DES algorithms.
- After being encrypted with both AES and 3DES algorithm's, the chosen file is uploaded as an encrypted file in directly in to the database.
- After the uploading any file (PDF, Audio, Video and Image), our file storage system will give two keys, the user can directly copy those both keys by clicking on the copy button on the screen and the user have to store those two keys manually.
- These unique keys will be created for each unique file and these particular keys has to be submmited when the user wants to download any particular file
- If the user lost the keys, then he/she cannot download that particular file
- Users can access and download files they've uploaded or have been granted access to.
- When user chooses a file for download, they must provide both keys for decryption.

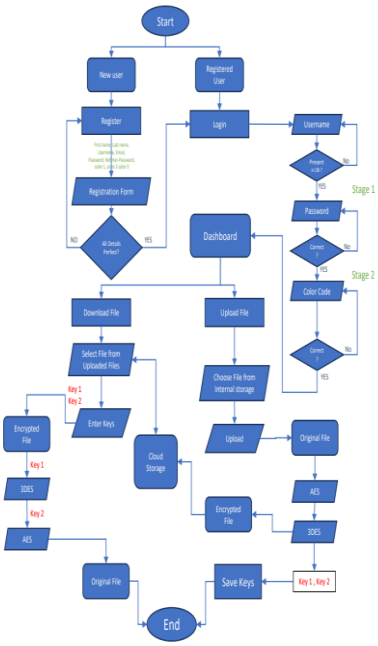

Fig.3. WorkFlow

- With this keys, the user can download the decrypted file and view it in its original form.
- The system also assesses the security of the two encryption algorithm combinations, AES and 3DES.
- Users can log in if they are already registered or register by providing details including name, email address, account password and color code

IV. Results

- The two layer password protection will be as shown in the below figure.

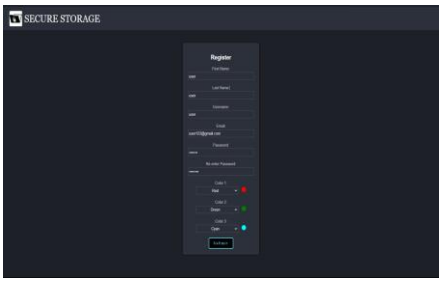

Fig.4.1 Two Layer password protection

- The file(document, image, audio and video) will be stored in the encrypted file in the database.

Fig.4.1 Encrypted Documents

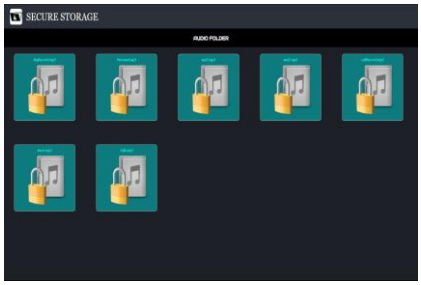

Fig.4.2. Encrypted Audios

Fig.4.3. Encrypted Video

Fig.4.4 Encrypted Image

V. Conclusion

In conclusion, this project stands as a significant achievement in the domains of data security and file management, reflecting our unwavering commitment to providing a secure, efficient, and user-friendly platform for digital asset management. The seamless registration and login processes emphasize the user-centric design, enabling swift access to the system and files.

Utilizing two robust hybrid encryption algorithms, AES and DES, underscores our dedication to storing data with the utmost security, enhancing

confidentiality, and showcasing strong security measures. The meticulously crafted user interface prioritizes ease of use, catering to users with varying levels of technical proficiency, facilitating effortless file management tasks such as uploading, viewing, and downloading.

Furthermore, the additional security layer of sending decryption keys to users' registered email addresses bolsters data protection, ensuring that only authorized users can access their files, thus thwarting unauthorized access attempts. An outstanding feature of our system is the empowerment of users to make informed decisions regarding their preferred encryption method, giving customers the ability to adjust security settings to suit their unique requirements and risk profiles.

Looking ahead, the system's scalability and flexibility ensure its adaptability to evolving technological landscapes, promising continued efficacy and relevance in safeguarding digital assets. As we progress in the realms of data security and file management, this project serves as a testament to our commitment to innovation, user empowerment, and upholding the highest standards of security.

VI. Future Work

- Incorporate multi-factor authentication (MFA) to enhance login security. This may include utilizing SMS-based codes, biometric verification, or hardware tokens for an additional layer of protection.
- Develop a mobile application for greater accessibility, enabling users to manage their files securely from their smartphones and tablets.
- Provide users with automated backup choices and the capacity to manage various versions of their files. Users may benefit from this if they inadvertently erase or alter data.
- As the user base grows, ensure the system can handle increased load by optimizing performance and scalability.

References

[1] Paul Stanton. Securing Data in Storage: A Review of Current Research. 2004.

[2] Zhirong Shen, Wei Xue, and Yingxun Fu. “Secure storage system and key technologies”. In: Jan. 2013, pp. 376–383. ISBN: 978-1-4673-3029-9.

[3] Priyanka Vadhera and Bhumika Lall. “Review paper on secure hashing algorithm and its variants”. In: International Journal of Science and Research (IJSR) 3.6 (2014), pp. 629–632.

[4] Nirmaljeet Kaur and Sukhmani Sodhi. “Data Encryption Standard Algorithm (DES) for Secure Data Transmission”. In: 2016

[5] Punam V. Maitri and Aruna Verma. “Secure file storage in cloud computing using hybrid cryptography algorithm”. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (2016), pp. 1635–1638.

[6] Ako Abdullah. “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”. In: (June 2017).

[7] N. Khatri. “Blowfish Algorithm”. In: IOSR Journal of Computer Engineering (IOSR-JCE) 16.2 (10 2017), pp. 80–83. ISSN: 2278-0661 (e-ISSN), 2278-8727 (p-ISSN).

[8] Rongzhi Wang. “Research on Data Security Technology Based on Cloud Storage”. In: Procedia Engineering 174 (Dec. 2017), pp. 1340–1355.

[9] Lovejeet Kamboj. “SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM”. In: International Journal of Advanced Research in Computer Science 9 (Feb. 2018), pp. 773–776.

[10] Swarna and Marrynal S. Eastaff. “Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm”. In: 2018.

[11] Thilina Dharmakeerthi. A Study on Secure File Storage in Cloud Computing using Cryptography (April 2020). May 2020.

[12] A. Sadanand Ghadi. “Secure File Storage Using Hybrid Cryptography”. In: International Journal of Innovative Science and Research Technology 5 (12 2020). ISSN: 2456-2165.

[13] Amey Jadhav and Prachi Talwar. “Review of Secure File Storage on Cloud using Hybrid Cryptography”. In: INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY (IJERT) 09 (02 2020).

[14] Shruti Kanatt, Prachi Talwar, and Amey Jadhav. “Review of Secure File Storage on Cloud using Hybrid Cryptography”. In: INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY (IJERT) 09 (02 2020).

[15] Putta Bharathi et al. “Secure File Storage using Hybrid Cryptography”. In: 2021 6th International Conference on Communication and Electronics Systems (ICCES). 2021, pp.

[16] Uttam Kumar and Jay Prakash. “Secure File Storage”. In: International Journal of Pure and Applied Mathematics 10 (IV 2021), pp. 335–338. ISSN: 2321-9653.

[17] Joseph Selvanayagam et al. “SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY”. In: International Journal of Pure and Applied Mathematics. 2021.

[18] V. Sharma et al. “SECURE FILE STORAGE SYSTEM”. In: Proceedings of the 5th International Conference on Information Systems and Computer Networks (ISCON). 2021, pp. 600–609.

[19] M. Batra et al. “Secure File Storage in Cloud Computing Using Hybrid Encryption Algorithm”. In: INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY 07 (2022).

[20] Bello Buhari et al. “Design Of A Secure Virtual File Storage System On Cloud Using Hybrid Cryptography”. In: International Journal of Advanced Networking and Applications 13 (Apr. 2022), pp. 5143–5150.