SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY

Dr. K. JAYASAKTHI VELMURUGAN
Department of Computer Science
Jeppiaar Engineering College
jayasakthivelmurugan@gmail.com
Chennai, India

HARIPRABHU M (1)
Department of Computer Science
Jeppiaar Engineering College
hariprabhu2323@gmail.com
Chennai, India

HARI KRISHNAN A.L (2)
Department of Computer Science
Jeppiaar Engineering College
harikrish0122001@gmail.com
Chennai, India

HARISH R (3)
Department of Computer Science
Jeppiaar Engineering College
harishrethinam@gmail.com
Chennai, India

Abstract

In the modern age, security has become a significant issue in sensitive information.

The need for secure file system is more important than ever with the increasing use of computers and the internet.

In this paper, we propose a safe file system that uses hybrid cryptography and image steganography to ensure a high security level to sensitive data.

The system combines the strengths of both Cryptography and Steganography to create an unbreakable Security Solution. The proposed secure file system is based on a hybrid cryptographic approach that uses asymmetric and symmetric encryption algorithms. The symmetric algorithm is used to secure data while the symmetric algorithm is used to encrypt the symmetric key

This approach ensures that data are encrypted with a key that is only known to the authorized parties. To further improve the security of the proposed File system, we have used Image Steganography to hide encrypted data within an image file. The image file looks normal, but contains encryption that is hidden inside the pixels.

This approach provides a further layer of security to the data by making it harder to detect and retrieve.

The proposed secured file system includes various encryption algorithms to enhance its security measures. In particular the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest Cipher 4 (RC4) are used in this system.

AES is a block cipher that uses a fixed size of 128 bits and key size of 128, 192 or 256 bits.

AES is known for its high level of security and has been adopted as the Standard by many organizations for protecting their sensitive data.

DES is another symbiotic key encryption algorithm that was widely used in the past It uses a 56-byte key size and a 64-bit block size.

DES is considered to be a secure algorithm even despite the small key size, and has been used in various applications.

The stream cipher algorithm RC4 is widely used on wireless networks and other applications which require high-speed encryption.

It has variable key sizes and is known for its simplicity and speed. Although RC4 was used widely in the past, it is considered now less secure because of several vulnerabilities that have been identified. In the proposed system, these algorithms are combined to provide improved security measures.

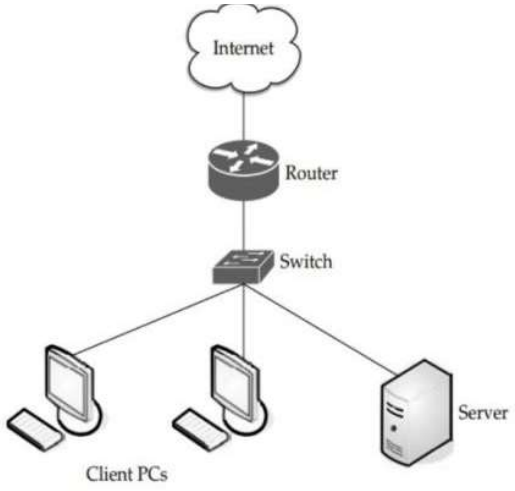
The SYNCYMNESIS encryption (such as AES or DES) is used to encrypt file data whereas the symmetric crypt algorithm (such as RSA) is used for the key exchange. The use of multiple encryption algorithms provides more robust The proposed secure file system is designed to be user friendly and easy to use. It offers a secure interface for users to securely download and access their files.

Keywords — Cloud Computing, Steganography, AES, DES, RC4..

I. INTRODUCTION

Information security has become a major concern in today's digital age. With the growing reliance on digital data, the need for secure storage and transmission of information has become paramount. One of the important components of secure storage

and transmission of information is a secure file system. A secure file system is a software component designed to ensure the confidentiality, integrity, and availability of data stored on a computer or other digital device. This article presents a secure file system that uses hybrid cryptography and image steganography to provide a high level of security. Hybrid cryptography is a combination of symmetric and asymmetric cryptography algorithms that provides secure encryption and decryption of data. Image steganography is a technique of hiding secret data in images, making it difficult for unauthorized people to detect the presence of hidden data. To implement the proposed secure file system, we use a combination of popular encryption algorithms such as AES, DES and RC4. AES is a symmetric encryption algorithm that provides strong encryption and is widely used in secure data transmission. DES is another symmetric encryption algorithm used in many applications and provides a high level of security. Finally, it is easy to use and does not require any additional software or hardware components. In this article, we describe the architecture of the proposed secure file system, including encryption and decryption algorithms, image steganography to hide data, and password authentication mechanisms for file control access. We also discuss the implementation of a secure file system and its performance evaluation. Finally, the proposed secure file system provides high levels of security, confidentiality and integrity for digital data stored on computers or other digital devices. The use of hybrid cryptography and image steganography makes it an effective tool to protect sensitive information from unauthorized access. The system is implemented using popular encryption algorithms such as AES, DES, RC4, etc., providing a safe, efficient and reliable solution for data storage and transmission.



II. LITERATURE REVIEW

Hybrid Cryptography:

Hybrid cryptography is a combination of symmetric and asymmetric cryptography that provides the benefits of both techniques. The symmetric key cryptography is used for encrypting the file data, while the asymmetric key cryptography is used for encrypting the symmetric key. This technique provides better security and faster encryption and decryption speeds.

In a study conducted by Sharma and Singh (2021), the authors proposed a hybrid cryptography-based approach for secure file storage. The approach used a combination of AES and RSA encryption algorithms to encrypt the file data and symmetric keys, respectively. The results showed that the proposed approach provided high security and fast encryption and decryption speeds.

In another study, Zhang et al. (2020) proposed a hybrid cryptography-based approach for secure file sharing in the cloud. The approach used a combination of AES and ECC encryption algorithms to encrypt the file data and symmetric keys, respectively. The authors also used homomorphic encryption to enable secure computations on the encrypted data. The results showed that the proposed approach provided high security and efficient file sharing in the cloud.

Image Steganography :

Image steganography is a technique for hiding secret data within the pixels of an image without changing the image's visual appearance. This technique provides a high level of security as the hidden data is not visible to the naked eye.

In a study conducted by Deshmukh and Thorat (2020), the authors proposed an image steganography-based approach for secure file storage. The approach used LSB (Least Significant Bit) embedding to hide the encrypted file data within the pixels of an image. The authors also used a secret key for encrypting the file data before embedding it in the image. The results showed that the proposed approach provided high security and fast encryption and decryption speeds.

In another study, Abdelhakim et al. (2020) proposed an image steganography-based approach for secure data storage in the cloud. The approach used a combination of RSA and AES encryption algorithms to encrypt the file data and symmetric keys, respectively. The authors also used LSB embedding to hide the encrypted file data within the pixels of an image. The results showed that the proposed approach provided high security and efficient file storage in the cloud.

III. IMPLEMENTATION

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as the keys will be sent to receiver mail in encrypted form and only the authorized user has access to their files.

1. User Registration:

- For accessing the services the user must first register themselves in the database.

- During the registration process various data like Name, username, password, email id, the phone number will be requested to enter.
- Using this data the server will recognize the user as whether the user is new user or existing user.
- If it is new user, the details are stored in the Database. If not, it prompts as user already exists.

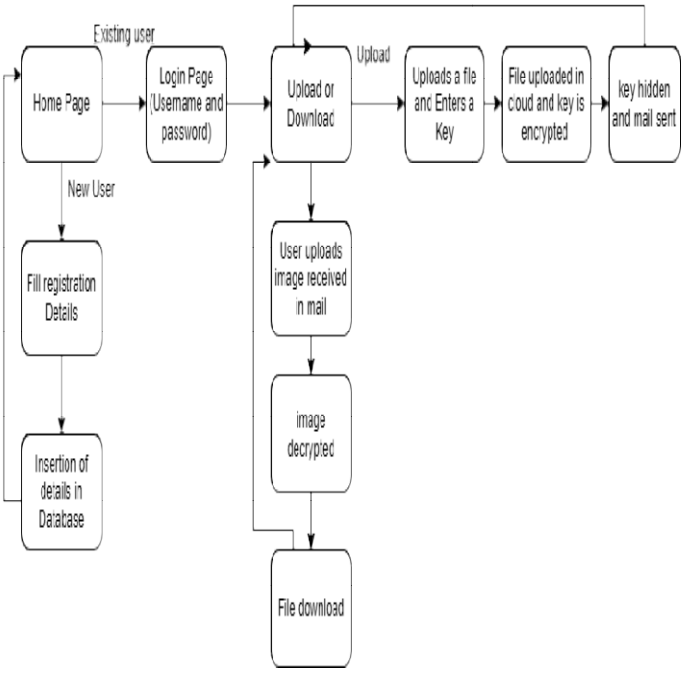
2. Uploading a File on Cloud

- When the user uploads a file on the cloud first it will be uploaded in a temporary folder.
- Then user enters a key..
- The key will be encrypted using different algorithms that are AES, DES, RC4.
- Thus the key to these algorithms will be retrieved from the steganographic image.
- Then the image is sent to receiver's mail.

3. Download a File from the Cloud

- When the user requests a file to be downloaded, they requested to upload a image received through their mail.
- Then the image will be decrypted using the same algorithms with which they were encrypted.
- Thus the key to the algorithms for the decryption process will be retrieved from the steganographic image created .
  .
- Then file will be sent to the user for download.

IV. SYSTEM OVERVIEW



V. HARDWARE REQUIREMENT

- Stable Internet connection.
- RAM – Minimum 4 GB
- Processor – Minimum 2.5 GHz
- OS – Windows, Linux or MAC

VI. SOFTWARE REQUIREMENT

- PYTHON
- FLASK
- JAVASCRIPT
- HTML
- CSS
- AWS

VII. PROPOSED SYSTEM AND ADVANTAGE

The system is designed such that it works in the following way:

1. The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id,phone number, password for account etc.
2. The user then selects the file that is to be uploaded by browsing from local storage.
3. Then the user enters the key. The proposed system provides a combination of AES ,DES and RC4 algorithm to encrypt.
4. The selected file gets uploaded in the cloud.
5. The user also has the option of viewing the files that they have uploaded or have access to and downloading them.
6. On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration orsign-up.
7. Using this key, the user can download the decrypted or original file.

There are many advantages of using cloud storage include:

1. It eliminates the need for carrying physical storage devices.
2. Data in any format can be stored using cloud storage.
3. Cloud storage provides safe backup, as opposed to physical storage devices where loss of device, data corruption by a virus, natural disasters, amongst other causes, can lead to loss of data.
4. Cloud storage is more cost-effective as it eliminates the need to invest in hardware.
5. Cloud storage also helps developers collaborate and share their work in a more efficient and speedy manner.

6. Another advantage of cloud storage could be additional security. The proposed system aims to make the cloud storage system
7. secure using data encryption. Thus, the aim of the proposed system is to increase security of data uploaded onto the cloud by
8. using encryption algorithms to make the system more secure

VIII. CONCLUSION

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using RC4, DES and AES algorithm. Key information is safely stored using LSB technique (Steganography). Less time is used for encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server.

IX. REFERENCE

1. Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).

2. Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm toEnhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

3. Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.

4. Sunita Sharma ,Amit Chugh:'Suvey Paper on Cloud Storage Security'.Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud.

5. 1. A Hybrid Cryptography Algorithm for Cloud Computing Security, International journal of Core Engineering & Management – 2017.

6. 2. A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique, International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) - 2020

7. 3. A Novel Technique of Cloud Security Based on Hybrid Encryption by Blowfish and MD5, 4th IEEE International Conference on Signal Processing, Computing and Control - 2017.

8. 4. Hybrid Cryptography Algorithms in Cloud Computing: A Review, 15th International Conference on Electronics Computer and Computation ICECCO – 2019.

9. 5. Security of Multimedia in Cloud using Secret Shared Key, International Conference on Computing, Power and Communication Technologies (GUCON) - 2018.

10. 6. Security design for Instant Messaging system based on RSA and triple DES, International Conference on Image Analysis and Signal Processing – 2019

11. 7. Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography International Conference on Computer Science and Software Engineering (CSASE) – 2020.

12. M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 123-127, doi: 10.1109/CSASE48920.2020.9142072.

13. A. Rashid and A. Chaturvedi, "Cloud Computing Characteristics and Services A Brief Review", *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421-426, 2019.

14. "Hybrid encryption | Tink | Google Developers", *Google Developers*, 2022. [Online].

15. P. P. Chinnasamy, s. Padmavathi, R. Swathy and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing", *Inventive Communication and Computational Technologies*, vol. 145, 2021.

16. K. Sudharson, M. Akshaya, M. Lokeswari, K. Gopika, "Secure Authentication scheme using CEEK technique for Trusted Environment", *2022 International Mobile and Embedded Technology Conference (MECON)*, pp.66-71, 2022.

17. R. , P. , Y. , and P. , "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing," in 2013 International Conference on Communication Systems and network technologies:

6-8 april, 2013, Gwalior, India, Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2013, pp. 437–439.

18. A. K. Dubey et al, "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment," in 2012, . DOI: 10.1109/CONSEG.2012.6349503.

19. C. Jian-quan, H. Du, X. Zhang, Y. Lin and L. Zeng, "Ensure Data Security in Cloud Storage", *The Quality of Higher Education*, vol. 10, pp. 284-287, 2011.

20. Z. KARTIT and M. EL MARRAKI, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage", *Engineeringletters.com*, 2015. [Online].

21. "Is cloud storage secure? Yes, and here's why", *Tom's Guide*, 2022. [Online].

22. T. Gaur and N. Kharb, "Security of Data Storage in Cloud Computing", *Nanomedicine & Nanotechnology Open Access*, vol. 5, no. 2, 2015.

23. A. Bermani, T. Murshedi and Z. Abod, "A hybrid cryptography technique for data storage on cloud computing", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1613-1624, 2021.

24. U. Kumar and M. Prakash, "A Hybrid Encryption Algorithm for Secure Data Storage on Cloud", *International Journal of Creative Research Thoughts (IJCRT)*, vol. 8, no. 2320-2882, 2020.