IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

File Storage System using Hybrid Cryptography

Ms. S. Suma[1], S. Failur Rahuman[2], A. Ghoushick[3] , R. Hari Ganesh[4]
Assistant Professor, Department of Computer Science And Engineering[1]
UG Scholar, Department of Computer Science and Engineering,[2,3,4]
SRM Valliammai Engineering College, Chengalpattu, India

Abstract: *Now a days file storage system is used in many areas where we can retrieve the data on the users request However, providing our sensitive, personal data to a third party is not exactly the best practice. The only alternative is to make a storage system of our own but that can be tedious to do so and also even if achieved the major stumbling trying to create a secure file storage system is using cryptography, even though it is an excellent and only security measure, but there is a significant drawback in using such technique. Cryptography is based primarily on generation and the proper using of keys if those keys are accidentally leaked or stolen then the entire data, data security is destroyed. A perfect solution is the use of hybrid cryptography in which current encryption is used in combination for additional security. Hybrid cryptography is a concept where we use multiple encryption algorithms to encrypt the file in such a way that the information security is massively improved. Instead of having one good algorithm we will now have multiple 'good' algorithms working in unison to protect the data.*

Keywords: File storage, Hybrid Cryptography, File security

I. INTRODUCTION

In this modern world security is the major concern for many of us, in fact it is the major force that drives us to upgrade ourselves to use all the latest secure technologies. As we see there are a lot of data transferred over the internet and a wide range of applications use secure storage and transferring of data. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from the server. Existing systems often fail when only a certain form of encoding is utilized, depending on a consumer requirement. However, the major issue with this scheme is that each encryption is done with encryption keys, and if these keys are leaked in some manner, the entire data security is destroyed, so we need a solution that can have additional security. As a result, hybrid cryptography is used in this project, in which current encryption techniques are used in a combination. Users must first recover the keys from the authorized person before they can access the data from the server. These keys are then used to decrypt the data, once more with encryption techniques. This approach increases the security and consistency of the data stored in the server.

II. LITERATURE SURVEY

Vivek Sharma& et.alSecure File Storage on Cloud using Hybrid Cryptography: he abstract discusses the importance of Cloud Computing in various industries and how it has changed the way computing is used. However, the security of data stored on the cloud is a concern for many users. The paper proposes a hybrid cryptographic mechanism that combines multiple encryption techniques, such as 3DES and Blowfish, to provide better security for data stored on a single cloud server. The encryption is divided into three parts, each encrypted using a different algorithm and decrypted using different keys when required. This approach ensures that the data is highly secure and cannot be easily accessed by unauthorized users.

Vyom Verma & et.alA Novel Approach for Security in Cloud Data Storage Using AES-DES Hybrid Cryptography: The paper discusses the importance of data security in the era of online communication and the risks associated with transferring data over the internet. It proposes a hybrid cryptographic system that combines parts of AES and DES encryption algorithms to enhance data security on the cloud. The system allows for secure retrieval of data without direct access to the server computer. The paper concludes by comparing the proposed hybrid algorithm to existing AES and DES algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Punam V & et.al Storage in Cloud Computing using Cryptography: The abstract describes a proposed security mechanism that combines symmetric key cryptography algorithms and steganography to enhance data security in cloud computing. The system uses AES, blowfish, RC6, and BRA algorithms for block-wise security and splits the file into eight parts, encrypting each part with a different algorithm simultaneously using multithreading. The system also uses LSB steganography to hide the key information, including which part of the file is encrypted using which algorithm and key. The encrypted file is sent to the receiver via email, and the decryption process involves reversing the encryption process. The paper highlights the issues related to delivering keys to multiple users and discusses the benefits and drawbacks of symmetric and public key cryptography algorithms, including RSA and ECC. Finally, the text emphasizes the use of text steganography technique to provide high security for data while keeping its existence hidden from unauthorized users.

Putta Bharathi & et Secure File Storage using Cryptography: One of the components of the image processing in the medical area, which is the most recent field to see growth, is the processing of magnetic resonance imaging (MRI). Finding the tumour is frequently the first stage. This study explains the thresholding method for brain tumour identification. The suggested method can effectively be used to recognise and isolate brain tumours in MRI images collected from patient databases. It functions as a useful tool for doctors who practise in this area.

III. EXISTING SYSTEM

The file storage systems that are currently in use brings out the case of data security where the user have no other choice but to provide his personal/sensitive data to a third-party vendor who provides a file storage system. Even if you managed to create a file storage system it will end up using cryptographic security measures even though it is secure there is always a chance for a skilled person with malicious intent to get control of our files. The amount of storage required to store the data is huge as there is no compression or workaround methods for it.

IV. PROPOSED SYSTEM

The main purpose of the system is to achieve a way to protect our sensitive, personal files by creating our very own secure file storage system. Improving security massively by the usage of multiple encryption algorithms viz., RSA algorithm, AES algorithm, CHACHA algorithm in a combination for a single file to make the storage system virtually impenetrable for the outsiders. Providing a way to store large files on a single central location with lot of storage whereas devices with less storage can delete the file after uploading to the central system after uploading through the file storage system the resultant 'secret key' key size will be astronomically small as compared to the original file size.

V. SYSTEM ARCHITECTURE DESIGN

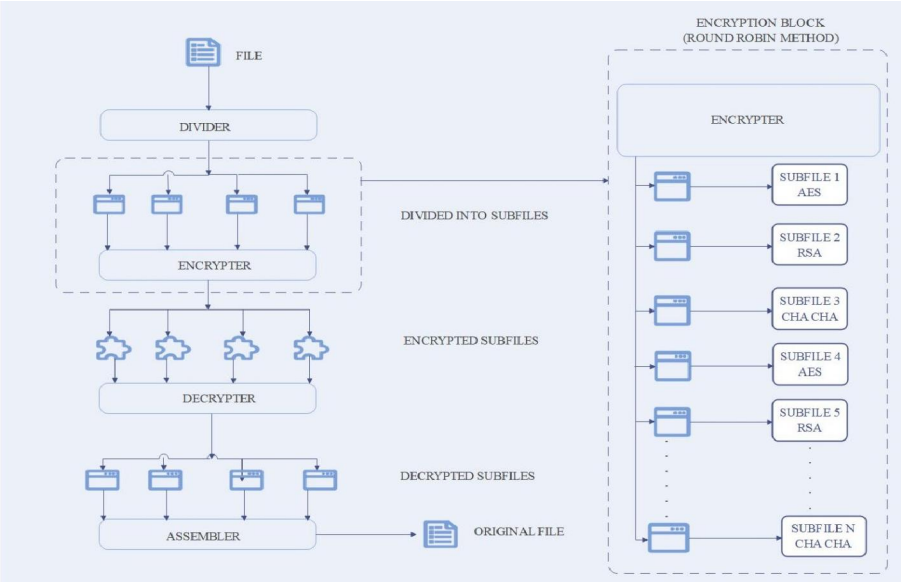

Figure 1: Hybrid Cryptography Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

VI. IMPLEMENTATION

6.1 Divider

Before the encryption process can begin, the input file is first passed into the divider module. The purpose of the divider module is to split the file into smaller blocks of a fixed size. Typically, the block size is set to 1 MB. This ensures that large files can be easily processed and encrypted without consuming too much memory or disk space. However, it is important to ensure that the block size does not exceed the buffer size, which is typically set to 50 GB. This prevents buffer overflow errors and ensures that the process runs smoothly. After the file has been divided into blocks, the blocks are saved in a folder named "Files". This folder will be used later in the encryption process. Additionally, a metadata file is created to store information about the blocks. This metadata file contains the number of blocks that the original file has been divided into, as well as the corresponding key filename. The metadata file is important for future reference, as it contains information that is needed for the reassembly of the encrypted file. The number of blocks indicates how many blocks need to be decrypted and reassembled to obtain the original file. The corresponding key filename is used to locate the key file that is needed to decrypt the data. Without this metadata file, it would be difficult to reassemble the encrypted data into the original file.

6.2 Encrypter

The encryption module is where the actual encryption takes place. The divided blocks that were stored in the "Files" folder during the divider module are used in this module. The encryption module employs four different algorithms for encryption: AESCCMA, AESGCMA, RSA, and CHACHA20POLY1305. The selection of the algorithm is done using the round-robin method to ensure that each block is encrypted using a different algorithm. This helps to ensure that the encryption is secure and cannot be easily decrypted. After each block has been encrypted, the encrypted block is saved with a filename "SECRET" and its corresponding block number. This ensures that the blocks can be easily identified and reassembled during the decryption process. Additionally, a key file is generated for the entire uploaded file. This key file is used later to restore the original file. The use of multiple encryption algorithms helps to ensure that the encrypted data is highly secure. Each algorithm has its own strengths and weaknesses, and by using multiple algorithms, the encryption process becomes more robust and less susceptible to attack. The round-robin method of selecting the algorithm ensures that each block is encrypted using a different algorithm, making it even more difficult to crack.

6.3 Decrypter

When it comes to decrypting encrypted data, the key used in the encryption process is crucial. Without the exact key, it is almost impossible to break the encryption algorithms used. The data is decrypted using the key that is uploaded by the user, and the key is used to unlock the levels of encryption, i.e., the key is used every time a level of decryption happens. After decryption, the data is obtained in the form of decrypted blocks. These blocks are arranged in a specific order, and the original data can only be obtained by arranging the blocks in the correct order. The decrypted blocks are then reassembled to form the original data. The key used in the encryption process is crucial in decrypting the encrypted data, and without it, it is almost impossible to break the encryption algorithms used. By using encryption techniques such as AESCCMA, AESGCMA, RSA, and CHACHA20POLY1305, we can keep our data safe from unauthorized access and theft.

6.4 Assembler

Once the data has been decrypted using the key, the assembler takes the decrypted blocks of data from the folder files. The assembler is a software component that reassembles the decrypted blocks into the original data file. It does this by accessing the metadata that was created in the Divider process. The metadata contains all the necessary details that are required for the reassembly of the blocks of data. The metadata consists of the number of blocks that the particular original file was divided into. This is important because the assembler needs to know how many blocks of data it needs to reassemble to obtain the original data file. The metadata also contains other information such as the size of each block and the order in which the blocks need to be reassembled. The assembler uses this information to reassemble the decrypted blocks of data into the original data file. This process is performed so that the assembly of decrypted blocks

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

to obtain the original data file is a seamless transition. The assembler ensures that the blocks are arranged in the correct order, and any missing or damaged blocks are detected and reported.

VII. CONCLUSION

The secure file storage system created through the combination of multiple encryption algorithms offers a robust and highly secure way to protect personal and sensitive data. By leveraging the strengths of the RSA, AES, and CHACHA algorithms, the system can create a virtually impenetrable shield against unauthorized access, ensuring the privacy and integrity of stored data. In addition to enhancing security, the file storage system offers a centralized storage solution that allows for the storage of large files on a single location. This reduces the need for multiple storage devices and makes it easier to manage and access files from a central location. The system also offers a solution for devices with limited storage by allowing them to delete files after uploading them to the central system. Furthermore, the use of hybrid cryptography results in a small secret key size, making it easier to store and transfer keys securely. Overall, the secure file storage system provides a powerful solution for protecting sensitive data and is an important step towards a more secure and private digital world.

VIII. FUTURE WORKS

- Optimization: When it comes to file storage systems that utilize hybrid cryptography, one of the challenges is optimizing the system for large file sizes. While the current system works well for large file sizes, it may take some time to encrypt or decrypt these files, which can be inconvenient for users who need quick access to their data, this will be minimized in future versions.
- Scalability: As file storage needs continue to grow, it will be important to ensure that the hybrid cryptography-based file storage system can scale to meet these needs. Future work could focus on developing strategies for scaling the system, such as distributing data across multiple servers or using cloud-based storage.
- Usability: Finally, future work could explore ways to make the hybrid cryptography-based file storage system more user-friendly and accessible to non-technical users. This could involve developing intuitive interfaces or providing clear documentation and support materials.

REFERENCES

[1]. Vivek Sharma; Abhishek Chauhan;Harsh Saxena;Shubham Mishra; Secure File Storage on Cloud using Hybrid Cryptography " 2021 5th International Conference on Information Systems and Computer Networks (ISCON).

[2]. Putta Bharathi;Gayathri Annam;Jaya Bindu Kandi;Vamsi KrishnaDuggana; Anjali T. "Secure File Storage using Hybrid Cryptography" 2021 6th International Conference on Communication and Electronics Systems (ICCES).

[3]. Punam V. Maitri;Aruna Verma " Secure file storage in cloud computing using hybrid cryptography algorithm" 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[4]. Vyom Verma; Pulkit Kumar; Raj Kumar Verma; Shristi Priya "A Novel Approach for Security in Cloud Data Storage Using AES-DES Hybrid Cryptography"

[5]. Surya Nepal; Carsten Friedrich; Leakha Henry; Shiping Chen "A Secure Storage Service in the Hybrid Cloud" 2011 Fourth IEEE International Conference on Utility and Cloud Computing.

[6]. H Sai Charan Reddy;Vajjala Veera Karthik;Dedeepya V;A Pavan;Sarasvathi V "Data Storage on Cloud using Split-Merge and Hybrid Cryptographic Techniques" 2022 International Conference for Advancement in Technology (ICONAT)

[7]. Osama Ahmed Khashan "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System".

[8]. Guilherme Sperb Machado;Thomas Bocek;Burkhard Stiller "PiCsMu: A system to aggregate multiple heterogeneous Cloud Services' storage" 2014 IEEE Network Operations and Management Symposium (NOMS).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

[9]. Sanjeev Kumar;Garima Karnani;Madhu Sharma Gaur;Anju Mishra "Cloud Security using Hybrid Cryptography Algorithms" 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM).

[10]. Osama Fouad Abdel Wahab;Ashraf A. M. Khalaf;Aziza I. Hussein;Hesham F. A. Hamed "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques".

[11]. Jun Ren;Zhiqiang Yao;Jinbo Xiong;Yuanyuan Zhang;Ayong Ye "A Secure Data Deduplication Scheme Based on Differential Privacy"2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS).

[12]. V. P. Lalitha;M. Y. Sagar;S. Sharanappa;Shredar Hanji;R Swarup Data security in cloud 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)

[13]. C. Radhakrishnan;K. Karthick;R. Asokan "Fragmentation Based Hybridized Encryption Scheme for Cloud Environment" 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).