WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Secure File Storage Using Hybrid Cryptography on Cloud

[1]Birendra Kumar Saraswat, [2]Dr. Amit Singhal, [3]Pavan Bhardwaj, [4]Muhammad Shafique Khan, 5Ankit Sharma, [6]Latika Saini

[1]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) birendrasaraswat@gmail.com
[2]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) amit1408@gmail.com
[3]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) pavan08101999@gmail.com
[4]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) shafique1999s@gmail.com
[5]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) ankitshrama9aug2002@gmail.com
[6]Computer Science & Engineering Raj kumar Goel Institute of Technology Ghaziabad, UP(India) latikasaini2152000@gmail.com

ABSTRACT

Cloud Computing is the on demand availability of resources, through the use of internet. It also provides process and storage of large amount of data online with the help of computing power. However, storing large amount of data creates a concern due to its security and privacy issues. One solution for this problem is to use hybrid cryptography technique for the security issues as it combines both the features of symmetric as well as asymmetric cryptography and it provides secure file storage on the cloud. Data security and privacy protection are the primary problems that need to be solved. The model proposed here is a secure hybrid cryptography approach scenario to provide a safe storage and safe transmission for Confidential Data files. iv Here we've taken several cryptographic algorithms like AES, DES and RC6. These algorithm are want to give block wise security to the whole info so these are going to be used as a hybrid cryptographic algorithm. Here the methodology has firstly loaded the file on the server so divide the file into 3 parts means file slicing is finished then any of those select above cryptographic algorithms & these algorithms are often changed with every part and then uploaded over the different cloud server nodes and can only be encrypted using its key .

Keywords - Cloud Computing and Storage, AES Algorithm, DES Algorithm, RC6 Algorithm

Introduction

The aim of the project is to create an encrypted and secured file storage system to transfer files with in users in a remote location. This model requires an input that is encrypted using algorithm and we can store them anywhere. The uploaded file can be downloaded by the users, they can read them and need to decrypt the file using the decryption algorithm. The system uses public-key cryptographic techniques like RSA and Symmetric key cryptography like AES. Static hashing and dynamic hashing are the techniques used to perform integrity. Due to the encryption of data, confidentiality is also achieved in the process. The project is also open to new challenges and future changes to other advanced technologies in keeping the data secured.

Literature Review

[1]. "Enhanced Security for Cloud Storage using Hybrid Cryptography" by S.S.S Sharma and S. Kumari (2021)

This research proposes an enhanced security model for cloud storage using hybrid cryptography, which combines AES and RSA algorithms for encryption and decryption. The proposed model also includes secure key management system, ensuring the confidentiality and integrity of data in cloud storage. The study evaluates the effectiveness of the proposed model through simulations and experiments, demonstrating its potential for secure cloud storage.

[2]. "A Hybrid Encryption Scheme for Cloud Storage Security" by M.A. Khan, M.A. Rahman, and M. Islam(2020)

This research proposes a hybrid encryption scheme for cloud storage security, which uses both symmetric and asymmetric encryption. The proposed scheme employs AES and RSA algorithms for encryption and decryption, respectively. The study evaluates the security and performance of the proposed scheme through simulations and experiments, demonstrating its effectiveness in mitigating security risks in cloud storage.

[3]. "Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography" by P. Kumar and P. Singh (2019)

This study proposes a hybrid cryptographic model for secure file storage and sharing in cloud computing. The model uses a combination of AES and RSA encryption algorithms, ensuring both confidentiality and integrity of data. The study demonstrates the effectiveness of the proposed model in terms of security and performance through simulations and experiments.

[4]. "Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography" by Mr. Rohit Barvekar, Mr. ShrajalBehere, Mr. Yash Pounikar, Ms. Anushka Gulhane (2018)

The proposed security mechanisms will prevent confidential data from being misused making the system more reliable. The proposed method will make encryption and decryption with keys.

[5]. " Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography" by A. Sharma and K. Sharma(2017)

This study proposes a hybrid cryptography-based model for secure file storage and cloud computing, uses a combination of AES and ECC encryption algorithms. The proposed model ensures confidentiality, integrity and availability through the use of encryption and decryption techniques. The study demonstrates the effectiveness of the proposed model in terms of security and performance through simulations and experiments.

Algorithms Used

Advanced Encryption Standard (AES)

AES is a technique for encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is mostly used nowadays as it is stronger than DES and triple DES and harder to implement[1]. It takes 128 bits as input and outputs 128 bits of encrypted cipher text. AES relies on substitution-permutation network principle.

Data Encryption Standard (DES)

DES is very powerful for attacks and DES is not much popular. DES is a block cipher and encrypts the data, which means 64 bits of plain text go as the input to DES, which produces 64 bits of cipher text. For encryption and decryption same algorithm and key are used[2]. The key length is 56 bits.

Rivest Cipher 6 (RC6)

RC6 is a fast block cipher. It was based on RC5. It works faster as it has more registers than RC5. RC6 uses multiplication of integer number in algorithmic computation[3]. RC6 has a block size of 128 bits and key sizes of 128, 192, and 256 bits up to 2040 bits.

Proposed Model

In this proposed model, for securely storing of data hybrid cryptography is used in the cloud. In this user stores the file in online cloud storage and these will be stored in encrypted format and only the authorized user has access to these files.

Registration of User:

For accessing the services the user must first register themselves. During the registration process various data like the name, username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose[4]. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

Uploading a File on Cloud:

When user uploads the file on the cloud, it will be uploaded in a temporary folder. After that this file will splits into three parts. These three parts will be encrypted using cryptographic algorithms[5]. Each part uses a different encryption algorithm. These three parts will be encrypted using these algorithms that are AES, 3DES, RC6. The key will be retrieved from the steganographic image which is created during the registration. After the split encryption, all three encrypted segments will be stored and over different cloud server nodes.

Downloading splitted file from the Cloud When the user requests a file to be downloaded first the encrypted splitted parts will be downloaded. Then these three parts will be decrypted using the same algorithms with which they were encrypted. Keys to these algorithms for the decryption will be retrieved from steganographic image which is created during the registration[6]. Then these parts are re-combined to form a decrypted file. After that his file will be sent to the user for download.

Conclusion

In conclusion, secure file storage using cryptography on cloud computing is essential for organizations and individuals who want to protect their sensitive data from unauthorized access and breaches. Cryptography provides a secure way to encrypt files, ensuring that only authorized parties can access them.

The use of hybrid cryptography offers a higher level of security for storing files in the cloud, as it combines the benefits of both symmetric and asymmetric encryption. This allows for a more efficient and secure way to store data in the cloud, making it more difficult for hackers to access.

While cloud computing offers numerous benefits, including scalability and cost-effectiveness, it also presents security risks. However, with the implementation of strong encryption methods, including hybrid cryptography, organizations and individuals can mitigate these risks and ensure their data remains secure in the cloud.

Overall, secure file storage using cryptography on cloud computing is a critical component of any organization's security strategy. With advancements in technology and increased awareness of security risks, we can expect to see more sophisticated and effective solutions in the future.

Future Scope

The future scope of secure file storage using hybrid cryptography on cloud computing is promising as more organizations and individuals continue to rely on cloud-based storage and computing solutions. Hybrid cryptography, which combines the benefits of both symmetric and asymmetric encryption, offers a higher level of security for storing sensitive files in the cloud.

Some of future developments in this area are:

1. Increased adoption of hybrid cryptography: As more organizations and individuals become aware of the benefits of hybrid cryptography for secure file storage, we can expect to see an increase in its adoption. This leads to the development of more advanced hybrid encryption algorithms and tools.
2. Advancements in cloud security: As cloud providers continue to invest in their security capabilities, we can expect to see more advanced security features such a key
3. management, access controls, and multi-factor authentication. This will make it easier for users to secure their data in the cloud.
4. Integration with blockchain: The use of blockchain technology can add an additional layer of security to cloud-based file storage. Blockchain-based solutions can provide immutable records of data transactions, ensuring that files remain secure and tamper-proof.
5. Development of quantum-safe cryptography: As quantum computing technology advances, traditional encryption methods may become vulnerable. Quantum-safe cryptography, which is designed to withstand attacks from quantum computers, will become increasingly important for secure file storage in the cloud.

References

[1] Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using a hybrid cryptography algorithm. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 1635–1638.

[2] RashiDhagat, Purvi Joshi (2016)."Secure file sharing using cryptographic techniques in the cloud."International Conference on Communication and Electronics Systems (ICCES).

[3] Tulip Dutta, Amarjyoti Pathak (2016). Secure data sharin in cloud storage using key aggregation cryptography. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304– 1309.

[4] Bhale Pradeep Kumar Gajendra, Vinay Kumar Singh, More Sujeet. (2016). An approach to hybrid cryptography on cloud environment. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 188–192.

[5] Anjali Patil, Nimisha Patel, Dr. Hiren Patel. (2016). Secure data sharing using cryptography in a cloud environment. Far East Journal of Electronics and Communications, 18(4), 521–546.

[6] Bilal Habib, Bertrand Cambou, DuaneBooher, Christopher Philabaum.(2017). Secure data sharing in cloud storage using key aggregation cryptography. International Journal of Pure and Applied Mathematics, 119(16), 3257-3262.

[7] Sharma and K. Sharma(2017), " Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography".

[8] Mr. Rohit Barvekar, Mr. ShrajalBehere, Mr. Yash Pounikar, Ms. Anushka Gulhane (2018). Security in Cloud Computing using Cryptographic Algorithms.

[9] Mr. Rohit Barvekar, Mr. ShrajalBehere, Mr. Yash Pounikar, Ms. Anushka Gulhane(2018), "Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography"

[10] P. Kumar and P. Singh(2019) , "Secure File Storage and Sharing in Cloud Computing using Hybrid Cryptography".

[11] M.A. Khan, M.A. Rahman, and M. Islam(2020), "A Hybrid Encryption Scheme for Cloud Storage Security".

[12] S.S.S Sharma and S. Kumari(2021), "Enhanced Security for Cloud Storage using Hybrid Cryptography".