International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | June 2022 www.irjet.net p-ISSN: 2395-0072

Hybrid Cryptography Algorithm Based Secured Storage Android App

Prathamesh Jagtap[1], Harshal Patil[2]

[1,2]IT Engineer, Savitribai Phule Pune University, Pune, Maharashtra India

---

Abstract - *Currently the ever-increasing usage of portable gadgets and advancement in networking technology is directing us to secure file storage over the internet. Cryptography is the most popularized technology employed for all sorts of data protection. This paper is a broad review of the diverse approaches which are used for securely storing files, and sharing it over the internet. This suggested scheme will also assure the entire system to have confidentiality, integrity, and accessibility mechanisms to be executed in it. In Cloud computing files and software aren't completely held on the user's system. Files are stored on cloud providers system. The cloud provider can provide a solution to this security problem by encrypting the files by employing encryption algorithm. This paper presents a file security system to give an effective result for the underlying problem of security in cloud systems. In this model, hybrid encryption is employed where files are ciphered by file splitting and RSA is used for the secured communication between users and the servers.*

Key Words: Hybrid Cryptography, Storage, Android App, Cloud Server, Integrity, Confidentiality.

1. INTRODUCTION

The idea of the system is to develop an encoded and protected file depository system to transfer files within users in a remote locality. This system will need an input that's successfully ciphered using any of the algorithm methodologies and store them anywhere. The uploaded files and folders can be downloaded by other users through the same app, but to read the data present in it, they've to decipher the file using the decryption algorithm and the data provided about the file within the users by the possessor. The system uses public-key cryptographic approaches like RSA and AES. Hashing methodologies like static hashing and dynamic hashing are used for achieving integrity. Due to the encryption of data, confidentiality is also attained in the course. The project is also open to new challenges and upcoming changes to other advanced technologies in keeping the data protected.

The hybrid cryptographic systems usually have two phases as discussed below:

1. Encryption Phase

Both file and the key generated are encrypted in this phase. The file is then stored to cloud server either fully or as slices. In case of slices, each slice will have hash data.

2. Decryption Phase

The key is first decrypted and is then used to decrypt the file stored on the cloud server.

2. LITERATURE SURVEY

"Secure Storage of Data in Cloud Computing" [1] - Cloud storage brings accessible repository of data, at the same moment there are also hidden security consequences. Data storage security includes authentic access to the data stored in the cloud, namely access authorization and authentication security data sharing and the encryption of stored data to guarantee data confidentiality, cohering of the attainability to effective cryptographic data and inaccessibility to the deleted cryptographic data, using tamper- proof technology to guarantee the verity of the data, as well as using tracking technology to guarantee data traceability. This paper aims secure data deletion in the file system. Here they have designed a file system which supports secure deletion of data that uses CP- ABE which supports fine-coarse access policy to cipher files.

"Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm" [2] - The paper focuses on how files are securely reposited on a cloud platform. Also, it discusses the problem of using only a single algorithm to cipher the file and how inefficient it'll be on the cloud. This paper splits the file into slices and each slice is ciphered using AES, blowfish, RC6algorithm. The key information about which file uses which algorithm is transferred to the receiver utilizing steganography modern approach to file system integrity checking.

3. SYSTEM ARCHITECTURE & FLOW DIAGRAMS

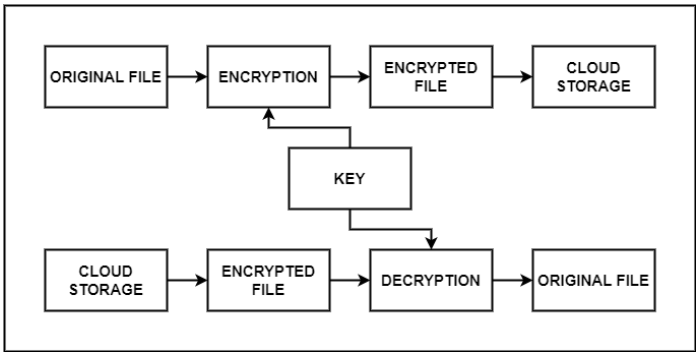

Fig -1: System Architecture

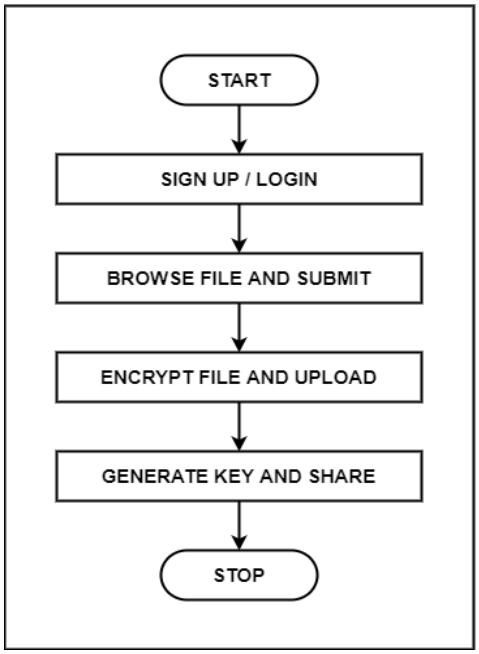

Fig -2: Encryption Flow

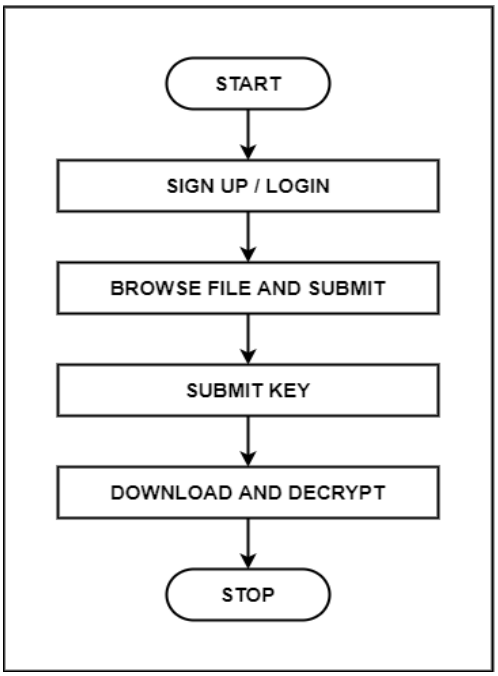

Fig -3: Decryption Flow

4. PROPOSED METHODOLOGY

The methodology proposed and developed in this system is as given below:

1. An Android App is developed in this system.

2. The Android App is built using Android Studio and Java is used as the main programming language.

3. The cloud server used in this system is Google Firebase.

4. The first step includes user Sign Up using a Google Account.

5. The user once registered can now start uploading files to the server.

6. The user can select the file of his/her choice through the local storage i.e., through ROM or SD Card mounted on the system.

7. This file will now be encrypted using Encryption Algorithm and a key for the same will be generated using RSA Key Technique.

8. The encryption algorithm used is AES (Advanced Encryption Standard).

9. This file is then stored to cloud server. A link is then generated for sharing the file.

10. The link can be used to share the file to other users or also to decrypt the file.

11. When the link is accessed through the application it prompts for the key.

12. The key is then authenticated and then the file is downloaded and decrypted into users' local storage.

13. The main user or the owner has the ability to delete the file.

14. He/she cannot edit the contents of the file once it is stored on the cloud as it is encrypted.

15. Files stored without encryption can be edited as well as deleted similar to the files stored on any normal cloud server with proper access to the cloud account.

5. CONCLUSIONS & FUTURE WORK

Considering the survey done in this paper it was identified that secure file storage and sharing would not only requires confidentiality of the files but also authentication and integrity. To meet these requirements an Android Application is proposed and developed which tries to provide an end-to-end solution for securely storing the files. The stored file is completely secured, as the file is being encrypted by employing hybrid cryptographic techniques. Data of the users is stored on a crypted cloud server which helps in avoiding unauthorized access to the files. Data security is a major priority. The system is highly robust, reliable and secure. The android application developed has option for storing normal text file as well as images in any format such as png, jpg, jpeg, gif etc. Future work will include securing and storing other file types such as pdf, doc, exe etc. Finger print authentication and face recognition for granting access to the app can also be employed. Steganography can also be used to some extent to secure images.

REFERENCES

[1] Zhangjie Fu, Xinyue Cao, Jin Wang, Xingming Sun, "Secure Storage of Data in Cloud Computing" - Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014.

[2] Maitri, P. V., & Verma, A. "Secure File Storage in Cloud Computing Using a Hybrid Cryptography Algorithm" - International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016.

[3] Ronak Karani, Tejas Choudhari, Anindita Bhajan, Madhu Nashipudimath, "Secure File Storage using Hybrid Cryptography" International Journal of Innovative Research in Technology, 2020.

[4] Shakeeba S. Khan, Prof. R. R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", 2015.

[5] Anjali Patil, Nimisha Patel, Dr. Hiren Patel "Secure Data Sharing Using Cryptography in Cloud Environment", 2016

[6] Fortine Mata, Michael Kimwele, George Okeyo, "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)".