WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Secure Sharing and Storing Data on Cloud using Hybrid Cryptography

Sahil Paraswal, Riyaj Patel, Ruchita Sarode, Pradhuman Vaidya

Students, Dept. of Computer Science & Engineering, Acropolis Institute of Technology and Research Indore, Madhya Pradesh, India.

ABSTRACT

In Today's world, large amounts of data are seen as a liability from a security standpoint. The more data you have, the greater the number of targets for hackers. Cryptography is the most popular technology used for all types of data security. Our main aim in this project is to provide the ability to user to share the data on different platforms with multiple users and store the data on cloud & their devices securely using Hybrid Cryptography with pure validation and authentication.

Key-Words: - Cryptography, Cloud, Security, Storage, Hybrid Algorithms.

Introduction

Cloud storage enables you to store your data on hosted servers. There is a huge risk of data misuse, when different organizations implement the use of the cloud to save their data. To avoid any such risk and to secure the user data, there is an urgent need to secure the data repositories. Since, sensitive data is present on the cloud there is a need to protect this data from Unauthorized Access.
The proposed paper meets the required security needs and implementation of cryptic data sharing technology. The Paper uses different cryptographic algorithms as per Hybrid Cryptography for encryption of data. The idea of splitting and merging adds on to meet the principle of data security. With the help of our system user can share their encrypted data with others on different platforms like Clouds, Whatsapp, Gmail, Telegram etc. and after pure validation through owner of data others can access it.

Problem Formulation

Security is a very necessary service for any network whether wired or the wireless network communication for enhancement of what was offered by the cloud. Simply by only storing the information and knowledge on clouds does not solve the matter. The matter isn't about data availability, but about the security of information. The characteristic of this method is that the key requires to be joined by reconstruction.Here it is – biggest data breaches in recent history, including details of those affected :

Facebook

Date: April 2019
Impact: 533 million users

In April 2019, it was revealed that two datasets from Facebook apps had been exposed to the public internet. The information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs.

Yahoo

Date: 2014
Impact: 500 million accounts

Yahoo, which suffered an attack in 2014 separate to the one in 2013 cited.
Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for application and data in cloud.

Literature Review

As we have done so much research related to our project, the following published articles have been referred to create a base for my project. Some research papers are publish in recent years on that technology which emphasizes following tenets on this technology :-

It discusses the problem of using only a single algorithm to encrypt the file and how ineffective it will be on the cloud.

The method used for pattern generation is cryptographic hash functions. The system also uses a database that stores the files that need to be protected and their hash codes.

To check the integrity of the file the hash code of the file is produced and checked with one in the database. If the file is successfully tested positively then access is granted otherwise the administrator gets alerted and if it is saved copy is available of the same file then the file is restored. This system uses a database that stores the names of all files that are to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. After the file is verified then only access is granted else the administrator is been alerted about the problems and a saved copy of the same file is restored safely.

The method discussed in the paper uses group signature and encryption techniques. The advantage of this proposed method is that data owners can store the file without showing their true identity to others in the cloud.

Methodology

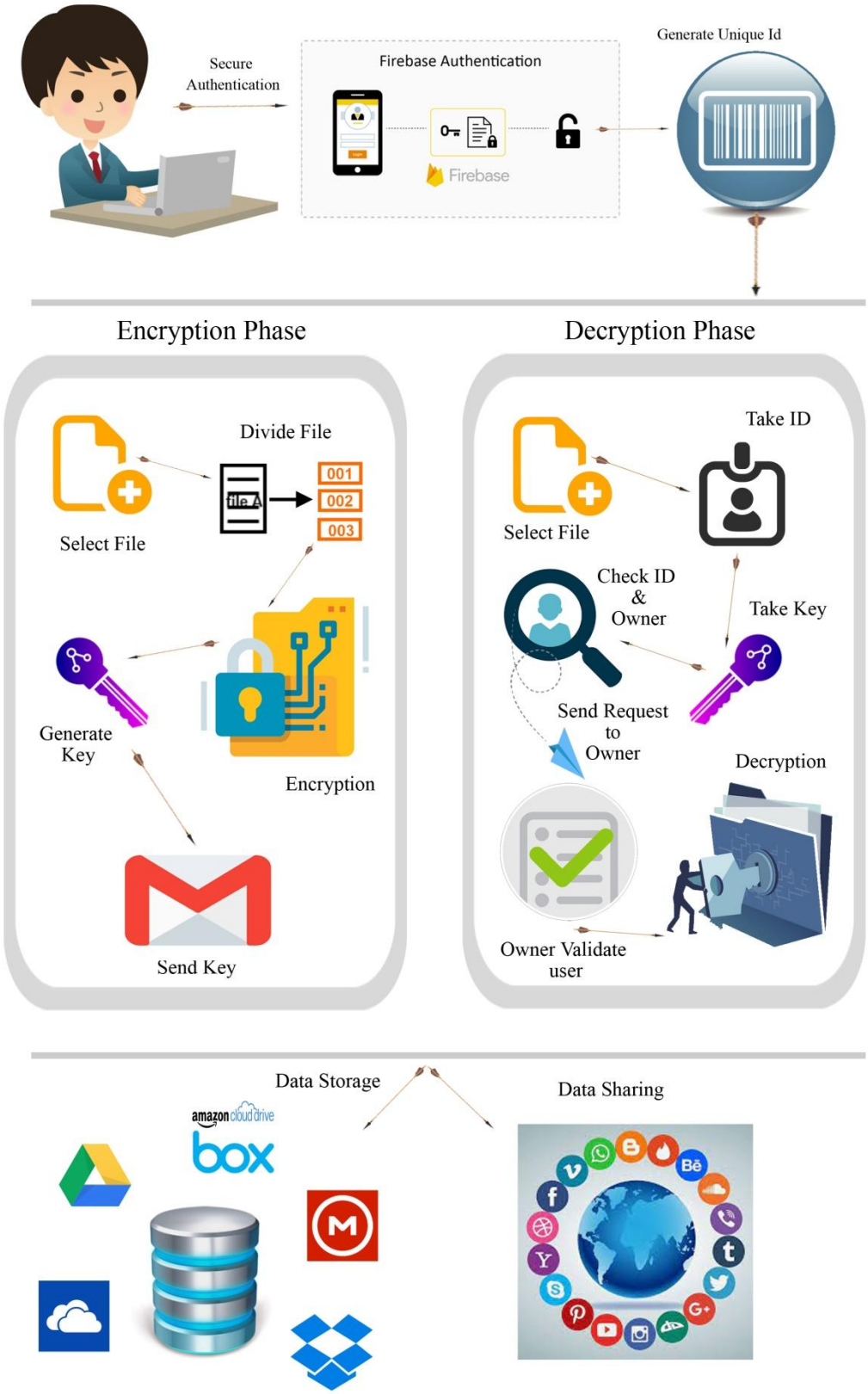
The research process aims to encrypt the user data with the highly securable technology Hybrid Cryptography and the give facility to user to store the data on cloud and second thing is to provide actions to user to share their encrypted data on different platforms and If the friend of user is want to decrypt the data then they can decrypt it in our platform after the complete validation from the owner of data.

Here are the different cryptographic algorithms we use like MD5, Fernet, Multifernet, DES, SHA and AESCCM for hybrid cryptographic algorithm.

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

1. **Secure Authentication:**
   Firstly authenticate the user with the Firebase, The Firebase Authentication SDK provides methods to create and manage users that use their email addresses and passwords to sign in. Firebase Authentication also handles sending password reset emails.
2. **Generate User ID:**
   After the complete authentication, we generate the unique User ID for user. Once the user's credential is validated the user data is stored in our database.
3. **Data Encryption:**
   a. **Select the File :** The user then selects the file by browsing from local storage.
   b. **Divider :** Dividing the uploaded file into N parts.
   c. **Encryption :** As we don't store the user data a first line of file is filled with the unique User ID so it can use for further validation at time of decryption then Encrypting all the parts of the file using any one of the selected .
   d. **Generate Key :** When the encryption is performed at the moment the new encrypted key is generate.
   e. **Email to User :** After the key is generate it will send to user through Email.

1. **Storage:**
   Provide two options two user, first user can store their data in their device local storage and second allowed user to store encrypted data on clouds like Google Drive, Microsoft OneDrive, Dropbox, Amazon Drive.
2. **Sharing:**
   Allow user to share their encrypted data with friends with encrypted key on different platforms like Email, Whatsapp, Telegram, Clouds.
3. **Data Decryption:**
   a. **Select the File :** The user then selects the file by browsing from local storage.
   b. **Take ID :** After the select the file, we take the unique User ID.
   c. **Take Key :** Then take the key from the user.
   d. **Check User ID :** Before decrypt the whole file we first check the User ID which mention in first line of the file at the time of Encryption.
   e. **Check Owner :**
      i. If the User ID in file is match with current user then decrypt the File.
      ii. If the User ID in file is not match then send the request to the owner.
   f. **Send Request :** Send the request to owner of the file for validate their friend.
   g. **Check Validation :** If owner of the file grant the access then decrypt the File otherwise stop the process.
   h. **Decryption :** After all validation and authentication the data of user is proceed for the decryption process, gather the all key and decrypt the all data with help of proposed algorithms.


Secure Authentication
Firebase Authentication
Firebase
Generate Unique Id
Encryption Phase
Decryption Phase
Select File
Divide File
file A
001
002
003
Generate Key
Encryption
Send Key
Take ID
Select File
Check ID & Owner
Take Key
Send Request to Owner
Decryption
Owner Validate user
Data Storage
Data Sharing
amazon cloud drive
box

Result Discussions

In this study the proposed web application was built to provide an encryption/decryption tool and securely share and store the files using cryptographic modules and packages. Now the stored file is completely encrypted we can say that is totally secured from the outside world. The system is very secure and robust. Data of the users is secured on a any cloud server, we don't force to store the data in our cloud user can upload their data on any clouds with the help of our encryption technology which helps in avoiding unauthorized access from the outside world.. Data security is a major priority. This system can be implemented in the banking and corporate sectors to securely transfer confidential data.

Here's the Screenshots of our app:

Firstly user will Sign In or Sign Up.

Fig.1 User Select the File.

Fig.2 Option of Encryption/Decryption is given to user.

Fig.3 After the file is Encrypted, provide the services to user to store and share their data.

Fig.4 For Decryption, take the some information from user like Unique ID, Decryption Key etc.

Fig.5 If the user is the file owner then the file is decrypted otherwise generate the access request to the owner after the file owner is grant the access the file processing for the decryption.

Fig.6 After the file is Decrypted, provide the services to user to store and share their data.

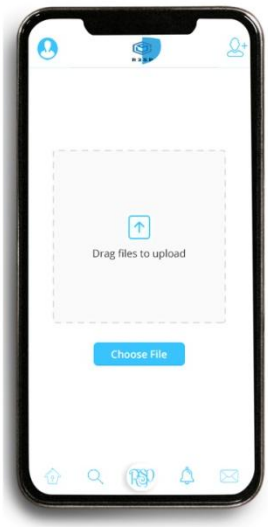


Fig.1

Fig.2

Fig.3

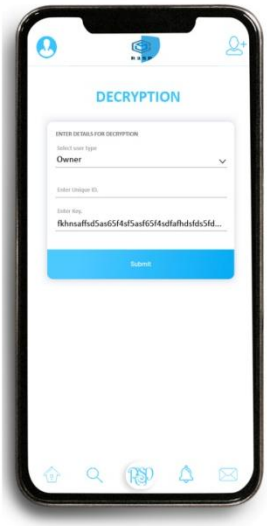


Fig.4

Fig.5

Fig.6

Conclusion

With the growing demands on the cloud storage platforms, simplifying the Interface and solidifying the underlying security is the main concern as the sharing of an individual's data is not as private as one assumes.Security and Sharing of data and their protection are the problems that is solved. Our project build the perfect system with the help of proper validation and authentication so that user can tention free share their data across the globe. Cloud is able to handle the longer-term requirements for accessing multimedia files thanks to limited capabilities of low configured devices available. But the cloud and its users have many privacies and security related aspects that needs special attention.

Acknowledgment

This research is supported by Acropolis Institute of Technology & Research, Faculty of Engineering and Technology. We are thankful to the Professors of our department who assisted this research. We express our appreciation towards our Guide, Prof. Shaifali Shrivastava, Assistant Professor, Dept of CSE, AITR, for providing her guidance and support during this research. We are also thankful for her comments and suggestions on the earlier versions of the manuscript, although any existing errors are our own and should not stain the reputations of respectable professionals.

References

Reference Format for Journal Paper

[1] Kranthi Kumar K, Devi T,(2018). Secured Data Transmission in Cloud Using Hybrid Cryptography. International Journal of Pure and Applied Mathematics, 119(16), 3257-3262.

[2] Bhandari, A., Gupta, A., & Das, D. (2016). Secure algorithm for cloud computing and its applications. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 188–192. https://doi.org/10.1109/confluence.2016.7508111

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

[4] Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies ,pp. 217-222, Dec. 2011.

[5] Srinivasarao D., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[6] R.Nivedhaa and J.Jean Justus. A Secure Erasure Cloud Storage system using Advanced Encryption Standard algorithm and Proxy Re-encryption. Institute of Electrical and Electronics Engineers.2018.

[7] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.

[8] 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.

[9] https://doi.org/10.1109/wispnet.2016.7566416