SECURE DATA TRANSFER USING CRYPTOGRAPHY

Shilpa v
Assistant Professor
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India
shilpav.cse@cambridge.edu.in

Anushree Krishnamurthy
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India
anushree.19cs022@cambridge.edu.in

Bindu S
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India
bindu.19cs033@cambridge.edu.in

Balaji Reddy D
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India
balaji.19cs030@cambridge.edu.in

Aman Mani G
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India
aman.19cs057@cambridge.edu.in

Abstract— **Nowadays clouds have become a very common plot form in the internet world. Cloud computing provides many services in that storage as service is one. When you are storing our data in a public cloud, securing our data becomes a big challenge. Our data will be stored in remote cloud servers. We can access our cloud remotely. In this case we have obeyed the provider licence agreements. We need to trust providers blindly. So it is very important to secure our data with encryption. We are implementing a secure cloud storage system with AES,Triple DES and Blowfish algorithms by applying the fragmentation. The secret agencies can use our systems to share the information.In our project we have the modules named Administrator, Data owner, Data User and Cloud server. The administrator will manage the data owner accounts, data user accounts, file access permissions. The administrator can monitor uploads and downloads. The data owner will upload the files into the system. We are applying double encryption on the file. The generated cipher text is going to be divided into seven fragments. These fragments will upload into the firebase cloud. The user can download the files by requesting the file key. The user will receive the key through email after a request processed by the data owner. If the key is valid the file will download. while downloading the seven fragments will combine as a single fragment and double description will apply on the file. The plain text will download as a text file. The cloud can track the upload and downloads, the cloud can view data owners and data users details.**

I. INTRODUCTION

The data owner and data user will register from our application. We are not giving access to the anonymous persons, the administrator needs to verify the data owner and data user. After verification the data owner and data user can login into the system. The Data owner will upload the files into the cloud, the data user will download the files from the cloud. We are using Firebase's real time database as our cloud. The data owner will upload the files into the cloud server. After that if the file size is small, second encryption will apply with Blowfish encryption technique, if the file size is big Triple DES encryption will apply. The double encrypted file will split into seven equal fragments. The seven fragments will store in the firebase.
.

While uploading the text file, the file will be encrypted with AES encryption technique. After that if the file size is small, second encryption will apply with Blowfish encryption technique, if the file size is big Triple DES encryption will apply. The double encrypted file will split into seven equal fragments. The seven fragments will store in the firebase realtime database cloud. The encryption keys will be stored in our local database which we are using as MySql. We are storing the encrypted data in the cloud. We are not storing the file keys in the cloud. The data owner can view the uploaded file. The data user will download the file from the cloud, for this the data user should get the permission to view the files list which are available in the cloud. The data user will send the file access request to the administrator. If the administrator accepts the request, the data user can view the files available in the cloud. If a data user wants to download the file, the data user needs to send the request to the data owner. While the data owner accepts the request the key will generate and will send to the data user email address.

The generated key will work only for the particular user and particular file. We are not sharing the data encryption keys. While downloading the file the data user will provide the key that was received by the email. If the provided key is correct then the fragmented file will download from the firebase. The seven fragments will combine as a single fragment. Now the decrypting will apply to the file it will decrypt with either Triple DES or Blowfish. after the file will decrypt with AES algorithms. The plan text will download as a text file. The user can view the original file. The algorithm keys will fetch automatically from the database. The administrator, data owner and cloud person can view the uploads and downloads, the data user can view the downloaded file by them. When you are storing our data in a public cloud, securing our data becomes a big challenge. Our data will be stored in remote cloud servers. We can access our cloud remotely. In this case we have obeyed the provider licence agreements. We need to trust providers blindly.Triple DES or Blowfish .after the file will decrypt with AES algorithms. The plan text will download as a text file. The user can view the original file. The algorithm keys will fetch automatically from the database. The administrator, data owner and cloud person can view the uploads and downloads,the data user can view the downloaded file by them

II. RELATED WORK

Now ways the internet users utilizing cloud service in many ways. The cloud will not available at the customer end physically. The customer can access the cloud vertically. The customers not even knows where the data storing and how the data storing. In this case we need to trust the service providers. It's very challenging issue. Particularly for the secrets agencies. The information is everything, sharing the information securely is a challenging issue. When we use secure socket layer (SSL). The information over the internet is encrypted, information will transfer securely from client to server and server to client. But the original data will store in the cloud database. For this we need to encrypt the data while uploading into the cloud. There many cryptography techniques available to encrypt the data. Still in case of keys stolen the information can decrypt.

III. SYSTEM ARCHITECTURE
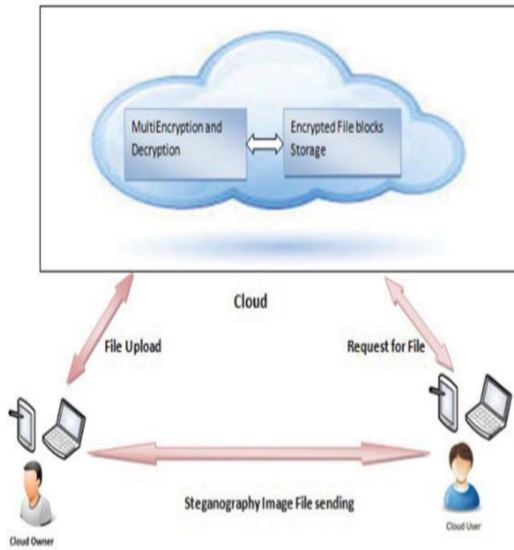
The system consists of four modules

Fig.1 Architecture of File Transfer between Owner and User
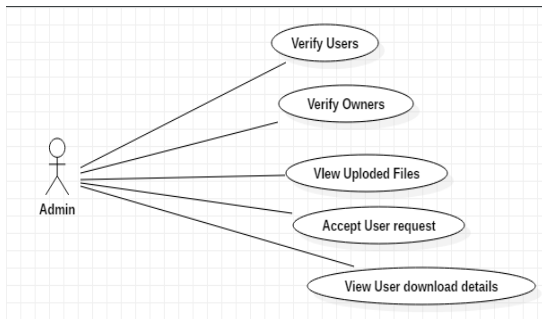
1. Administrator

Fig.2 Use case diagram of Administrator

The administrator can login with default credentials, the entered username and password is correct then only admin enter into the home page, if entered details are incorrect admin can't login to home page, after entered into the home page admin act like owner of this application and admin activate and deactivate the user and owner. The admin can view all upload file details and download file details accessing permissions.
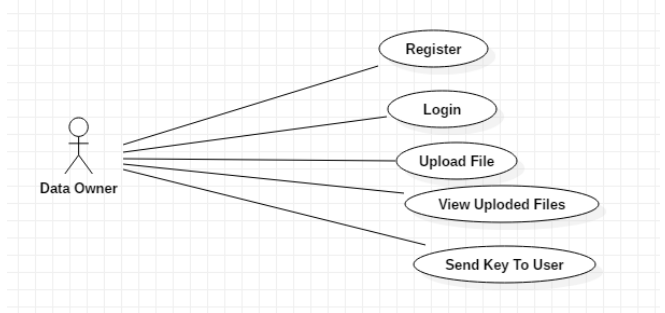
2. Data Owner

Fig.3 Use case diagram of Data owner

The data owner will register from our application. We are not giving access to the anonymous persons, the administrator needs to verify the data owner. After verification the data owner can login into the system. The Data owner will upload the files into the cloud, We are using Firebase real time database as our cloud. The data owner will upload the files into the cloud server.
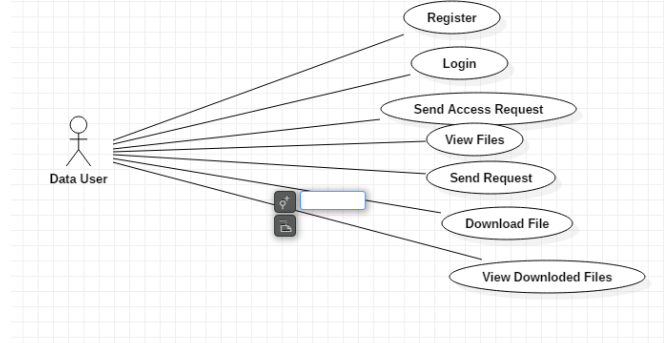
3. Data User

Fig.4 Use case diagram of Data User

The data user will register from our application, the administrator needs to verify the data user. After verification the data user can login into the system. The Data user will download the files from the cloud. The data user will download the file from the cloud, for this the data user should get the permission to view the files list which are available in the cloud. The data user will send the file access request to the administrator.
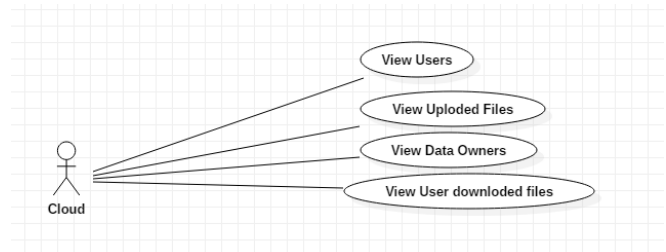
4. Cloud Person

Fig.5 Use case diagram of Cloud Person

Cloud module can operate by the admin in cloud module having all the registered users and owners details and owner uploaded file details and user downloaded details. The cloud person can monitor the cloud activities. The data user will download the file from the cloud, for this the data user should get the permission to view the files list which are available in the cloud. The data user will send the file access request to the administrator

IV. METHODOLOGIES

The data owner will upload the files into the cloud server. While uploading the text file, the file will be encrypted with AES encryption technique. After that if the file size is small, second encryption will apply with Blowfish encryption technique, if the file size is big Triple DES encryption will apply. The double encrypted file will split into seven equal fragments.

The seven fragments will store in the firebase realtime database cloud. The encryption keys will be stored in our local database which we are using as MySql. We are storing the encrypted data in the cloud. We are not storing the file keys in the cloud. The data owner can view the uploaded file.

The data owner will upload the files into the cloud server. While uploading the text file, the file will be encrypted with AES encryption technique. After that if the file size is small, second encryption will apply with Blowfish encryption technique, if the file size is big Triple DES encryption will apply. The double encrypted file will split into seven equal fragments. The seven fragments will store in the firebase realtime database cloud. The encryption keys will be stored in our local database which we are using as MySql. We are storing the encrypted data in the cloud. We are not storing the file keys in the cloud. The data owner can view the uploaded file. The data user will download the file from the cloud, for this the data user should get the permission to view the files list which are available in the cloud. The data user will send the file access request to the administrator. If the administrator accepts the request, the data user can view the files available in the cloud. If a data user wants to download the file, the data user needs to send the request to the data owner. While the data owner accepts the request the key will generate and will send to the data user email address.

The generated key will work only for the particular user and particular file. We are not sharing the data encryption keys. While downloading the file the data user will provide the key that was received by the email. If the provided key is correct then the fragmented file will download from the firebase.

The seven fragments will combine as a single fragment. Now the decrypting will apply to the file it will decrypt with either Triple DES or Blowfish.after the file will decrypt with AES algorithms. The plan text will download as a text file. The user can view the original file. The algorithm keys will fetch automatically from the database.

V. CONCLUSIONS

Our security model proved that we can provide hybrid security while storing the data in the public cloud. With this, irrespective of the cloud policies we can maintain security from our end. We can completely stop the hacking with conditional based double encryption. The key which we are providing for data users will work only for the particular user and particular file. We are not sharing original keys to the users and we are not storing the keys in the cloud. We are storing the file keys in our local database which we are using as mysql. So there is no chance of keys being stolen. our system will be suitable for a secret agency to share the information with the users. our system is suitable where the security matters.

VI. FUTURE SCOPE

The key which we are providing for data users will work only for the particular user and particular file. We are not sharing original keys to the users and we are not storing the keys in the cloud. We are storing the file keys in our local database which we are using as mysql. So there is no chance of keys being stolen. our system will be suitable for a secret agency to share the information with the users.our system is suitable where the security matters.

VII. REFERENCES

[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 to Enhance 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:'Survey Paper on Cloud Storage Security'.

[5] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).