SECURE DATA TRANSFER USING CRYPTOGRAPHY

Shilpa v
Assistant Professor
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

Anushree Krishnamurthy
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

Bindu S
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

Balaji Reddy D
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

Aman Mani G
Student
Department of Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

***Abstract*— Nowadays clouds have become a very common plot form in the internet world. Cloud computing provides many services in that storage as a service is one. When you are storing your data in a public cloud, securing your 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 license agreements. We needto trust providers blindly. So it is very important to secure our data with encryption. We are implementing a secure cloud storage systemwith AES, Triple DES, and Blowfish algorithms by applying fragmentation. Secret agencies can use our systems to share information. In our project, we have modules named Administrator, Data Owner, Data User, and Cloud Server. The administrator will manage the data owner accounts, data user accounts, and file access permissions. The administrator can monitoruploads and downloads. The data owner will upload the files into thesystem. We are applying double encryption on the file. The generatedcipher text is going to be divided into seven fragments. These fragments will upload into the Firebase cloud. The user can downloadthe files by requesting the file key. The user will receive the key through email after a request is processed by the data owner.**

***Key Words*: Encryption, AES Algorithm, DES Algorithm, Blowfish Algorithm, Cloud.**

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 log in to 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 to the cloud server. After that, if the file size is small, the second encryption will apply with the 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 the AES encryption technique. After that, if the file size is small, the second encryption will apply with the 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 real-time 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 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's 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 plain 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 your data in a public cloud, securing yourdata becomes a big challenge. Our data will be stored in remote cloud servers. We can access our cloud remotely. In this case, we have obeyedthe provider license agreements. We need to trust providers blindly. Triple DES or Blowfish .after the file will decrypt with AES algorithms. The plain 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 internet users utilize cloud services in many ways. Thecloud will not be available at the customer end physically. The customercan access the cloud vertically. The customers do not even know wherethe data storing and how the data storing. In this case, we need to trustthe service providers. It's a very challenging issue. Particularly for the secret agencies. Information is everything, and sharing information securely is a challenging issue. When we use a secure socket layer (SSL). The information over the internet is encrypted, and 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 it into the cloud. There are 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

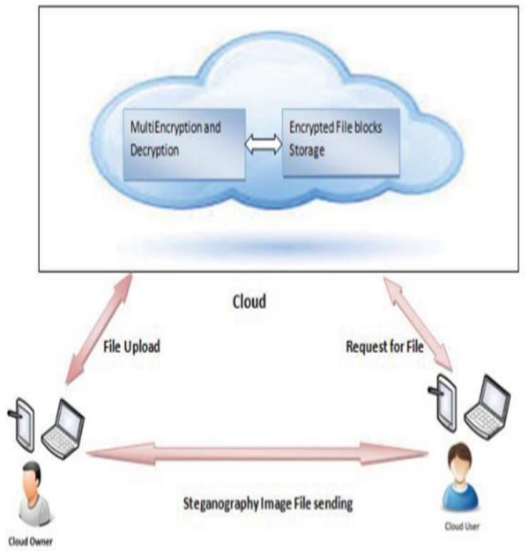

Fig.1 Architecture of File Transfer between Owner and User

1. Administrator

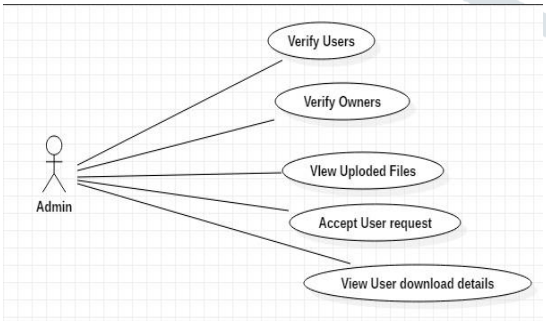

Fig.2 Use case diagram of Administrator

The administrator can log in with default credentials, the entered username and password is correct then only the admin enter the home page, if entered details are incorrect admin can't log in to the home page, after entering 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 uploaded file details and download file details by accessing the permit

2. Data Owner

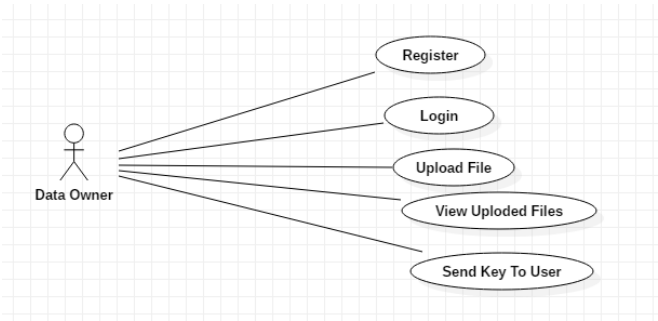

Fig.3 Use case diagram of Data owner

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 log in to 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 to the cloud server.

3. Data User

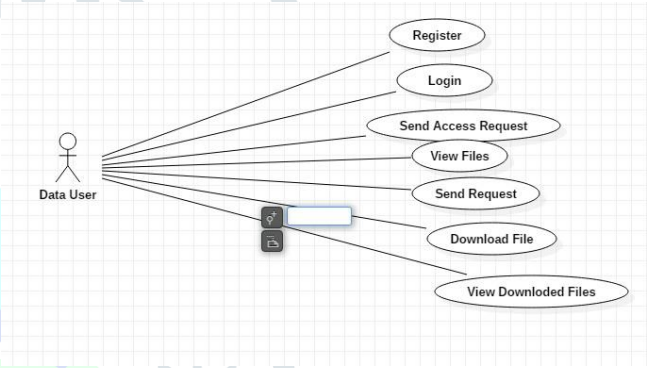

Fig.4 Use case diagram of Data User

The data user will register from our application, the administrator needs to verify the data user. After verification, the data user can log in to 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 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

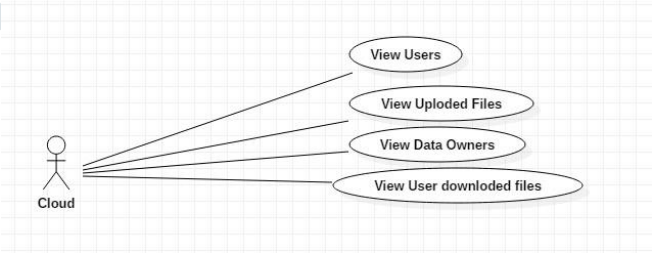

Fig.5 Use case diagram of Cloud Person

The cloud module can operate by the admin in the cloud module having all theregistered users and owners' details and owner uploaded file details anduser-downloaded details. The cloud person can monitor the cloudactivities. The data user will download the file from the cloud, for this the data user should get 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 to the cloud server. While uploading the text file, the file will be encrypted with the AES encryption technique. After that, if the file size is small, the second encryption will apply with the Blowfish encryption technique, if thefile 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 real-time 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 to the cloud server. While uploading the text file, the file will be encrypted with the AES encryption technique. After that, if the file size is small, the second encryption will apply with the 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 willstore in the Firebase real-time 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 thedata user should get permission to view the files list which are available in the cloud. The data user will send the file access requestto 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 keywill generate and will send to the data user's 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 plain 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 the original keys with 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 information with the users. our system is suitable where 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 the original keys with 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 information with the users. our system is suitable where 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 Encryptionand 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).