Protection of Personal Data on Distributed Cloud using Biometrics

Gangamma B N[1], Sindhura H R[2], Shubha K Shetti[3], Kusuma B R[4], Mrs.Jayasri B S[5]

[1,2,3,4]Student, CSE/The National Institute of Engineering, Mysuru, Karnataka, India
[5]Associate Professor, CSE/The National Institute of Engineering, Mysuru, Karnataka, India

---***---

Abstract - *The proposed system aims at providing a secure and efficient solution to end users to access their own personal files in the cloud servers using biometric authentication. Biometric fingerprint scanner is used for the processing of finger print based authentication. The user's own personal files are stored in the free public multiple cloud storages namely AWS and Google drive using two techniques called splitting and merging techniques. Rijndael algorithm will improve the security in cloud environment. Files or details are stored in multiple clouds using cryptographic techniques. Data gets split into fragments and gets stored in various distinct cloud servers with encrypted key. At once the authorized token for the specific is requested by the user, the cloud server performs a keyword based on the search's encrypted data and combines the fragments, this is sent to the verifier for the verification.*

***Key Words*: Cloud Computing, Fingerprint, Rijndael algorithm, AWS, Google drive.**

1. INTRODUCTION

In daily life, though Cloud computing plays an important role however it invokes various security threats such as Phishing, Session Hijacking, Malicious software and wire-less connection vulnerabilities[1]. In this project, secured architecture for storing end user's necessary data like Birth certificate, Death certificate, Academic certificate, Transfer certificate, Passport and other personal and important details in Cloud. The proposed architecture focuses on Finger print based user authentication onto access the detail in the cloud computing. For each and every individual a special or unique signature/pattern are obtained. The proposed architecture involves multiple cloud storage. The feature extraction and matching is performed using required algorithm for the finger print. Presently Finger print sensor has been integrated in all Laptops, personal computers and mobile devices, so it can use the in-built sensor or integrating an external user finger print sensor can authenticate, store/ download the respective data. The document is split into the fragments and stored in the AWS and Google Drive. Using encryption algorithm, the fragments are encrypted and stored in the cloud servers.

1.1 Existing System

Cloud computing refers to the practice of using the network of remote servers hosted on internet to store, manage and process data rather than a local server or personal computer. There is increasing demand for usage of cloud. The user can store his personal documents in cloud and perform various types of computations on it. However, the security issues related to the data stored in cloud poses a threat. In the existing system, the user stores his documents in a single cloud. Therefore, when a hacker gets access to this cloud by some means then he can get all the information stored [2].

Drawbacks in the existing system-

1) Safety of the data is compromised. Since the data is not encrypted the hacker can easily get the information.

2) Single cloud storage poses a threat. Since the user stores all the information on single cloud if the security of the cloud is not good enough then the cloud can be hacked to get the information[1].

2. PROPOSED SYSTEM

This system is proposed to provide a security and efficient solution to end users to access their own personal files in the cloud servers using biometric authentication. Required algorithm is implemented for the processing of finger print based authentication. The user's personal files are stored in the free public multiple cloud storages and the algorithm will improve the security in cloud environment.
Advantages of the proposed system-

1) Safety of the data is enhanced. Since the data is encrypted using encrypting keys, though it is hacked the hacker cannot access the data hacked.

2) This project gives a special solution invoking security in single/multiple cloud storages. It is secured and requires less processing time for the Rijndael encryption algorithm when compared with other algorithms.

3) Our proposed architecture also involves multiple cloud storage system, the user files get converted into fragments, split and stored data in cloud storages[2].

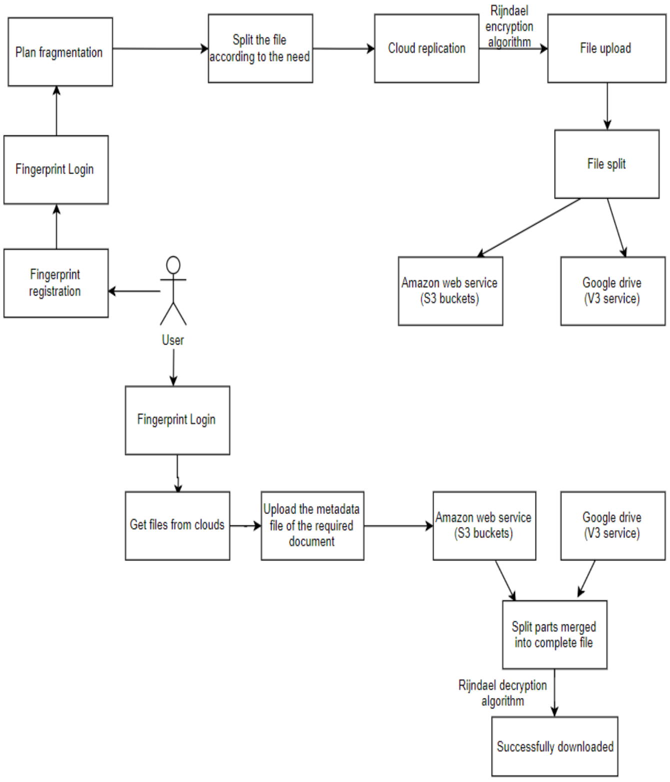
Plan fragmentation
Split the file according to the need
Cloud replication
Rijndael encryption algorithm
File upload
Fingerprint Login
File split
Fingerprint registration
Amazon web service (S3 buckets)
Google drive (V3 service)
User
Fingerprint Login
Get files from clouds
Upload the metadata file of the required document
Amazon web service (S3 buckets)
Google drive (V3 service)
Split parts merged into complete file
Rijndael decryption algorithm
Successfully downloaded

Fig -1: Architecture

The system architecture as shown in the fig 1 provides a secure and efficient solution to end users to store and access their own personal files in the cloud servers using biometric authentication. Required algorithm is implemented for the processing of finger print based authentication. The user's own personal files are stored in the public multiple cloud storages (AWS and Google drive). The user can decide the number of parts to be made as well as the size of each of the part. Once the splitting process is done he can upload the parts onto the clouds. These parts are first encrypted using Rijndael algorithm and the encrypted parts are uploaded onto clouds. The key used for encryption is stored in an XML file in user's local folder. The parts are stored in alternative manner in AWS S3 buckets[5] and Google drive[6]. When the user wants to download the file, he has to first upload the XML file that contains the key, Based on this, the parts are obtained from AWS and Google drive and decrypted using Rijndael algorithm. The parts are merged and the entire file gets downloaded.

2.1 Implementation

Registration and Login Module

Registration and Login module are provided for the user access to the system. The user who is accessing the system for the first time will be asked to register himself to the system, by providing his basic information like his name, contact number, email id, address etc., along with this he will be asked to register his fingerprint. If the details are valid the registration is successful. For the subsequent access to the system the user can directly login to the system by verifying his fingerprint and entering his password. After successful verification, the user will be directed to the homepage where the user can split the document, upload the document, and download the document.

Fragmentation Module

This module enables the user to plan the fragmentation for the data to be stored on the multiple clouds. The user can split the documents according to his needs. Each file can be split into multiple parts with each part having different size[3]. The size of each fragment is decided by the user. The number of pieces to be made is also left to choice of user. The total size and remaining size after forming each piece is displayed for user reference. The fragmented parts are stored along with a merger file. This merger file contains the number of bytes in each of the parts along with the start and end bytes. This is helpful for the merging process in download module.

Upload File Module

This module helps the user to upload the fragmented files to multiple clouds. To each of the fragment generated an encryption algorithm named Rijndael[4] is applied. Once the encryption algorithm is applied a metadata file is created containing the secret key. This metadata file will be stored in the local server thus preventing it from being corrupted or hacked. Finally the files can be uploaded onto AWS and Google Drive.

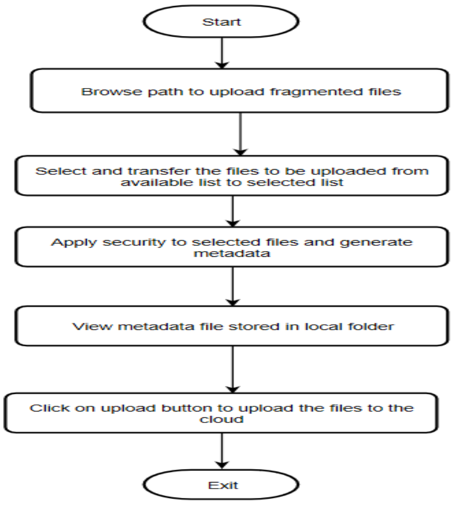
Start
Browse path to upload fragmented files
Select and transfer the files to be uploaded from available list to selected list
Apply security to selected files and generate metadata
View metadata file stored in local folder
Click on upload button to upload the files to the cloud
Exit

Fig -2: File Upload

Download File Module

Finally to download the file stored in multiple clouds, the user has to upload the metadata file that contains the encryption key. The rijndael decryption algorithm decrypts the parts into original format using the merger file generated in fragmentation module. All the individual parts get merged to a complete file and gets downloaded[3].

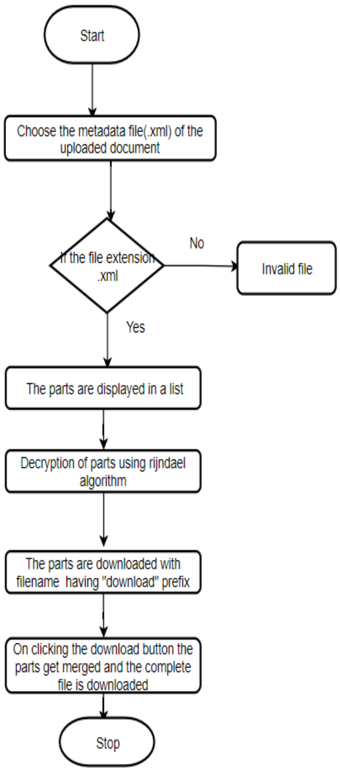
Start
Choose the metadata file(.xml) of the uploaded document
f the file extension .xml
No
Invalid file
Yes
The parts are displayed in a list
Decryption of parts using rijndael algorithm
The parts are downloaded with filename having "download" prefix
On clicking the download button the parts get merged and the complete file is downloaded
Stop

Fig -3: File Download

3. CONCLUSION

This system gives a special solution invoking security in single/multiple cloud storages. Our proposed architecture involves multiple cloud storage system, the user files are split into fragments, encrypted using Rijndael encryption algorithm and stored data in two cloud storages namely AWS and Google drive. The study results shows Rijndael algorithm as secured and requires less processing time. This system deals with the enhancement of security to cloud servers by implementation detection and prevention techniques against cyber attacks. Safety of the data is enhanced in this system. Hence this architecture provides complete secure access/storage of data across multiple clouds. In future, we can add more number of clouds and also keep a backup copy of each of the parts. Also it can be improvised by integrating other biometric authentication.

REFERENCES

[1] Hubbard D, Sutton M.Top treats to Cloud Computing V 1.0 : http://www.cloudsecurityalliance.org/topthreats

[2] Bohli J M,Jensen M.Security and Privacy-Enhancing Multicloud Architectures.2013 August:10(4):212-224.

[3] A.N.Vinodhini, Dr.S.Ayyasamy. Prevention of Personal Data in Cloud Computing Using Bio-Metric. IEEE International Conference on Innovations in Green Energy and Healthcare Technologies(ICIGEHT'17).

[4] How does the encryption algorithm Rijndael work? https://www.password-depot.de/en/knowhow/blowfish_and_rijndael.htm

[5]Amazon Web Services-http://www.wikipedia.com/aws.

[6] Google Drive-https://www.cloudwards.net/how-does-google-drive-work/.