ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

[1] R.Gokula Priya , [2] Unnimaya P Madhu, [3] M.Yuvashree, [4] M.Karthikeyan
[1][2][3] Final Year Student, [4] Assistant Professor
[1][2][3][4]Department of Cse, Sengunthar College of Engineering, Tiruchengode

Abstract – **With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.**

1. INTRODUCTION

Cloud computing means storing data and accessing that data from the Internet instead of Using Traditional hardware for most of the operations. More than 50% of IT companies have moved their Business to the cloud. Sharing of data over the cloud is the new trend that is being set on. The amount of data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity.

Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data. [1] Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Therefore, privacy of the personal sensitive data is a big concern for many data owners.

When any of the people upload the data onto the cloud they are leaving their data in a place where monitoring over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data over the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome.

Therefore, to solve this problem data should be encrypted before uploading it onto the cloud which can be safe from everyone. Now the data encryption part brings some new problems such as we have to provide an efficient encryption algorithm such that if the data Is in encrypted format it cannot be easily to get break or get accessed by any exploiters.

The next big concern is time consumption for encryption. Traditional Hardware with big configuration can encrypt data in short amount of time but limited resource devices suffer from this problem. They require more amount of time of encryption and decryption. So, an efficient crypto system is to be proposed which can worked equally or heterogeneously on all of the devices.

II RELATED WORK

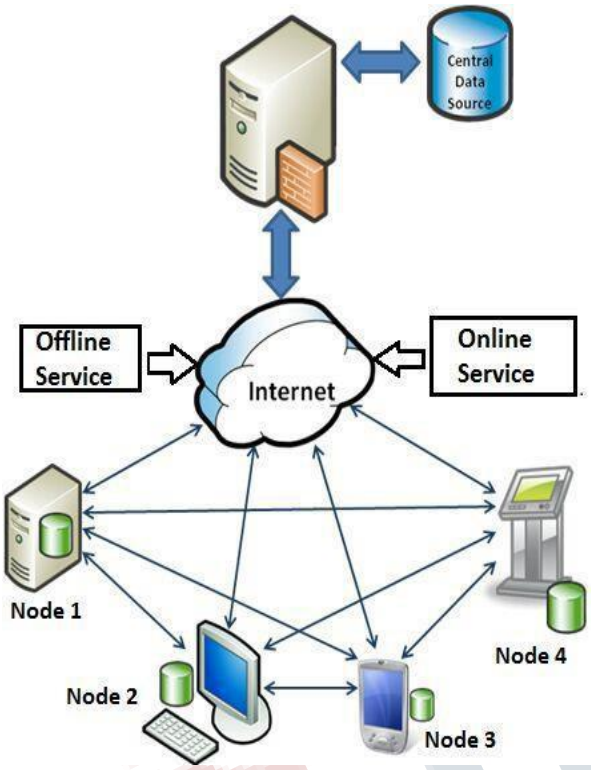
Attribute-based encryption (ABE) is proposed by Sahai and Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes.

In an ABE, a person's keys and cipher-texts are labeled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person's key. It reduces the quantity of key used and hence makes encryption and decryption technique faster

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

III ARCHITECTURE AND MODULES DETAILS



The architecture of the proposed system is shown in the figure which shows the users and the operations involved. The detailed description of the architecture is explained as follows:

Nodes: The User is responsible for uploading and sharing its personal data on the cloud.

On-line and Off-line Services: In On-line Service data will encrypted and directly transfer to the respective user. In Off-line Service if there is no Internet Connection the data will get encrypted first and then it will get stored in Main Server. Until the system does not comes on-line the data will not be shared over the cloud

Cloud Service Provider: Cloud service provider is responsible for providing all the required services to its users according to their demands.

Encryption and Decryption: Here we are using the combination of ABE and BRE algorithm to encrypt and decrypt the files.

File Upload and Download: The files which are uploaded on cloud are encrypted form.

IV EXISTING SYSTEM:

With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

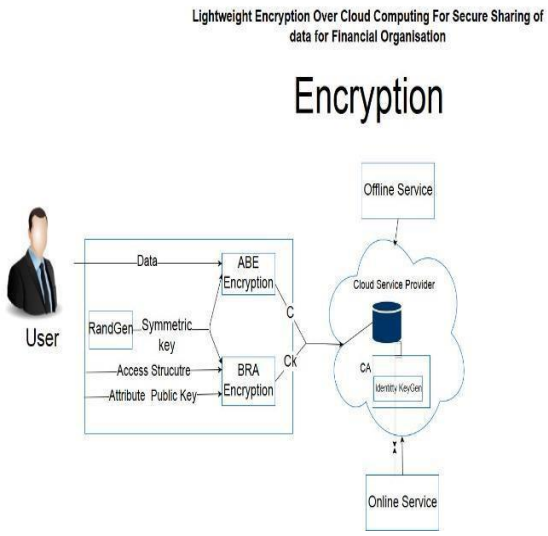
the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

V PROPOSED SYSTEM:

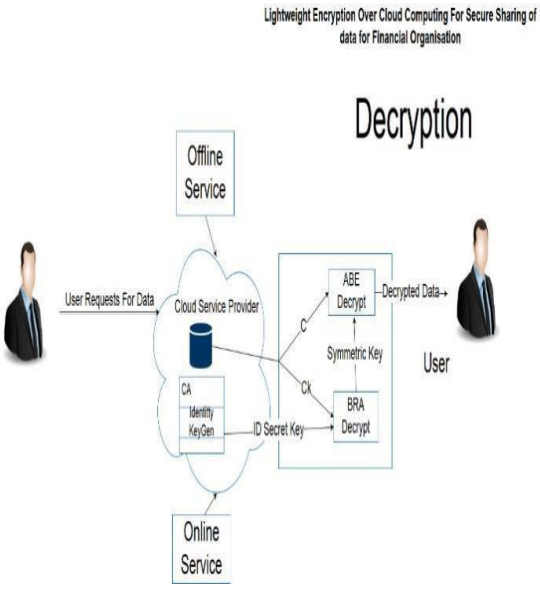
Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems. How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owner's effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over cipher text. In these researches, they have the following common assumptions. First, the CSP is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment.

ISSN (Online) 2394-2320

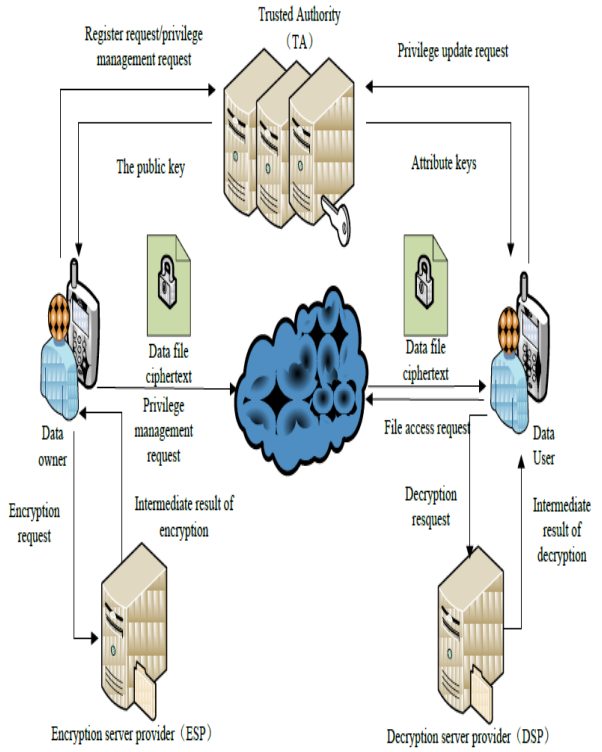
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018



(OTP) which will be matched with key In our proposed system data is encrypted before uploading to the cloud. Combination of Attribute Based Encryption and Byte Rotation Algorithm are used for the encryption of the data. ABE will help to identify the attributes of the data and BREA will perform matrix operations on the block of the data to be encrypted. After performing encryption operation, a random key is generated alongside the encrypted data. Data will be send in encrypted format to respective user. To decrypt this data receiver has to enter the One Time Password generated using ABE algorithm.



ARCHITECTURE



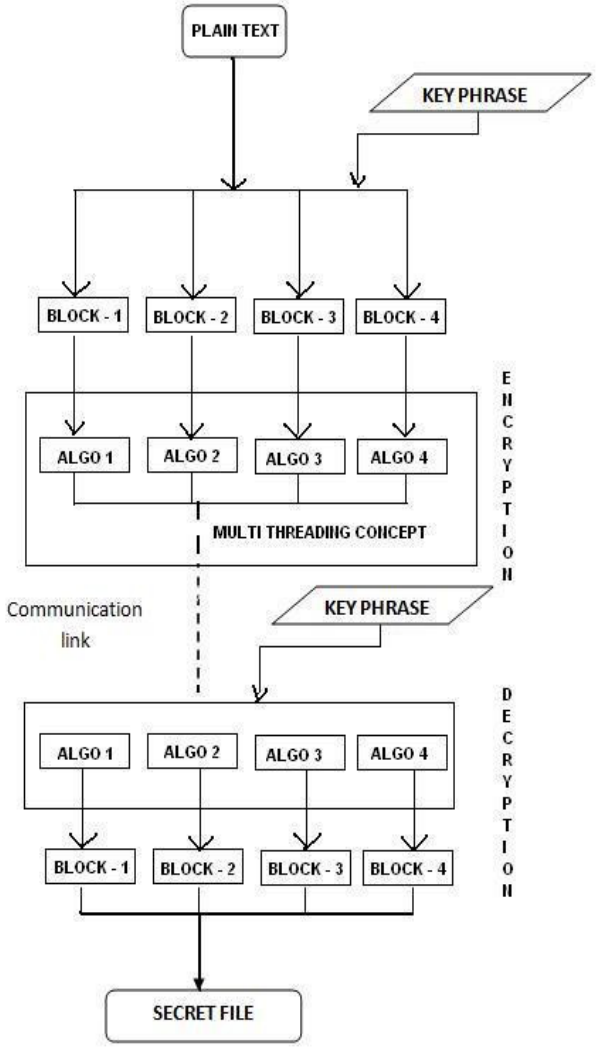
Proposed System Algorithm

Step-1: Start
Step-2: Accept the data from the user.
Step-3: The Attributes of the data from the users' formats are obtained by the Attribute-Based Encryption.
Step-4: With the help of these Attributes, Random Key is generated, and type of data is obtained for encryption by BRE algorithm.
Step-5: The data is converted into equal number of blocks and N x N matrix will be generated on the basis of these blocks.
Step-6: Based on no. of blocks, pool of threads will be created.
Step-7: Run the threads in multi core system to create encrypted data in short amount of time.
Step-8: A secret key is generated in order to open the encrypted file which is stored in the cloud.
Step-9: The secret key is shared to the user via email or mobile number of the authorized user. This key will be used to decrypt the encrypted file.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Step- 10: The file selected will be decrypted in the original form using the key. Step-11: Stop.



VI IMPLEMENTATION

This period of the venture is critical in light of the fact that at this stage the hypothetical plan is changed over into functional one. This stage is a basic stage since this stage require exceptionally exact arranging and need the learning of existing framework and its detriments. The execution stage ought to be created by considering every one of the prerequisites, imperatives. The new framework ought to be successful and work appropriately

VII ANDROID MODULES:

1. Text Encryption and Decryption
2. Image Encryption and decryption
3. Text request
4. Image request

SERVER SIDE:

5. View encrypted data
6. View user request
7. Provide password

1.Text Encryption and Decryption

In this module user encrypted the plain text to encrypted format and uploaded to the cloud. The encryption is done by using a password. Only using this password only any one can decrypt the text. The user upload the password also include with encrypted data. The trusted authority id responsible for passing the password to the requested user

2.Image Encryption and decryption

Like the same as the image encryption is also done. And the encrypted images and password will also be uploaded to the cloud. The trusted authority id responsible for passing the password to the requested user

3.Text request

Any user can view the file uploaded in the server. All the files are in encrypted format. User cant view the files without know the password. For view the file first user need to request the password to Trusted Authority The Authority check the user and provide the password for valid user.

4.Image request

Image request is also same as the Text Request. The list of images can view in the application. But user can only view the images after getting the password from trusted authority

5.View Encrypted Data

The user uploaded encrypted data can be view in the server side. The trusted authority act as server they have the responsibility to provide password for the requested user.

6.View user request

After user view the encrypted data they can request the password for encrypted data. This user request can be view in the Trusted authority

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

7. Provide password

After view the request Trusted authority validating the user and if the user is valid the Trusted authority provide password for the requested file via email. Using this password user can decrypt the file

VIII CONCLUSION:

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do cipher text retrieval over existing data sharing schemes.

IX REFERENCES

[1] "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing "Ruixuan Li, Member,IEEE, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, Member, IEEE

[2] "Towards Se-cure Data Sharing in Cloud Computing Using Attribute Based Proxy Re-Encryption with Keyword Search" Hanshu Hong; Zhixin Sun

[3] X. Liang, Z. Cao, H. Lin, and 1. Shao, "Attribute based proxy re-encryption with delegating capabilities," in Proc. 4th ACM Int. Symp.

[4] Priya Dudhale Pise, Dr. Nilesh J Uke,"Efficient Security Protocol for Sensitive Data Sharing on Cloud Platforms" in 2017 IEEE.

[5] K. Liang et aI., "A OFA -based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security,vol. 9, no. 10, pp. 1667-1680, Oct. 2014.

[6] H. Hong, Z. Sun. "An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing", JoCCASA, 5(2).pp.I -8,201 6.

[7] J. Liu, X. Huang, and 1. K. Liu, "Secure sharing of personal health records in cloud computing: Cipher text-policy attribute-based signcryption," Future Gene rat. Com put. Syst., vol. 52, pp. 67-76, Nov. 2015.