International Journal on Applications in Engineering and Technology
Volume 4: Issue 1: March 2018, pp 40 - 42. www.aetsjournal.com ISSN (Online) : 2455 - 0523

SURVEY ON A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

E.KAYALVIZHI , R.VETRIVENTHAN, SENTHIL KUMARAN

Abstract— Cloud has been around for two decades and it consists of the vast amount of data from all over the world. Most of the people at a personal level and organization level have moved their data to the cloud and share data across all around the world. The main challenge faced by everyone is to share the data all over the world or at organizational level securely without giving away the important data to any exploiters. To overcome the challenge to share the data securely over the cloud, an efficient data encryption algorithm for encrypting data before sending it to the cloud. In this proposed we are using a combination of Attribute-Based Encryption and Byte Rotation Encryption Algorithm for encrypting the data before sending it to the cloud. This will help the user to securely store and share the data in encrypted form.

Keywords— Cloud Computing, Data Privacy, Encryption, Data Security, Data Sharing, Access Control.

I. 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.

E.Kayalvizhi , Master of Computer Applications , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

R.Vetriventhan , BE , MTech , MISTE , Head of the department , Department of MCA , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

Dr.Senthil Kumaran , ME Phd , Managing Director , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu.

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 suffers 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.

III. PROPOSED SYSTEM

To address privacy issue in existing system we propose a crypto-system for secure sharing of data over the cloud, which uses combination Attribute Based Encryption and Byte Rotation Encryption Algorithm for secure encryption of the data over cloud.

The main three works are as follows:

1. Identify the issues in cloud system for data storage on cloud. Since data is not secure on cloud user can upload the data in encrypted format.
2. Propose a crypto-system which can run on all limited resources devices. It can take data from the user and provide off-line-online service.

Apply Attribute Based Encryption Algorithm and Byte Rotation Algorithm for encryption of data to securely transfer

the data between the users.

1) ADVANTAGES

- Here data can be transferred from one user to another securely over the cloud.
- The system cost will be decreased.
- It will work on all limited resource devices.

2) ARCHITECTURE AND MODULES DETAILS

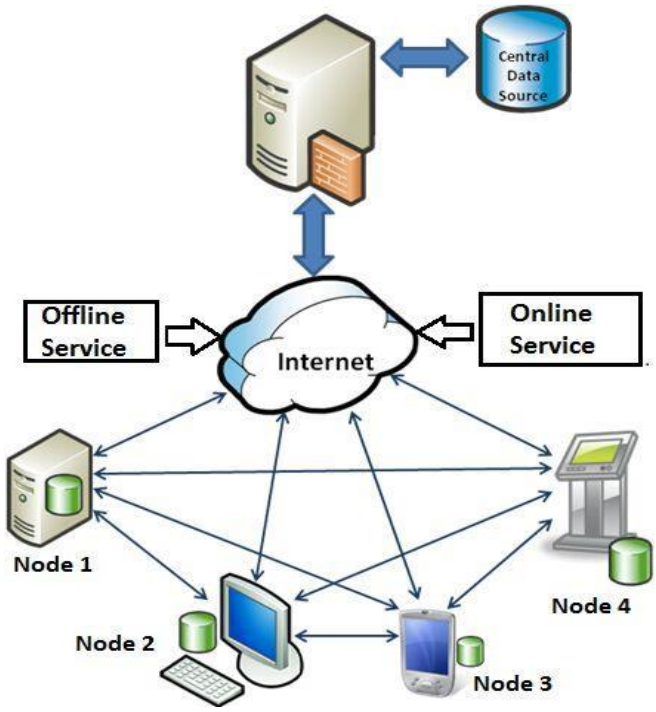

Figure 1: System model

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:

1. **Nodes**:
   The User is responsible for uploading and sharing its personal data on the cloud.
2. **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
3. **Cloud Service Provider**:
   Cloud service provider is responsible for providing all the required services to its users according to their demands.
4. **Encryption and Decryption**:
   Here we are using the combination of ABE and BRE algorithm to encrypt and decrypt the files.
5. **File Upload and Download**:
   The file which are uploaded on cloud are encrypted form. Users can download the file which are decrypted if he is authorized.

IV. PROPOSED SYSTEM ENCRYPTION ALGORITHM

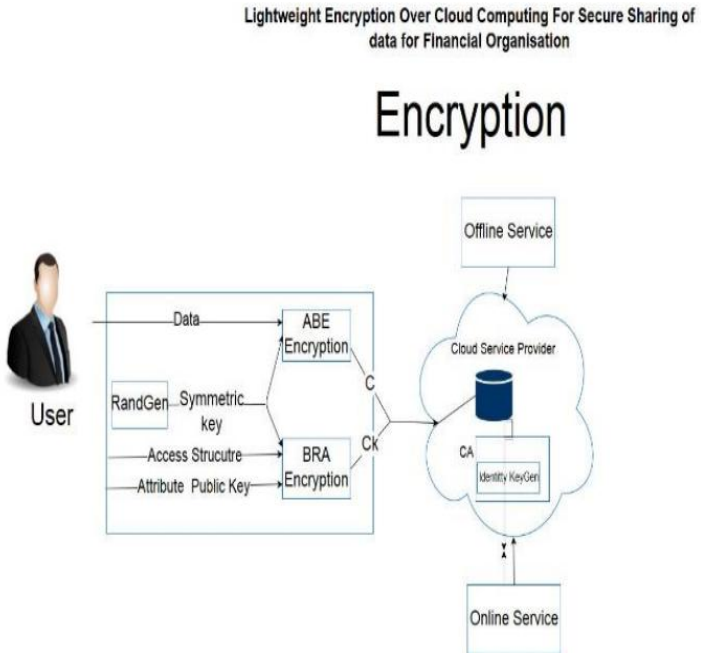

Figure 2: Encryption Diagram

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 (OTP) which will be matched with key generated using ABE algorithm.

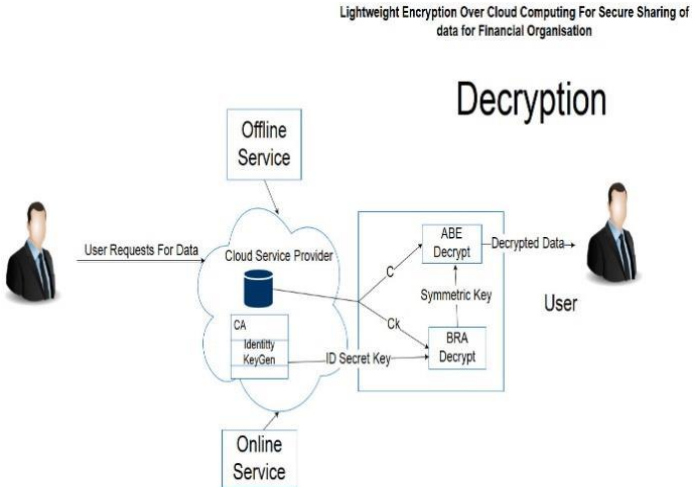

Figure 3: Decryption Diagram

1) 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 authorised user. This key will be used to decrypt the encrypted file.
Step-10 : The file selected will be decrypted in the original form using the key.
Step-11 : Stop.

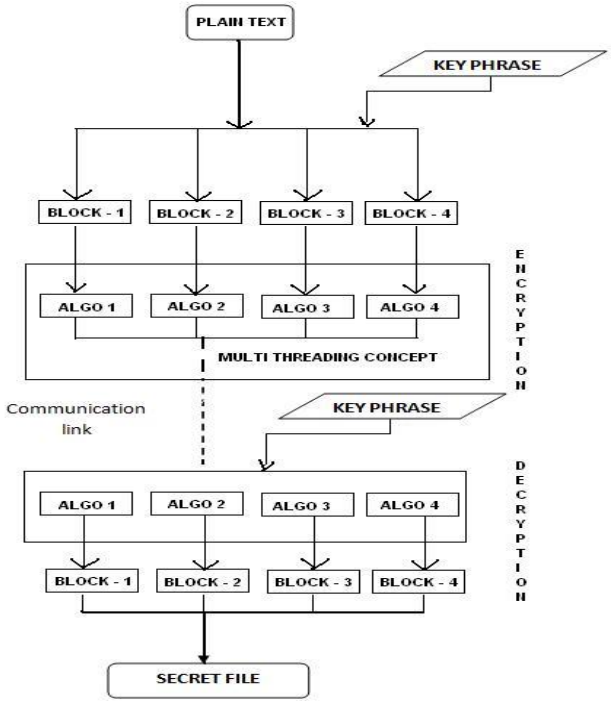

Figure 4: Flow Diagram

2) 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.

V. CONCLUSION

In this paper, the issue of sharing the data in cloud computing securely is resolved. Data privacy can be maintained by combination of ABE and BRE algorithm. Authentication is used to guarantee data privacy and data integrity. This indicates that the proposed system can be used to enhance privacy preservation in cloud services.

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 capa-bilities," 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 datasharing," 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: Ciphertext-policy attribute-based signcryption," Future Generat. Com put. Syst., vol. 52, pp. 67-76,Nov. 2015.