International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 01, January-2018

A LEIGHTWEIGHT SECURE INFORMATION SHARING PLAN FOR PORTABLE DISTRIBUTED COMPUTING

[1]VAITLA NARENDER, [2]Y APPARAO

[1]PG SCHOLAR, DEPT OF CSE, MARRI LAXMAN REDDY INSTITUTE OF TECHNOLOGY & MANAGEMENT, DUNDIGAL(V), QUTHBULLAPUR (MD), HYDERABAD-500043.

[2]ASSOCIATE PROFESSOR, DEPT OF CSE, MARRI LAXMAN REDDY INSTITUTE OF TECHNOLOGY & MANAGEMENT, DUNDIGAL(V), QUTHBULLAPUR (MD), HYDERABAD-500043.

ABSTRACT: Cloud has been around for two decades and it comprises of the tremendous measure of information from everywhere throughout the world. The vast majority of the general population at an individual level and association level has moved their information to the cloud and offer information over all around the globe. The primary test looked by everybody is to share the information everywhere throughout the world or at authoritative level safely without giving endlessly the critical information to any exploiters. To defeat the test to share the information safely finished the cloud, a productive information encryption calculation for encoding information before sending it to the cloud. In this proposed we are utilizing a blend of Attribute-Based Encryption and Byte Rotation Encryption Algorithm for encoding the information before sending it to the cloud.

KEY WORDS: Cloud Computing, Data Privacy, Encryption, Data Sharing.

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 information over is the following huge worry for a large portion of us. In the wake of transferring the information to the cloud utilizes loses its control over that information. [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. In this way, an effective crypto framework is to be proposed which can work similarly or heterogeneously on the majority of the gadgets.

2. 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.
Trait based encryption (ABE) is proposed by Sahai and Waters. Quality based encryption (ABE) is a reasonably late approach that re-assesses the possibility of open key cryptography.

3. PROPOSED SYSTEM

To address protection issue in existing framework we propose a crypto - framework for secure sharing of information over the cloud, which utilizes blend Attribute Based Encryption and Byte Rotation Encryption Algorithm for secure encryption of the information over cloud. The main three works are as follows:
Identify the issues in cloud framework for information stockpiling on cloud. Since information isn't secure on cloud client can transfer the information in encoded design.
Propose a crypto-framework which can keep running on every single constrained asset gadgets. It can take information from the client and give disconnected online administration.

3.1 ADVANTAGES

• Here information can be exchanged starting with one client then onto the next safely finished the cloud.
• The framework cost will be decreased.
• It will deal with all restricted asset devices

AND MODULES 3.2ARCHITECTURE DETAILS

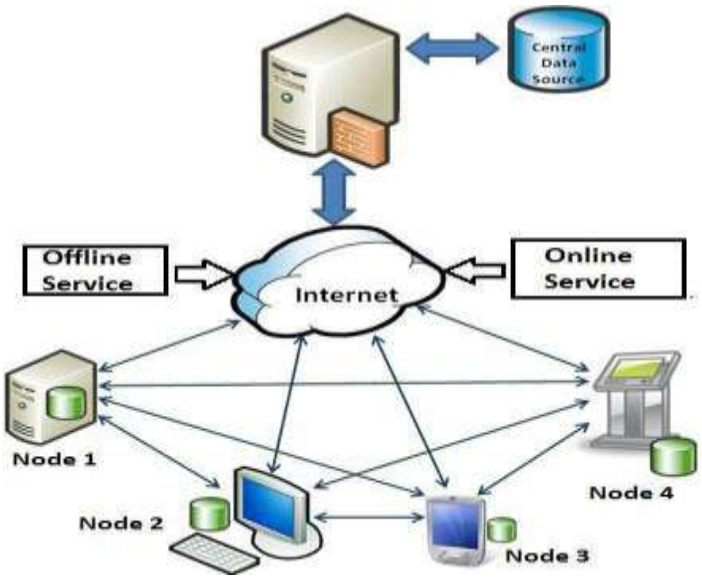

Figure 1: System model

The engineering of the proposed framework is appeared in the figure which demonstrates the clients and the operations included. The definite portrayal of the design is clarified as takes after:

On-line and Off-line Services: In On-line Service information will scrambled and specifically exchange to the particular client. In Off-line Service if there is no Internet Connection the information will get scrambled first and after that it will get put away in Main Server. Until the point that the framework does not goes ahead line the information will not be shared over the cloud.
Cloud Service Provider: is responsible for providing all the required services to its users according to their demands.
Encryption and Decryption: Here we are utilizing the mix of ABE and BRE calculation to encrypt and unscramble the files.
File Upload and Download: the files which are uploaded on cloud are encrypted form users.

4. PROPOSED SYSTEM

ENCRYPTION ALGORITHM

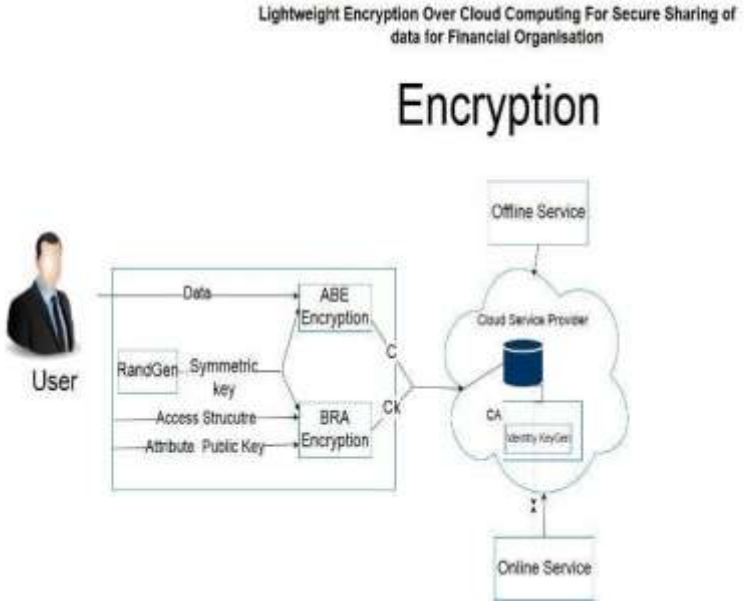

Figure 2: Encryption Diagram

In our proposed framework information is scrambled before transferring to the cloud. Blend of Attribute Based Encryption and Byte Rotation Algorithm are utilized for the encryption of the information. ABE will distinguish the properties of the information and BREA will perform network operations on the piece of the information to be scrambled. Subsequent to performing encryption operation, an arbitrary key is created nearby the encoded information. Information will be sending in scrambled arrangement to individual client. To decode this information recipient needs to enter the One Time Password (OTP) which will be coordinated with key created utilizing ABE calculation.

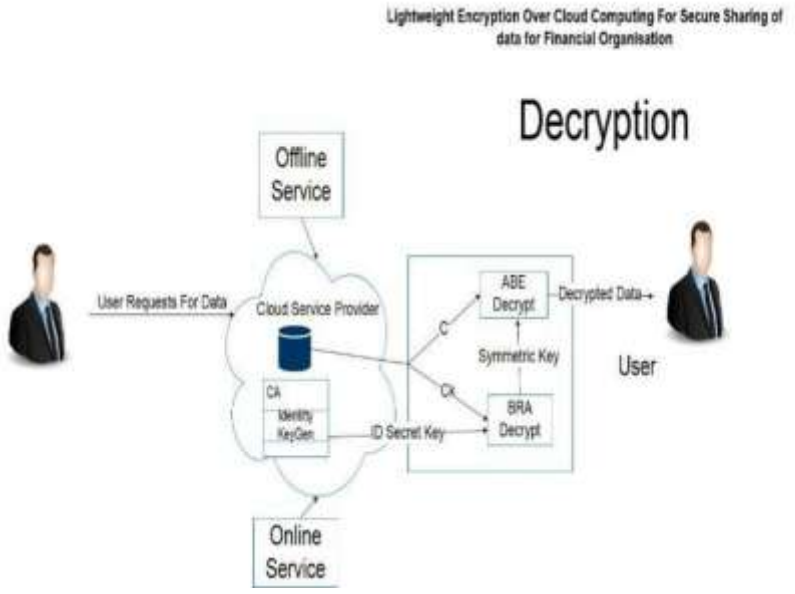

Figure 3: Decryption Diagram

4.1 PROPOSED SYSTEM ALGORITHM

Step-1: Start
Step-2: Accept the information from the client.
Step-3: The Attributes of the information from the clients' arrangements are acquired by the Attribute-Based Encryption.
Step-4: With the assistance of these Attributes, Random Key is produced, and kind of information is gotten for encryption by BRE calculation.
Step-5: The information is changed over into level with number of squares and N x N grid will be created based on these pieces.
Step-6: Based on no. of pieces, pool of strings will be made.
Step-7: Run the strings in multi center framework to make scrambled information in short measure of time.
Step-8: A mystery enters is created so as to open the encoded record which is put away in the cloud.
Step-9: The mystery key is shared to the client by means of email or portable number of the approved client. This key will be utilized to decode the encoded record.
Step-10: The record chose will be decoded in the first shape utilizing the key.
Step-11: Stop.

4.2. IMPLEMENTATION

This time of the wander is basic in light of the way that at this stage the speculative arrangement is changed over into useful one. This stage is an essential stage since this stage requires especially correct masterminding and need the learning of existing system and its impediments. The execution organize should be made by thinking about each one of the requirements, goals. The new structure should be fruitful and work fittingly.

5. CONCLUSION

In this project, the issue of sharing the information in distributed computing safely is settled.
Information protection can be kept up by mix of ABE and BRE calculation. Validation is utilized to ensure information security and information honesty. This shows the proposed framework can be utilized to improve protection conservation in cloud administrations.

6. 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.