A NOVEL TIME BASED SECURE DATA HANDLING IN PUBLIC CLOUD WITH DE-DUPLICATION

M.A. BIBI AYSHA[1], Md.ASIM[2]

[1]PG Scholar, Dept. Of CSE, Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool, A.P.

[2] Assistant Professor, Dept. Of CSE, Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool, A.P.

ABSTRACT: ***In recent years one of the most important technique emerged in IT industry is cloud computing. This technology requires the data stored in cloud to be trusted, concept of security and privacy has increased. Most of the schemes proposed so far doesn't have flexibility in implementing complex access control. This paper achieves the flexibility and fine-grained access control in public cloud. We know that data security is an important factor in cloud which is to be concentrated because of data outsourcing and lack of trust in cloud servers. Another important pattern in cloud computing is the storage which acts as a service which provides great flexibility and also economic savings. The most important technique for data sharing in cloud is achieved by encrypting the data and issuing decryption keys by the data owners to the authorized users. One of the best technique used here is the CP-ABE (Ciphertext Policy Attribute Based Encryption) in which both keys and attributes are managed by a trusted authority. To protect the confidentiality of the data from the CSP (Cloud Service Provider) many schemes have been invented. However, there is no efficient scheme, which embeds fine-grained access control together with the time sensitive data. A time and attribute factors combined access control is necessary to handle time-sensitive data in public cloud storage. Timed release encryption is a kind of encryption in which owner encrypts a message for the purpose that intended users can decrypt it after a designated time. Apart from access control,the proposed system embeds the TRE and CP-ABE with Redundancy check by which the TAFC with De-duplication system is formed to overcome the problems of time based access control and storage.***

Keywords: Cloud Storage, Time-sensitive data, access control, De-duplication

I.INTRODUCTION

Cloud computing is a technical and social reality and an emerging technology. Scientific and engineering applications, data mining, computational financing, gaming, and social networking as well as many other computational and data intensive activities can benefit from cloud computing. A broad range of data can be stored in cloud.Informations and applications in the cloud can be maintained by using internet and central remote servers. The main advantage of cloud computing is outsourcing of data to the cloud. As a result users can free from burden of data storage and its related maintenance. But it leads to another sophisticated issue such as integrity and confidentiality of data stored in the cloud. We use different strategies to provide security on data stored in cloud. To achieve this, we provide overall control to data owners instead of these un-trusted cloud service provider. Data stored in the cloud can be protected by using an effective method like information access mechanism. But the present server oriented access control methods are not beneficial for prolonged period of time frame. Nowadays many users can get access to data simultaneously. Different users can access the same data on different time period.so the data owner always stay online for giving variety encryption of same data. This leads more burden to data owner.

And additionally, it leads to take extra storage for preserving these different keys, due to more than copies of cipher text for every information. To solve these problem by combining "CP-ABE and TRE" mechanism in public cloud. So different users can get different releasing time points. To avoid redundancy the user performs the De-duplication.

II. Problem Statement

Security of information stored in public cloud is a difficult process. It uses encryption and decryption method to protect data. It uses secret keys and public keys to protect data. The technique known as CP-ABE (Cipher text Attribute-Based Encryption) is used in old data security method. Using new technique a user can decrypt data not only using the secret key but also satisfy some attribute values. But nowadays data stored in the cloud are time sensitive, so we introduce a new system including CP-ABE and time based accessing.

- Difficult to identify the behavior of cloud service provider, if they are providing secured data to the requested user.
- Any time user can access data without that user's time arrival.
- Security either in backward or forward is difficult.
- How to avoid similar copy of data

III. SECURITY ASSUMPTION , SECURITY REQUIREMENTS AND SYSTEM ARCHITECTURE:

To solve above all problems. This system uses an asymmetric key algorithm for encryption and decryption that means we are using the same key for both encryption and decryption. In this mechanism, we are introducing a technique known as time release encryption with De-duplication to the architecture of cipher text attribute-based policy encryption. As a result, it helps data owners with the capability to flexibly release the access privilege to different users at a different time, by satisfying access policy that contains attributes and releases time and to overcome the de-duplication.

3.1 TAFC with De-duplication:

This ensures the security of data stored in the cloud by combining two factors such as time and attributes. This method ensures the efficient access control for time-sensitive data in public cloud, known as TAFC. It can be achieved by a) CP-ABE mechanism is used for inheriting fine granularity property b) Trap door mechanism known as TRE. [6].Below figure, fig1 shows the architecture of TAFC with Redundancy Check. It mainly contains Cloud service provider, a central authority, many information owners and several data consumers (users).

3.2 Cipher Text Policy Attribute-Based Encryption

This encryption technique consists of three entities: The central authority, user and information owner. The keys are issued by the central authority for the intended users. Then intended user can get data from the owner based on the access policy. Attribute and

logic gate groups can be expressed as a tree that represents access policy in the CP-ABE mechanism. Attributes of each user can define the secret key generated from authority. Based on this scheme the cloud server has no responsibility related to this encryption and decryption.This scheme uses four algorithms to achieve its goal, that are a)Setup b)Key generation c)Encryption d)Decryption

Admin:

The main function of Admin are a) Login b) Authenticate Data owner c) Authenticate Data User d) View all files e) View time sensitive files f) Sent time key.

Cloud Service Provider: is a third party that offers infrastructure, cloud platform, storage and different application for requested users or organizations. It stores a large amount of data from users and provides data to users based on their demand. Cloud service provider has the right to view all information in the file, view all data owner and users, view all files related to time-sensitive information and it performs redundancy check.

The central authority: is handling the overall protection of data in the cloud. It publishes the private key and secret key of each data based on its predefined time period. The main function of central authority are a) View b) viewing all user information c) viewing user's request d) issuing secret keys.

The Data Owner: Any number of owners is present in this module and to register before doing any operations. After successful registration, owners can upload the file to the using the registered valid user name and password.

The Data User: Any number of users is present in this module for accessing the requested file from the cloud after satisfying secret keys and time. After successful registration, users will get a valid user name and password. Using those only users can search the requested file present there or not.

3.3 Timed Release Encryption

This encryption mainly provides security to someone who wants to send a message to another one at later time or future. The data owner can set the time schedule for each user. Based on this scheme same data can be viewed by different users at the different time period. After the time is over, no user can access the information the cipher text can be generated along with a particular releasing time and the public key of the intended user.

3.4 System Architecture:

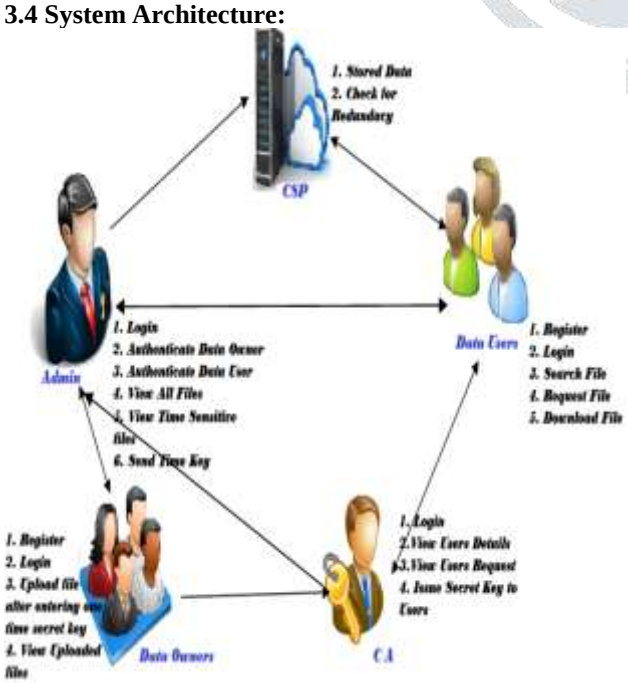

Figure 1: System Architecture

To properly elaborate the concept of proposed system, we have implemented it in a client and server platform. Initiation of the procedure starts from the data owner or owner registering on the portal using his/her mail id. As soon as owner registers, a secret key is generated and sent through mail which is registered and used for login. Upon logging in, owner uploads the necessary documents to cloud. The owner will have access to his/her uploaded documents. After uploading, the owner can set a time seal. The time seal allows the recipient to access the specific document within that time span. And on addition to it, the files can be accessed only with the secret key.

After completion of owner part, the user will register when he/she is notified. As soon as user registers, the secret key is generated and sent through mail which was used for login. Then user will search for the owner by entering keywords as per directed and a send a request to owner for accessing the file. After receiving the request, owner activates the request and the user can download a file using secret key and only the Data user can update or download the files.

In addition to this take care is used which act as alternative to user. An emergency can be filed on behalf of data owner and they send a file request to take care. The take care activates the request and thus emergency can download the file using secret key. On other hand admin will have all information about user, owner and downloaded files and when ever the data owner want to store the redundant data the data owner gets the popup message the file exist by which the redundancy of data is handle by which user avoid redundancy with the help of De-duplication method.

4.Conclusion:

The proposed system mainly focuses on secure storage of data in public cloud. It also provides facility for grain grained access control of time sensitive data and De-duplication for data. To achieve this by integrating CP-ABE and TRE mechanism. Based on this scheme data owners can be decided which user able to be access data and its provide relevant accessed privilege releasing time point according to a well define access policy over an attribute and releasing time. And it provide a lightweight overhead on together central authority and a data owners. This mechanism is highly applicable for large scale access control system for cloud storage.

5. REFERENCES

[1] K.Yang, X.Jia, K.Ren, B.Zhang, and R.Xie,"DAC-MACS: Effective data access control for multi-authority cloud storage systems,"IEEE transactions on Information Forensics & Security, vol. 7, 2012

[2] Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute-based encryption,"IEEE transactions on parallel and distributed systems, vol 24, 2013

[3] Elli Androulaki, Claudio Soriente, Luka malisa & Srdjan Capkun, "Enforcing location and time-based access control on cloud-stored data, IEEE 34 international conference on Distributed computing systems,2014.

[4] Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, "DABKS: Dynamic attribute-based Keyword search in cloud computing", IEEE communication and information systems security symposium,2017

[5] Quin Liu, Guojun Wang, & Jie wu," Clock based proxy Re-encryption scheme in the unreliable cloud,"IEEE 41 international Conference on parallel processing workshops, 2012

[6] Kan Yang, he Liu, Xiao Hua jia, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach, IEEE Transaction on Multimedia, vol 18, 2016.

[7] Kui Ren, Cong Wang & Quian Wang, "Security Challenges for the Public Cloud, IEEE Computer Society, Jan 2012
[8]Cong Wang, Quian Wang & Kui Ren, "Privacy-preserving public auditing for data Storage Security in Cloud Computing", IEEE communication society,2010.
[9] C.Wang, J.Luo,"An efficient key policy attribute-based encryption scheme with constant cipher text length "Mathematical Problems in engineering, 2013
[10] K.Yang, Z.Liu, X.lia, &X.Shen, "Time-domain attribute based access control for cloud based video content sharing",IEEE transactions,2016

About Authors:

M.A. BIBI AYSHA is current pursuing M.Tech in CSE. dept., Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool, AP, India**.**
Md.ASIM$_{M.Tech}$, Assistant Professor (CSE), Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool, AP, India.