Survey on Secure Data Self-Destruct Scheme & Division and Replication of data on cloud.

Navanath Bhosale, Sumeet Karn, Sunil Moosad, Mayur Pare, Mr. Rajesh Lomte.

[1] *Student, Computer Department, P.C.C.O.E-Pune, Maharashtra, India*
[2] *Student, Computer Department, P.C.C.O.E-Pune, Maharashtra, India*
[3] *Student, Computer Department, P.C.C.O.E-Pune, Maharashtra, India*
[4] *Student, Computer Department, P.C.C.O.E-Pune, Maharashtra, India*
[5] *Professor, Computer Department, P.C.C.O.E-Pune, Maharashtra, India*

ABSTRACT

There is always a risk of unauthorized users accessing the private data. Fine grained data loss prevention policies helps to manage what get stored in the cloud, how it gets stored and what stays on-premises. In this paper, we proposed using KP-TSABE (Key Policy-Time Specified Attribute Based Encryption) scheme for securely self-destructing data and DROPS (Division and Replication of data in cloud for Optimal Performance and Security) for secure storage in cloud.KP-TSABE policy used in this model is superior to other present schemes. DROPS scheme allows the data to be fragmented which are stored in the nodes separated by some distance by using graph T-coloring method for preventing data breach. Also we propose Time-Based One Time Password (OTP) for authentication of legitimate user and SHA-2 hash function for data integrity check. For encryption and decryption we propose modern Advanced Encryption Standard (AES) algorithm. Using all these levels of security slight overhead was observed in the performance of the system. By using high security techniques we aim to secure data within the cloud ecosystem.

Keyword: - *Fine grained data loss prevention, KP-TSABE, DROPS, Time-Based One Time Password (TOTP) security.*

1. INTRODUCTION

The number of cloud services being used in enterprise is growing daily. Cloud applications are easy for users to buy and require minimal effort to get up and running. It provides users and enterprises the capability of storing and processing their data in either privately owned or third party data centers. But the downside of this public cloud is that management of data storage is not in the hand of business enterprises. The shared data can be user's sensitive information (for e.g. personal profile information, financial details, and other important data) must be well protected. That's why the security and privacy becomes big challenge in cloud computing. So it is essential to provide comprehensive solutions against these circumstances.

One of the best ways to secure data is to provide specific predefined authorization period and to give fine grained access within that period. And the sensitive data should be self-destroyed after that expired time span. Key Policy-Time Specified Attribute Based Encryption (KP-TSABE) policy is used for this purpose[1]. Sometimes owner of data wants to share their information with particular user, then Attribute Based Encryption (ABE) technique plays vital role, this technique has significant properties based on public key encryption which provides one-to-many encryption[2]. So data owner sets specific attributes for that particular user. After the validation of these attributes, user gets grant for accessing data. Then only that user can access.

In general, the data owner has specific right to specify the time limit for accessing the sensitive data. After that time period user won't be able to access this sensitive information. Time release encryption (TRE) technique provides service for Client to construct the decryption key before the expiration of predefined time. This is happened because

of time specific encryption (TSE) which provide authority to the data owner to specify suitable period of time, such that client can access received data only within that span[3].

2. SYSTEM ARCHITECTURE

The system consists of four parts, Cloud Server, Users, Administrator, Authority and Time Server. Amongst these units Administrator and Users are provided with GUIs. In this system the users request for the files they want and after authenticating the user the administrator will upload the file. The file is then encrypted during the uploading process. This file is then sent to the cloud server. Thereafter the cloud server has a fragmentation algorithm called DROPS (Division and Replication of data in cloud for Optimal Performance and Security) which is used to divide the file into specified number of partitions. These partitions are then stored into different nodes in the file server of cloud. To decide which nodes are to be selected for storage T-Coloring graph is used[4].

2.1 Cloud Server

The cloud servers are maintained by the cloud service provider, a third party system. Therefore, it is necessary that the files and information to be stored be completely secure. Here we use DROPS algorithm to safeguard the data because the control of maintenance of those servers are not in the hands of administrators or users.

This end does following tasks:

- Running the DROPS algorithm to divide the file into different fragments[4].
- Placing the fragments into different nodes using T-Coloring graphs[4].

A database is used to keep track of the fragments of the file. The path of each file fragments will be stored in this database in encrypted format. This can ensure that the data is not accessible to the cloud service providers. Hence improving the security of the system.

Fig -1: Architecture block diagram

2.2 Administrator

The administrator is responsible to serve the requests of the user. Here a database is maintained to store the user information and login credentials. This database is used to authenticate each user according to their requirements. A SQL database is used to store the login details. The administrator has to login to upload a file. Also Admin is responsible to set the time-limit as this system uses KP-TSABE scheme[1]. This end specifically does following tasks:

- Login to the cloud ecosystem
- Encrypts the file using AES algorithm

- Uploads file and sets the time limit

The AES algorithm is found to be more efficient than the asymmetric key cryptographic algorithm RSA[5]. Also KP-TSABE scheme provides best security to data access since it specifies time limit during which the data will be available[1]. After the time limit even if data is available it will not be decrypted.

2.3 Authority and Time server

An authority is responsible for authenticating the user using the user attributes stored in the database. The Time Server is used to keep track of the time interval and uploading as well as downloading times of the data at the users end[3]. This end do not have any UI controls.

Authority has following functionalities:

- It is responsible for key management of the users.
- It coordinates with the time server and administrator to check whether the time limit is not exceeded.
- Once the users are verified and the current time is checked with time interval the decryption key is sent to the user.

2.4 Users

User end is designed for the people who want to access the data. For this purpose the user has to request the administrator for a particular data. After authentication and verification of the user the user will be able to access the file on the cloud. The file downloaded by the user will be decrypted only if it is in the specified time interval. Otherwise it is not decrypted and it is said to be self-destroyed[1].

This end has following features:

- A rich GUI which will be used by user to access the files uploaded on the cloud.
- Users will have attributes related to them specifically.
- These attributes are used by cloud system and authority to authenticate and grant permission to the user.

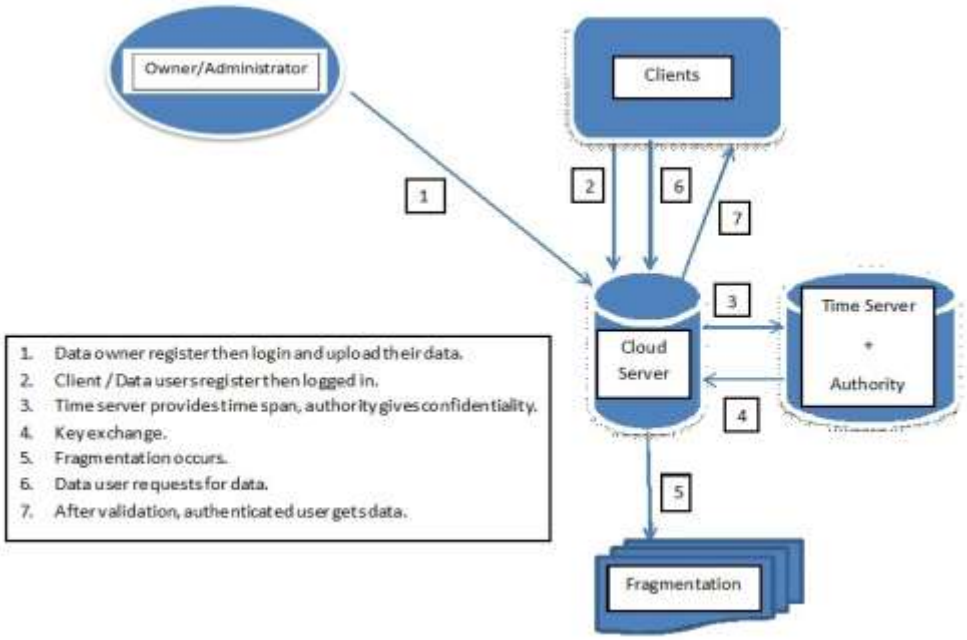

Fig -2: Overview of functioning

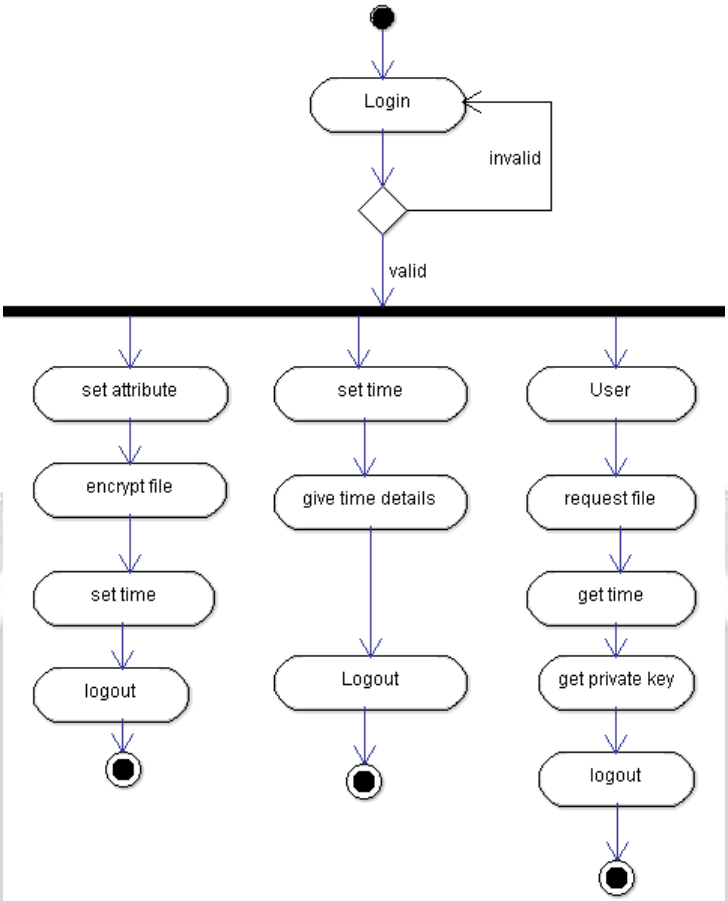

Fig -3: Flow diagram of system

3. ADVANTAGES

Attributes	DES	RSA	AES
Type	Symmetric	Asymmetric	Symmetric
Speed	Slow	Slower	Faster
Security	Less secure	Enough secure	Highly secure
Usage	Rarely use	Typical use	As per security concern

- The data is not stored in contiguous memory blocks therefore it reduces the risk of data breaches.
- Specific time interval provides fine grained access control during that period.
- Time based OTP is used to authenticate the user. It ensures OTP is not accessed after the time span[6].
- The system does not require any special hardware or infrastructure to be implemented.
- Initial investment is very low and can be ignored.

4. CONCLUSIONS

KP-TSABE policy has some disadvantages like data is stored in contiguous block of memory. So if unauthorized user gets access to that block, he can misuse our all data. Therefore, in this paper we used DROPS scheme to store the data on non-contiguous memory location.

5. REFERENCES

[1] Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen, "A secure data self-destructing scheme in cloud computing*," IEEE transactions on cloud computing* vol:pp no:99, 2014

[2] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," *International Journal of Network Security*, vol. 16, no. 4, pp. 351–357, 2014.

[3] K. Kasamatsu, T. Matsuda, K. Emura, N. Attrapadung, G. Hanaoka, and H. Imai, "Time-specific encryption from forward-secure encryption," in *Security and Cryptography for Networks*. Springer, 2012, pp. 184–204.

[4] Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," IEEE Transactions on Cloud Computing, 2015

[5] Nilesh R. Patil, Rajesh Dharmik "Secured Cloud Architecture for Cloud Service Provider," World conference on futuristic trends in research and innovation for social welfare, 2016

[6] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A Secure Cloud Storage System Combining Time-based One Time Password and Automatic Blocker Protocol," *IEEE,* 2015