ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Time Specified Data Self-Destruction Scheme in Cloud

Sriram.M[1], Dr.R.Anand[2]

Department of Information Technology, K.C.G. College of Technology, Chennai, India[1,2]

Associate Professor, Department of Information Technology, K.C.G. College of Technology, Chennai, India[3]

ABSTRACT: To reduce the lack of security of data stored in cloud, we propose a time specified scheme to remove the outsourced data in cloud. A data owner can upload the file with certain time interval. Data user should access the file within the time interval. Our system has an admin to assign secret key to each user to access the file from the cloud. The time specified scheme used in this system will allow data owner to set time interval for each data uploaded. After the time period the file uploaded will get self-destructed.

KEYWORDS: Data security, Time specified self-destruction, Cloud, privacy preserving, outsourced data.

I. INTRODUCTION

Cloud is anoverall term used to label a new class of network based computing that continues over the Internet.These platforms hide the complication and details of the primary infrastructure from users and applications by providing very simple graphical interface or API Basically a step on from Usefulness Computing Using the Internet for statement and transport provides hardware, software and networking services to clients. A collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform).

1.1 Cloud security

Security ruins a primary concern for businesses anticipating cloud adoption especially public cloud adoption. Nevertheless, this resistance is vanishing, as logical remoteness has proven reliable, and the addition of data encryption and various identity and access management tools has improved security within the public cloud.This environment demands copious isolation between logical compute resources. Public cloud service providers share their primary hardware infrastructure between frequent customers, as public cloud is a multi-tenant location. the cloud servers may transfer users' data to other cloud servers in outsourcing or share them in cloud searching. Therefore, it becomes a big experiment to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authorization period and to provide fine-grained access control during this period. The shared data should be self-destroyed after the user-defined expiration time.

1.2 Related work

LITERATURE SURVEY

Data pertaining to health is a typical example of the type of sensitive information handled in cloud computing environments, and it is obvious that most individuals will want information related to their health to be secure. Sensitive information in the framework of cloud computing encompasses data from a wide range of dissimilar areas and disciplines

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

1.2.1 System description

This explains quite a few privacy issues associated with genomic sequencing. This study also described several open examine problem along with giving suggestions to improve privacy through association between different entities and organizations.The author's implement a server-side indexing configuration to produce a system that allows a single database owner to privately and efficiently write data to, and multiple database clients to confidentially read data from, an outsourced database .The authors define the concept of "outsourcing privacy" where a database owner updates the database over time on untrusted servers. This definition assumes that database clients and the untrusted servers are not able to learn anything about the contents of the databases without authorized access

1.2.2 Implementation

Homorphic encryption is a different privacy-preserving solution that is based on the idea of computing over encrypted data without knowing the keys belong to different parties. To make sure confidentiality, the data owner may encrypt data with a public key and store data in the cloud. When the progression engine reads the data, there is no need to have the DP's private key to decrypt the data. In private computation on encrypted genomic data, the authors proposed a privacy-preserving model for genomic data processing using holomorphic encryption on genome-wide association studies.

1.2.3 Secret key sharing:

Secret allotment schemes are ideal for packing information that is highly sensitive and highly vital users of a group wish to interconnect using symmetric encryption, Admin must share a common key A secret key sharing scheme allocatessections so that anyone with fewer than 'T' shares has no extra information about the secret than someone with 0 shares. Recently, we conferred a secure secret key sharing algorithm using non-standardized equation .In this paper, an algorithm for such perfectly secure scheme by using Pell's equation is introduced.

1.2.4Secure deletion

Many systems have been proposed which essentially overwrite the data in order to delete it Some methods are very flexible and can be integrated with arbitrary file systems provided their source code is available FADE comes closest to the approach among the existing work .its policies are intertwined with an implementation from a particular public-key crypto system. In contrast, a work permits general policies using Boolean expressions with threshold operators, may use generic crypto systems, including secret-key systems, and supplies security proofs for all constructions. . Nevertheless, all solutions using overwriting depend heavily on the properties of the underlying physical storage. The FADE system uses public-key cryptography and introduces some simple policies with Boolean operators overriding deletion.

II. MOTIVATION

In Time specified data self-destruction scheme, As a result unauthorized users can freely access to the sensitive data and this flaw would lead to a serious privacy disclosure. Outsourced data should be identified and deleted accordingly in cloud. Availability of outsourced data occupies more storage space.

III. CONTRIBUTIONS

In this paper, we propose a time specified scheme, which is time interval for self-destructing scheme for data sharing in cloud computing. We first introduce the notion of TSS formalize the model of time specified scheme and give the security model of it. Then, we give a specific construction method about the scheme. Finally, we prove that the time specified scheme is secure. Especially, Time specified scheme has the following advantages with regard to security and fine-grained access control compared to other secure self-destructing schemes.

1. Time specified scheme supports the function of user defined authorization period and ensures that the sensitive data cannot be read both before its desired release time and after its expiration.
2. Time specified encryption does not require the ideal assumption of "No attacks on VDO before it expires"

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

3. Time specified scheme is able to contrivance fine-grained access control during the endorsement period and to create the complex data self-destruction after expiration without any human intervention.

IV. SYSTEM MODULES

In our system, we mainly focus on how to achieve fine-grained access control during the authorization period of the shared data in cloud and how to implement self-destruction after expiration. We define the system model by dividing the time specified scheme into the following four entities as shown below

4.1 Data Owner:
Data owner can provide data or files that contain some sensitive information, which are used for sharing with his/her friends (data users). All these shared data are outsourced to the cloud servers to store.

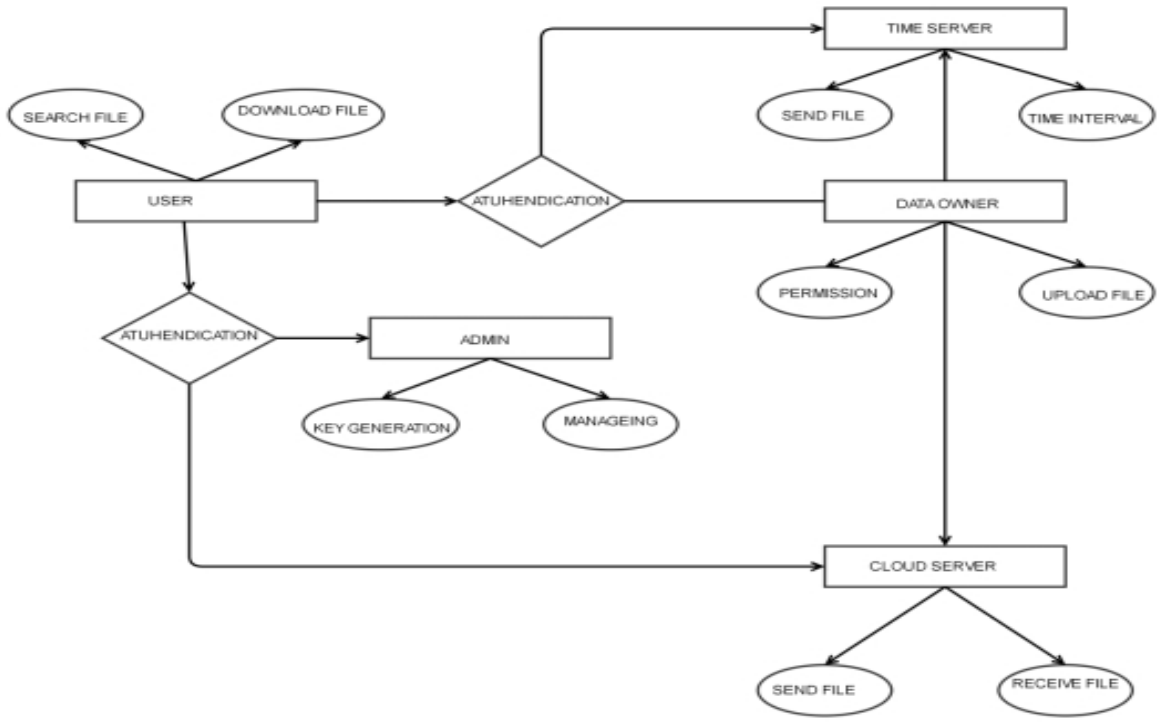
4.2 Admin:
It is an indispensable entity which is responsible for generating, distributing and managing all the private keys, and is trusted by all the other entities involved in the system.

4.3 Time server:
It is a time reference server without any interaction with other entities involved in the system. It is responsible for a precise release time specification.

4.4 Data users:
Data users are some peoples who passed the identity authentication and access to the data outsourced by the data owner. Notice that, the shared data can only be accessed by the authorized users during its authorization period.

4.5 Cloud Servers:
It contains almost unlimited storage space which is able to store and manage all the data or files in the system. Other entities with limited storage space can store their data to the cloud server

V. METHODOLOGY



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

VI. ALGORITHM DESCRIPTION

1. **Upload:** In the system initialization phase, a data owner uploads the file through data owner login
2. **Encryption with time constraint:** The data owner chooses a file for the shared message and defines a time interval. Then, the data owner invokes the algorithm to encrypt file to its cipher text, which is associated with the time interval. Finally, Cipher text is sent to cloud servers.
3. **Authorization time:** When a user wants to access the shared data M during its authorization period, he must pass the identity authentication and should perform the following processes: Firstly, the current time interval will be specified therefore, time specified scheme allows for extremely flexible implementation of fine-grained access control through combining different attributes with corresponding time intervals.
4. **Time specified data destruction after end of the time interval:** Once the current time instant becomes after the threshold value (expiration time) of the valid time interval, the user cannot obtain the true private key. Therefore, the cipher text is not able to be decrypted in polynomial time, facilitating the self-destruction of the shared data after expiration.

VII.CONCLUSION

With the rapid development of versatile cloud services, a lot of new challenges have emerged. One of the most important problems is how to securely delete the outsourced data stored in the cloud. In this paper, a proposed system of time specified constraints for each file or data uploaded by the data owner in cloud. Time interval will be send to user. And key generation will be done by Admin where unique key will be generated to each user. When the time interval ends data will be self-destructed from cloud.

REFERENCES

1. Ali Gholami and Erwin Laure HPCViz Dept., KTH- Royal Institute of Technology, Stockholm, Sweden “Security and privacy of sensitive data in cloud computing”: a survey of recent developments
2. Christian Cachin , KristiyanHaralambiev , Hsu-Chun Hsiao† ,Alessandro Sorniotti ACM Transactions on Information and System Security “Policy-based Secure Deletion”
3. E. Muralikrishna1 §, S. Srinivasan2, N. Chandramowliswaran3 1,2School of Advanced Sciences VIT University “secure schemes for secret sharing and key distribution using pell’s equation”
4. J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, “A full lifecycle privacy protection scheme for sensitive data in cloud computing,” Peerto-Peer Networking and Applications. [Online]. Available
5. R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, “Toward efficient and privacy-preserving computing in big data era,” Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.