ISSN:0975-9646

Survey on Secure Data Self-Destructing Scheme in Cloud Computing

M.Bhandari, Pooja Chaudhari, Sonal Sonawane, Bhagyashree Shetkar,. Manisha Konde

Department of Computer Engineering.
G.H.Raisoni Institute of Engineering and Technology,
Wagholi.

Abstract-The Cloud Computing is use for large amount of storage data, but the main drawback is security and privacy of data in cloud computing. So this problem solve by using the Key Policy-Time Specified Attribute based encryption(KP-TSABE),secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, Each of the ciphertext are labeled with a time interval in that period of time private key is associated with a time instant. The KP-TSABE is solve some of the important security problems by supporting user-defined authorization period and by providing fine-grained access control during that period. The private data will be securely self-destructed after a user-specified expiration time.

INTRODUCTION

The Large Data is Store in Cloud Computing, but the data on cloud is open for everyone, one who has internet connection can access data present on cloud. The main Drawback is that the cloud is open for every one that means any one can access information present on this due to such fact the data becomes un-secure. That data may be accessed by malicious agent, attackers, etc. So we proposed the KP-TSABE scheme which means Key Policy Time Specified Attribute Based Encryption. In this scheme the data is encrypted and converted into ciphertext. Each ciphertext is labelled with specific time instant and private key is associated with it. Within that particular time instant allocated by the user (simply user defined time server) the ciphertext can be decrypted not after that period. The scheme also provides fine- grained access control to the data(means users can access data fully).

After the expiration of user defined time period the data is self-destructed. Our scheme provides solution to security problems and proved to be a superior among the other techniques.

KP-TSABE System Model

The system focuses on providing not only security to the data but also to provide the fine-grained access control to the data. With all this facilities the time based or time specified encryption is also provided to the data. That means the data can be encrypted or decrypted only within the specific time. This time can be given by the user i.e. it may be userdefined. We can derive the KP-TSABE scheme in following six entities:

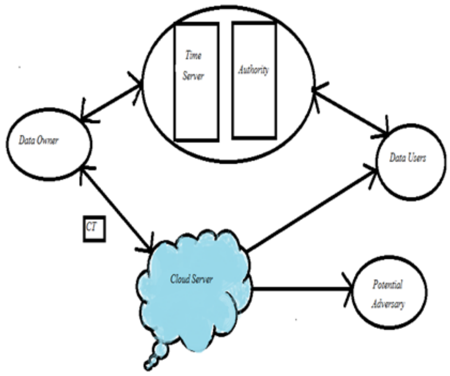

Fig.1.System model of the KP-TSABE scheme.

Following users are targeted to use the system:

***(1)Data Owner*:**

a) Logging into the system with proper authorization using username and password.
b) Data owner can provide data or files that contain some personnel information, which are used for sharing with his/her friends (data users).
c) All these shared data are outsourced to the cloud servers to store.

(2) *Authority*:

a) Checks request from authorised users.
b) Generates key k1 for the user.
c) Returns key as response to the user.

(3) *Time Server*:

a) It is a time reference server without any interaction with other entities involved in the system.
b) It is responsible for a precise release time specification.
c) Provides user defined time period t1 to the user.

(4) *Data Users*:

a) Passes the identity authentication and access to the data outsourced by the data owner.
b) The shared data can only be accessed by the authorized users during its authorization period.

(5) *Cloud Servers*.

a) It contains almost unlimited storage space which is able to store and manage all the data or files in the system.
b) Other entities with limited storage space can store their data to the cloud servers.

(6) *Potential Adversary*:

a) It is a polynomial time adversary and described in the security model.

Literature Survey

Attribute-based encryption:

Attribute-based encryption is important applications of identity-based encryption . ABE consist of two policies called KP-ABE and ciphertext -policy ABE (CP-ABE) . In CP-ABE, is the Ciphertext attribute based encryption. proposed the first CP-ABE scheme , security proof was only constructed under the generic group model is the main disadvantage of this scheme. Thus to solve this problem chang presented another construction under a standard model .

Time-Specific Encryption:

In Time Specific Encryption(TSE) the sender of a message can specify any time interval during the encryption process;the receiver can decrypt to recover the message only if it has a TLK(Time Instant Key)that corresponds to a time in that interval.

The time has always play important role in communication.sensitive data may not be released before a particular time or we may wish to enable access to information for only a limited period of time.

The specific time the receiver can be decrypt a ciphertext.If time is up then no one can be able to receive the data.

Advanced Encryption Standard

Like DES, AES is also symmetric algorithm. The same key is used for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations.A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively.

Comparison Of Analysis:

Parameters	**AES**	**DES**	**3DES**	**RSA**
Speed	Fast	Slow	Very slow	Slowest
Security	excellent	Not enough secure	Adequate security	Less
Type	symmetric	symmetric	symmetric	Asymmetric

Conclusion

The cloud services are developing day by day rapidly. With this rapid development the lot of new challenges are generating. The most important problem is how to provide security and how to securely outsource the data from cloud. To solve this problem in this paper we have developed a secure scheme i.e. KP-TSABE which provides time specified encryption decryption . Also our scheme provides the fine-grained access control to the data. Also time based encryption involves the user defined time period.

Also the self-destruction of the data after expiration of the user specified time instant is also done. We have given system model for the KP-TSABE scheme. Using such models we have proved that KP TSABE scheme is secured and have fine-grained access control with the time specified or time based encryption and decryption

Acknowledgement:

We extend our sincere thanks to Mr. Mahesh Bhandari Project Guide for his valuable guidance. He was always there for suggestion and help in order to achieve this goal.

We are indebted to Mrs. Deeksha Bharadwaj ,HOD and Dr. R.D. Kharadkar ,Principal, G.H. Raisoni Institute Of Engineering and Technology, Pune for encouragement and providing us the opportunity and facilities to carry out this work .

And finally we would like to thank the college for being such strength during the entire work .

References

1. "Attribute based access control with constant size Ciphertext in cloud computing",Wei Teng, Geng Yang,Member IEEE.
2. "Attribute based encryption for fine-grained access control of encrypted data",Vipul Goyal,Omkant Pandey,Amit Sahai,Brent Waters.
3. " Secure Schemes for Secret Sharing and Key Distribution",Amos Beimel.
4. "Time-Specific Encryption",Kenerth G.Paterson and Elizabeth A.Quaglia.
5. "A secure data self-destructing scheme in cloud computing",Jinbo Xiong,student member,IEEE,Zhiqiang Yao.