A Secure Data Self-Destructing Scheme In Cloud Computing

M S Jayaprabha
Department of Computer Science, Thassim Beevi Abdul Kader College For Women, Kilakarai
Email: prabha.jayams@gmail.com
Dr A R Nadira Banu Kamal
Department of Computer Science, Thassim Beevi Abdul Kader College For Women, Kilakarai.
Email: nadirakamal@gmail.com

ABSTRACT

The cloud computing is the on demand accessing of server which is used to store, manage and process data. The server is in network hosted as remote so the implementation of security and access control is tedious process. While the people use the data which is shared in environment at that time the security is major problem. So the sensitive data may not be in secured position. In order to tackle this problem I am introducing A Secure Data Self Destruction scheme in Cloud Computing Environment using KP- TSABE.

In the KP-TSABE scheme, every ciphertext is labeled with a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. The KP-TSABE is able to solve some important security problems by supporting user-defined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time.

Keywords: **Cloud computing, ciphertext, fine-grained access control, KP-TSABE, Self-destruction, Time interval.**

I. Introduction

A Secure Data Self-Destructing Scheme in Cloud Computing will gives the security for the files which is stored in cloud server. Cloud computing is considered as one of the next step in the evolution of on-demand information technology. It combines a set of existing and new techniques from research areas such as Service- Oriented Architectures (SOA) and virtualization.

Cloud computing is used to share data with known or unknown friend circle such as Dropbox, Google Drive and AliCloud [5]. In this case the security is an important characteristic of the sharing of data in the cloud computing environment. The shared data in cloud server may contain users' sensitive information such as personal profile, financial data and health records. So the information needs to be well protected from the third party [14]. As the ownership of the data is separated from the administration of them [11], the cloud servers may migrate users' data to other cloud servers in outsourcing or share them in cloud searching [18].

Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment [22]. 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. The data should be accessed by only the authorized user.

II. KP-TSABE Scheme

This scheme proposes a key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, every ciphertext is labeled with a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure.

The KP-TSABE is able to solve some important security problems by supporting userdefined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time. The KP-TSABE scheme is proved to be secure under the decision l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) assumption. This l-BDHI assumption holds in (G; G') if no t-time algorithm has the probability at least ε in solving the l-BDHI problem for non-negligible ε. The KP-TSABE scheme is indistinguishably secure against selective attribute chosen plaintext attack if all polynomial time adversaries have at most a negligible advantage. This method, mainly focus on how to achieve fine grained access control during the authorization period of the shared data in cloud and how to implement selfdestruction after expiration. The decryption is exempted because of the deletion of the data after the expiration time.

i. 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.

ii. **Authority**

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.

iii. **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.

iv. **Data users**

Data users are some people 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.

v. **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 servers.

vi. **Potential adversary**

It contains the security and validation of the data in the cloud server.

2.1 Advantages of KP-TSABE System:

- Attribute based encryption (ABE) has significant advantages based on the tradition public key encryption instead of one-to-one encryption because it achieves flexible advantages
- With regard to security and fine-grained access control compared to other secure self-destructing schemes.
- Supporting user-defined time-specific authorization, fine-grained access control and data secure self destruction.

The algorithm level of the KP-TSABE scheme includes four algorithms: Setup, Encrypt, Keygen, and Decrypt. The details of the algorithm specified in Table 1.

Alogrithm	Specification
Setup	This algorithm is run by the Authority and takes as input the security parameter
Encrypt	This algorithm generates the ciphertext which is associated with the fuzzy attribute.
KeyGen	This algorithm takes as input the master key, associated with a time instant and outputs a private key.
Decrypt	This algorithm takes as input the ciphertext and the private key When a set of time specific attributes satisfies, it is able to decrypt the ciphertext and return the plaintext.

Table 1: KP-TSABE scheme algorithms

2.2 System Descriptions of the KP-TSABE

2.2.1 System setup

In the system initialization phase, a data owner chooses a large security parameter k and attribute universe *U*, and invokes the algorithm Setup(1^k, *U*) belonging to the algorithm level to generate system parameters params and master key MSK.

2.2.2 Encryption with time constraint

The data owner chooses an attribute set *S* for the shared message *M* and defines a time interval set T_S for *S*. Then, the data owner invokes the algorithm *Encrypt(M, params, S,* T_S*)* to encrypt *M* to its ciphertext CT, which is associated with the set *S* and T_S. Finally, CT is sent to cloud servers.

2.2.3 Fine-grained access control during the authorization period

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 instant t_x is provided by the time server with t_x € T^t, which is associated with each attribute x. If T^t ε TS and the attribute set of the user matches the access tree ε. Then, the Authority runs the algorithm KeyGen MSK T^t to generate the private key SK and sends it to the user. Once the user received the SK, he will get the CT from the cloud servers and invokes the algorithm Decrypt CT to obtain the shared data M. Because each attribute x is associated with a current time instant t_x, if and only if t_x ε TS and attribute set matches ε, the user can obtain the correct private key SK to decrypt CT. Therefore, the KP-TSABE scheme allows for extremely flexible implementation of fine-grained access control through combining different attributes with corresponding time intervals.

2.2.4. Data self-destruction after expiration

Once the current time instant t_x lags behind after the threshold value (expiration time) of the valid time interval R the user cannot obtain the true private key SK. Therefore, the cyphertext CT is not able to be decrypted in polynomial time, facilitating the self-destruction of the shared data after expiration. Although the computational cost seems to be expensive, optimizations are made to alleviate the computational cost. After the optimization, the final computational cost is located in a reasonable range. The proposed KP-TSABE scheme provides a big advantage by supporting user-defined time-specific authorization, fine-grained access control and data secure self-destruction, which are not well satisfied by the existing schemes.

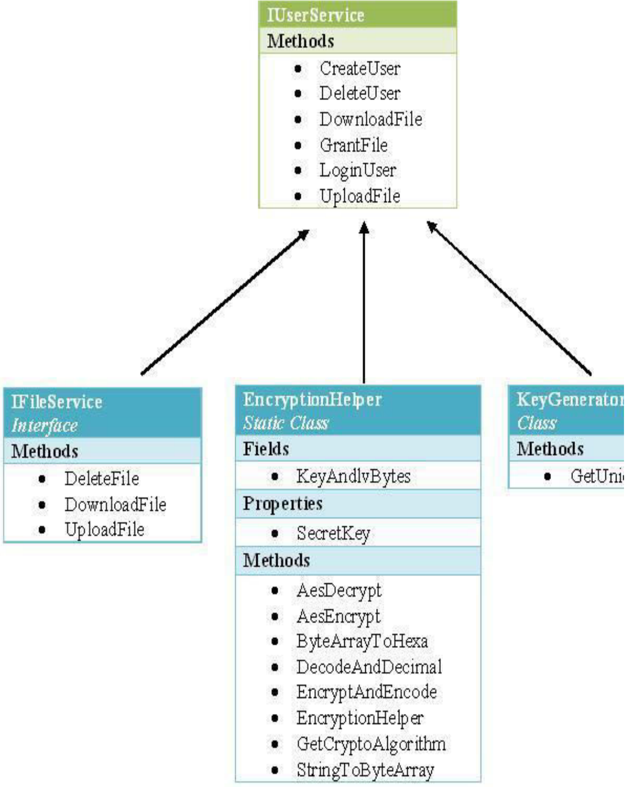

Figure 2: System Model

2.3 Comprehensive Comparison

The KP-TSABE scheme is proved to be secure under the standard model. Therefore, It systematically compare this scheme with the existing self-destruction solutions (e.g., Vanish [21], SSDD [8], ISS [12], and FullPP [11]) from the following aspects, e.g., prerequisite condition, algorithm, resistance on attacks, fine-grained access control, user-defined authorization period, etc. The schemes of Vanish [10], SSDD [6] and ISS [19] need the ideal assumption "no attacks on VDO before it expires", Sybil adversary is able to crawl sufficient key shares to reconstruct the decryption key. Once the adversary gets the VDO from the cloud servers before it expires, he/she will decrypt it with the reconstructed decryption key to obtain the plaintext. FullPP [11] does not need this ideal assumption because the decryption key is encrypted by the ID-TRE algorithm. Even if the adversary gets sufficient key shares from the DHT network, he cannot reconstruct the decryption key since he does not have the ID-TRE private key. The computational cost of Setup, Encryption, Key Generation and Decryption are very cost effective due to the need of pre-computation. The computational cost seems to be expensive, optimizations are made to alleviate the computational cost. In compensation to this, the proposed KP-TSABE scheme provides a big advantage by supporting user-defined time-specific authorization, fine-grained access control and data secure self-destruction, which are not well satisfied by the existing schemes.

IV Figures and Tables

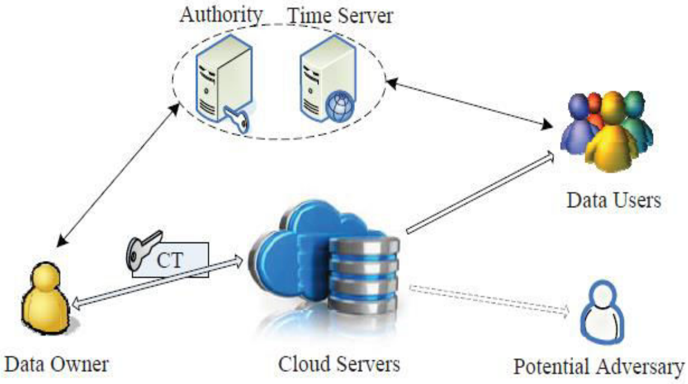

Figure 1: System Model of the KP-TSAPE scheme

The details of the algorithm specified in Table 1.

Alogrithm	Specification
Setup	This algorithm is run by the Authority and takes as input the security parameter
Encrypt	This algorithm generates the ciphertext which is associated with the fuzzy attribute.
KeyGen	This algorithm takes as input the master key, associated with a time instant and outputs a private key.
Decrypt	This algorithm takes as input the ciphertext and the private key When a set of time specific attributes satisfies, it is able to decrypt the ciphertext and return the plaintext.

Table 1: KP-TSABE scheme algorithms

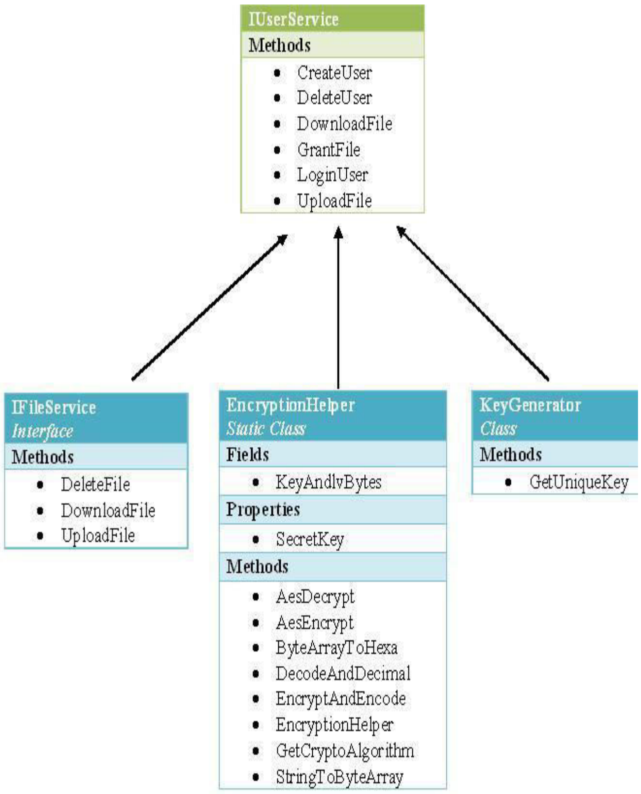

Figure 2: System Model

III Conclusion and Future Enhancement

Finally this **Secure Data Self-Destructing Scheme in Cloud Computing** system provides the security to the files stored in cloud server with the help of KP-TSABE. Due to this files can be easily uploaded, manipulated with secured method. This proposed system provides the security for the uploaded file into the cloud server. The authorized user can only have the permission to access file with the strict time constraint. In this system no need of decrypting the cipher text if the time is elapsed. This proposed system achieved by low cost. So the maintenance cost for this system is less than any other systems. Finally this dissertation concludes as providing the security for the data in cloud environment can be enhanced KP-TSABE system.

3.1 Future enhancement

- ➢ Providing the security for the all the file types such as images, videos, etc
- ➢ Implementing the compression of file size before uploading file in order to reduce the usage of cloud storage

V References

1. A. Beimel, “Secure schemes for secret sharing and key distribution,” Ph.D. dissertation, Israel Inst. Technol., Technion, Haifa, Israel, 1996.

2. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Adv. Cryptol., 2005, pp. 457–473.

3. A. W. Dent and Q. Tang, “Revisiting the security model for timedrelease encryption with pre-open capability,” in Proc. Inf. Security, 2007, pp. 158–174.

4. A.Beimel, “Secure schemes for secret sharing and key distribution,” Ph.D. dissertation, Israel Inst. Technol., Technion, Haifa, Israel, 1996.

5. B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan.–Mar. 2014.

6. C. Cachin, K. Haralambiev, H.-C. Hsiao, and A. Sorniotti, “Policybased secure deletion,” in Proc. ACM Conf. Comput. Commun Security, 2013, pp. 152–167.

7. Dino Esposito (2012) “Programming ASP.NET 4.0” Microsoft Press

8. G. Wang, F. Yue, and Q. Liu, “A secure self-destructing scheme for electronic data,” J. Comput. Syst. Sci., vol. 79, no. 2, pp. 279– 290, 2013. [25] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman, C. J. Rossbach, B. Waters, and E. Witchel, “Defeating vanish with low-cost sybil attacks against large DHTS,” in Proc. 17th Annu. Netw. Distrib. Syst. Security Conf., 2010, pp. 1–15.

9. J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov, “Provably secure timed-release public key encryption,” ACM Trans. Inf. Syst. Security, vol. 11, no. 2, p. 4, 2008.

10. J. Reardon, D. Basin, and S. Capkun, “Sok: Secure data deletion,” in Proc. 34th IEEE Symp. Security Privacy, 2013, pp. 1–15.

11. 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,” Peer-to-Peer Netw. Appl., Jun. 2014, DOI:10.1007/ s12083-014-0295-x.

12. J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, “A secure self-destruction scheme with IBE for the internet content privacy,” Chinese J. Comput., vol. 37, no. 1, pp. 139–150, 2014.

13. J. Xiong, Z. Yao, J. Ma, X. Liu, and Q. Li, “A secure document self destruction scheme: An abe approach,” in Proc. 15th IEEE Int. Conf. High Perform. Comput. Commun., 2013, pp. 59–64.

14. J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, “Priam: Privacy preserving identity and access management scheme in cloud,” KSII Trans. Internet Inf. Syst., vol. 8, no. 1, pp. 282–304, 2014.

15. John Sharp (2013) “Microsoft Visual C# Step by Step” Microsoft Press

16. K. G. Paterson and E. A. Quaglia, “Time-specific encryption,” in Proc. 7th Int. Conf. Security Cryptography Netw., 2010, pp. 1–16. [11] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, “Large universe decentralized key-policy attribute-based encryption,” Security Commun. Netw., Mar. 2014, DOI: 10.1002/sec.997.

17. K. Kasamatsu, T. Matsuda, K. Emura, N. Attrapadung, G. Hanaoka, and H. Imai, “Time-specific encryption from forwardsecure encryption,” in Proc. 8th Int. Conf. Security Cryptography Netw., 2012, pp. 184–204.

18. P. Jamshidi, A. Ahmad, and C. Pahl, “Cloud migration research: A systematic review,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 142–157, Jul.–Dec. 2013.

19. P. Tysowski and M. Hasan, “Hybrid attribute- and re-encryption based key management for secure and scalable mobile applications in clouds,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172– 186, Jul. 2013.

20 P. Tysowski and M. Hasan, “Hybrid attribute- and re-encryption based key management for secure and scalable mobile applications in clouds,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172– 186, Jul. 2013.

21. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, “Vanish: Increasing data privacy with self-destructing data,” in Proc. 18th USENIX Security Symp., 2009, pp. 299–315.

22. R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, “Toward efficient and privacy-preserving computing in big data era,” IEEE Netw., vol. 28, no. 4, pp. 46–50, Jul./Aug. 2014.

23. Rose Mistry (2014) “Introducing Microsoft SQL Server 2014” Microsoft Press S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. 29th IEEE Int. Conf. Comput. Commun., 2010, pp. 1–9.