ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on KP-TSABE Architecture for Secure Data Sharing and Self Data Destruction in Cloud Computing

Chakkar Pandurang N., Khemnar Kiran C, More Prajakta D., More Varsha D.

B.E Student, Department of Information Technology, PREC, Loni, Ahmednagar, Maharashtra, India

ABSTRACT: There is need of higher security especially when we share sensitive data on cloud servers. In order to solve this problem, we propose a key-policy attribute-based encryption with time-specified attributes (KP-TSABE). It is a novel secure data self-destructing scheme in cloud computing.In the KP-TSABE scheme, every cipher text is labeled with a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text 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.

KEYWORDS: Key-Policy, Chipher Text, Authorization, Attribute Based Encryption(ABE).

I. INTRODUCTION

We propose 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 cipher text is labeled with a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text 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

II. REATED WORK

A. *ATTRIBUTE BASED ENCRYPTION*

Attribute-based encryption is one of the importantapplications of fuzzy identity-based encryption . ABE comes in two flavors called KP-ABE and cipher text-policy ABE (CP-ABE). In CP-ABE, the cipher text is associated with the access structure while the private key contains a set of attributes. Bethencourt et al. proposed the first CPABE scheme; the drawback of their scheme is that security proof was only constructed under the generic group model. To address this weakness, Cheung et al. presented anotherconstruction under a standard model. Waters used a linear secret sharing scheme (LSSS) matrix as a general set of access structures over the attributes and proposed an efficient and provably secure CP-ABE scheme the generic group model. To address this weakness, Cheung et al. presented another construction under a standard model. Waters used a linear secret sharing scheme (LSSS) matrix as a general set of access structures over the attributes and proposed an efficient and provably secure CP-ABE scheme.

B. *PHASES OF KP-TSABE ARCHITECTURE*

1. System setup:

   Setup(1k, u): This Algo generates system Params and Master key MSK.

2. Encryption with time constraint:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Encrypt(M, params, S, TS): To encrypt M to its cipher text CT, which is associated with the set S and TS. Finally, CT is sent to cloud servers.

3. Fine-grained access control during the authorizationPeriod:

KeyGen(MSK,Y, T′): To generate the private key SK and sends it to the user.

4. Decrypt(CT, SK): To decrypt CT to obtain the shared data M.
5. Data self-destruction after expiration.

III. PROPOSED SYSTEM

A. *APPREHENSION*

Encrypted cloud data can be shared using user defined authorization time period. Fine grain access control. Shared data will be self destroyed after user defined expiration time period. Asynchronous Attribute Based Encryption (AC-ABE) Scheme are used. 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. Comprehensive comparisons of the security properties indicate that the KP-TSABE scheme proposed by us satisfies the security requirements and is superior to other existing schemes.

B. *ARCHITECTURE*

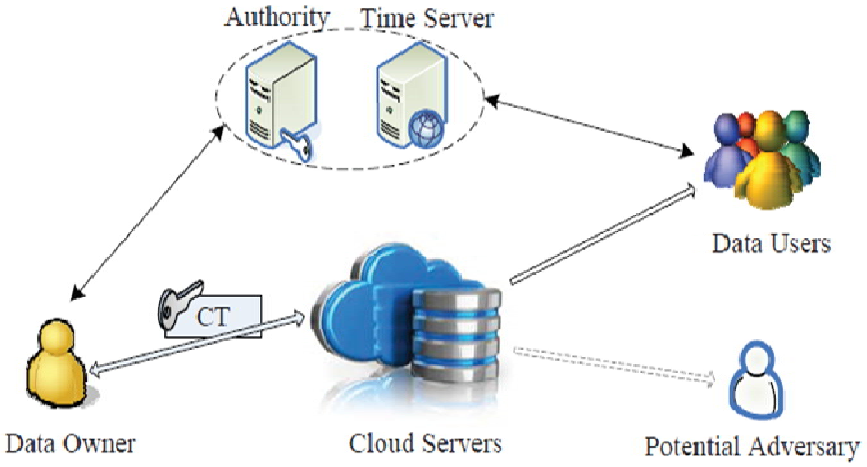

Figure 1: Architecture of KB-TSABE scheme

a) Data Owner. Data owner can provide data orfiles that contain some sensitive information, whichare used for sharing with his/her friends (data users). All these shared data are outsourced to the cloud servers to store.
b) Authority. It is an indispensable entity whichis responsible for generating, distributing and managingall the private keys, and is trusted by all theother entities involved in the system.
c) Time Server. It is a time reference serverwithout any interaction with other entities involvedin the system. It is responsible for a precise releasetime specification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

d) Data Users. Data users are some peoples whopassed the identity authentication and access to thedata outsourced by the data owner. Notice that, theshared data can only be accessed by the authorizedusers during its authorization period.
e) Cloud Servers. It contains almost unlimitedstorage space which is able to store and manageall the data or files in the system. Other entitieswith limited storage space can store their data tothe cloud servers.
f) Potential Adversary. It is a polynomial timeAdversary.

C. ***MODULES***

I. Register:

In This Module New User Register The Information In To Order Of The List For Client Purpose.

ii.Login:

In This Module User Can Login By Using his/her Name and Key

iii.Sensitive data:

As the-state-of-the-art of the secure self-destruction scheme, both SSDD and FullPP have some limitations. First, SSDD does not consider the issue of the desired release time of the sensitive data the expiration time of both SSDD and FullPP schemes is limited by the DHT network and cannot be determined by the user. Second, SSDD and many other schemes are dependent on the ideal assumption of "No attacks on VDO (vanishing data object) before it expires" . Third, it is demonstrated that the Vanish scheme is vulnerable to the Sybil attacks from the DHT network, the SSDD scheme and other schemes are similar. As a result, denoting that the encrypted data item can only be decrypted between The data owner encrypts his/her data to share with users in the system, in which every users key is associated with an access tree and each leaf node is associated with a time instant, The access tree of each user can be defined as a

iv. Secure self-destructing

A data self-destructing scheme, first proposed by Geambasu et al. [23], is a promising approach which designs a Vanish system enables users to control over the lifecycle of the sensitive data. Wang et al. improved the Vanish system and proposed a secure self-destructing scheme for electronic data (SSDD) [24]. In the SSDD scheme, a data is encrypted into a ciphertext, self-destructing scheme for data sharing in cloud computing. We first introduce the notion of KP-TSABE, formalize the model of KP-TSABE and give the security model of it. Then, we give a specific construction method about the scheme. Finally, we prove that the KP-TSABE scheme is secure.

v.Fine-grained access control

In order to implement fine-grained access control, we associate every attribute in the attribute set with a time interval (authorization period). The attribute is valid if and only if the current time instant is in this time interval. Only if the valid attribute in the ciphertext satisfies the access tree in the key, the algorithm can decrypt the message correctly. The algorithm level of the KP-TSABE scheme includes four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

vi.Privacy-preserving

Due to the lack of time constraints, the above-mentioned ABE schemes do not support user-defined authorization period and secure self-destruction after expiration for privacy-preserving of the data lifecycle in cloudcomputing. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment [5]. 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.

vii.Cloud computing

Tysowski et al. modified the ABE and leveraged re-encryption algorithm to propose a novel scheme to protect mobile user's data in cloud computing environment [1]. Due to the lack of time constraints, the above-mentioned ABE schemes do not support user-defined authorization period and secure self-destruction after expiration for privacy-preserving of the data lifecycle in cloud computing. It is a time interval from the creatiof the shared data, authorization period to expiration time. This paper provides full lifecycle privacy protection for shared data in cloud computing.

D. ***SCOPE OF PAPER***

It can be applicable where main goal is to share the secret data among geographically distributed clients of cloud services across multiple storage servers by keeping the confidentiality of the data. It is used to improve the reliability

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

and Security of client's outsourced data. The various organizations or Industries can use these applications to protect their dataset from unauthorized access.

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 .
[2] Luca Ferretti, Michele Colajanni, and Micro Marchetti,Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.
[3] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, Depot: Cloud Storage with Minimal Trust, ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.
[4] E. Mykletun and G. Tsudik Aggregation Queries in the Database-as-a-Service Model, Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.
[5] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, Database Management as a Service: Challenges and Opportunities, Proc. 25th IEEE Intl Conf. Data Eng., Mar.-Apr. 2009.
[6] L. Ferretti, M. Colajanni, and M. Marchetti, Supporting Security and Consistency for Cloud Database, Proc. Fourth Intl Symp. Cyberspace Safety and Security, Dec.2012.