International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 8, August 2015

A Highly Secure Data Self-destructing Scheme in CLOUD COMPUTING

[1]Keerthana.A, [2]Mounica Chandrasekhar, [3]Pruthvi Sai
[1][2][3]Department of Computer Science and Engineering
R.M.K. Engineering College, Kavaraipettai, Thiruvallur dist. India
[1]keerthana151094@gmail.com,[2]mounicreddy@gmail.com,[3]pruthvisai.24@gmail.com

Abstract: **The utilisation of cloud services in today's technological field is booming. People increasingly use cloud services for the purpose of sharing data. Hence there is a need to secure the sensitive data that is being shared through cloud servers. Providing a full life-cycle privacy security is not feasible, as it does not allow for access control. In order to provide a solution for this problem we put forward 'key-policy attribute-based encryption with time specified attribute'- a secure data self destructing scheme which can be implemented in cloud servers so as to provide complete security to the sensitive data that is being transferred via cloud services. In this scheme, every cipher-text is associated with a time interval while private key is associated with a time instant.It is possible to decrypt the cipher-text only if both the time instant is within the specified time interval and the attributes associated satisfy the access structure of the key. The major advantage of this scheme over others is that it supports user-defined authorisation period and provides a fine-grained access control. The sensitive data gets self-destructed when the user specified time gets expires.**

Key words- **cloud computing, self-destructed, access control, sensitive data,cipher-text,user-defined authorization**

I. INTRODUCTION

Cloud computing is pervasively transforming the Information technology sector.There is a rapid development in this field of research. People in this era use cloud services to share data e.g., Google drive, Dropbox etc. However the shared data in the cloud servers contains user sensitive information (i.e) personal details, banking details, medical records,etc. Hence these data needs to be well protected.

In cloud services however the owner of the data is isolated from those who administer the data.The cloud servers may transfer the users data to other cloud servers as a result of outsourcing or sharing them during cloud searching.Thus it becomes a challenging task to provide security especially in cross-cloud and big data environments.To overcome this challenge, a comprehensive solution that allows for user-defined authorisation and fine-grained access control is necessary and the shared data must be self-destructed after the expiration time.

To alleviate this problem is to store data as a common encrypted form, but encrypted data cannot be shared at a fine-grained level.When a use wants to share his information, he must know exactly the one with which he wants to share the data.In some scenarios the user wants to share his data with multiple other users.Public key encryption may prove significant for one-to-one encryption whereas Attribute-based encryption has a flexibility in that it can also be extended for one-to-many encryption.Thus, Attribute-based encryption scheme is a significant method to achieve both data security and fine grained access control. In this method a set of descriptive attribute is associated with the cipher-text . Only when this set of descriptive attributes satisfy the key's access structure, the user will be able to view the plain-text.

II. Drawbacks of Convention method

Usually, it will be possible to specify that certain sensitive information will be valid only for a limited period of time by the user, or should not be made available before a particular time, Example for this can be Internet Programming Contest.

However applying Attribute Based Encryption will lead to several problems regarding to time-specific constraint and self-destruction. If we apply Time Specific Encryption it will lead to problem with fine-grained access control.The conventional method thus fails to provide a fine-grained access control within the cloud computing environment.

The main problem to be explored is how to achieve the time-specified cipher-text into a fine-grained access control.In this paper we attempt to solve these problems using the 'Key-policy attribute based encryption with time specified attribute'.

III. MOTIVATION

Secure Self-Destructing Scheme for electronic data(SSDD) and Full life-cycle privacy protection scheme for sensitive data(FullPP) both have some limitations. SSDD scheme does not take into account the issue of the desired release time of the sensitive data and both the schemes is limited by the Distributed Hash Table(DHT) network which does not give the user the control to release time of the data.

It is illustrated that the vanish scheme is vulnerable to Sybil attacks from the DHT network.As a repercussion of such attack, unauthorised user can easily gain access to the sensitive data which in turn will leads to a serious privacy disclosure.

To overcome this limitations, we propose a solution called 'Key-policy based encryption with time-specified attribute' scheme.

IV. KEY-POLICY BASED ENCRYPTION WITH TIME-SPECIFIED ATTRIBUTE

This scheme is based on the observation that in a practical cloud application scenario, each data item had an associated set of attributes and every attribute is associated with a time interval which is known as the 'Decryption Attribute Time Interval'.Example [13.00 to 15.00] means that the data item can be decrypted only in the specified time interval on the specified date, and is not available before or after the specified time interval and the data item will be self-destructed after the specified interval expires.

To share data with the users, the owner first encrypts the data. The users of the system is associated with an access tree and each leaf node is associated with a time-instance eg. [14.45]. To succesfully decrypt the cipher-text, the valid attribute should satisfy the access tree, where the time instance of each node in the user should be within the Decryption Attribute Time Interval Example [14.45] belongs to the time-interval[13.00 to 15.00] which was specified by the user.If suppose the time-instance is not present in the specified time-interval, the user will not be able to decrypt the data. Thus this scheme gives the user the access level control.

V. ADVANTAGE OF THIS SCHEME

- This scheme provides for user-defined authorisation period and ensures that the sensitive data cannot be read prior to the release time or after its expiration.
- It is able to implement fine-grained access control during authorisation period and it also does not require any human intervention to make the sensitive data to get self-destructed after expiration time.
- It does not require the ideal assumption that 'No attacks on the VDO(Vanishing Data Object) before it expires'.

VI. COMPREHENSIVE COMPARISON

This model is secure under the standard model. Let us compare this scheme with other existing self-destruction scheme (Eg. SSDD, FullPP etc.)

- *Prerequisite condition :*

All the other schemes need the ideal assumption that "no attack on VDO before it expires". But this scheme requires no such prerequisite condition which gives an edge to this scheme.

- *Algorithm and Resistance on Attack:*

SSDD and Vanish uses symmetric encryption technique to encrypt the sensitive data, this kind of encryption brings about complex key management and cannot achieve fine-grained access control. Although these method can resist against complex cryptanalysis, they are still prone to Sybil attack.

Key-policy based encryption with time-specified attribute is resistant to Sybil attack as it does not make use of the DHT network. It can also provide fine-grained access control.

- *User-defined Authorisation period:*

In other conventional method the expiration time of the sensitive data is limited by the update period of the DHT network and does not give the data owner control to their sensitive data.

Whereas in this scheme,each data item had an associated set of attributes and every attribute is associated with a time interval, which is the authorisation period and it is pre-defined by the user, which places the owner in full control over their sensitive data.

- *Security Proof:*

The other existing methods do not provide us with security proof. Whereas Key-policy based encryption with time-specified attribute scheme proves to be secure under the standard model with *l*-expanded BDHI assumptions to resist against the traditional cryptanalysis and the collusion attack.

Thus in comparison with the above mentioned properties 'Key-policy based encryption with time-specified attribute'

scheme is superior to all the other existing self-destruction schemes.

CONCLUSION

As the utilisation of cloud services in today's technological field has become inevitable, the security challenges should given much importance. Mainly the outsourced data stored in cloud servers should be securely deleted. Hence we proposed '*Key-policy based encryption with time-specified attribute*' scheme which is able to achieve the secure self-destruction of data and also provides the user with the fine-grained access control. The comprehensive analysis clearly indicates that the proposed 'Key-policy based encryption with time-specified attribute' is superior to all other existing schemes.

REFERENCES

- B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditingfor shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014
- 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
-] 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.
- K. G. Paterson and E. A. Quaglia, "Time-specific encryption," in Security and Cryptography for Networks. Springer, 2010, pp. 1–16
- J. Reardon, D. Basin, and S. Capkun, "Sok: Secure data deletion," in Proceedings of the 34th IEEE Symposium on Security and Privacy. IEEE, 2013, pp. 1–15.
- J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, "A secure selfdestruction scheme with ibe for the internet content privacy," Chinese Journal of Computers, vol. 37, no. 1, pp. 139–150, 2014.