International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Self-Destructing Scheme in Cloud Computing for Data Security

Sangita B. Chavan† and Ashish Kumar‡*

†Raisoni College of Engineering Ahmednagar, Savitribai Phule Pune University, India
‡G.H. Raisoni COE, Ahmednagar, Savitribai Phule Pune University, India

Accepted 01 Jan 2016, Available online 02 Jan 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

Cloud computing have been playing very vital role in the rapidly growing organizations. It becomes mostly susceptible to use cloud services to share data between organizations, electronic businesses and a friend circle in the cloud computing environment. Because of the fastest development in electronic business by using the various cloud services, it is very difficult to provide full lifecycle privacy security and access control becomes a very tedious task, specifically when sharing the sensitive data on cloud servers for achieving the anytime, anywhere service for authentic person or organization. Also for sharing purpose we need efficient method and secure technique over cloud services. In order to grab this problem the key-policy attribute-based encryption with time-specified attributes KP-TSABE, which is focus on data security over specific time period and proposed new proxy re-encryption technique for providing full lifecycle privacy security solution(Jinbo Xiong et al, 2014). We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems in which new re-encryption schemes that realize a stronger notion of security.

Keywords: *Sensitive Data, Cloud Computing, privacy-preserving, fine-grained access control*

Introduction

Today's business applications hardly work in isolation manner; they need many numbers of applications to interaction to complete business requirements. The customer and clients is believed in the instant access to all business applications which offered by an enterprise, without worrying about which systems provides the functionality at anytime and anywhere (24x7). The cloud computing is playing very important role in business now a day.

The electronic business is becoming more and more dynamic which experiencing the major changes, since the market is in hurry to develop of new systems, databases, technologies for providing or adding efficient and dynamic nature to electronic business. As per IDC (International Development Corporation) survey todays around 70 to 80 percent of electronic data generated in last two to three years, most significant think is maximum data is very sensitive with respect to organization and person.

Cloud Computing is also called as the on-demand computing because of its features anytime, anywhere, as per your requirement with pay per use features. It is considered as modern way of evaluation on-demand information technology which combines a set of new and existing technologies from exploration areas such as Virtualization and service-oriented architectures (SOA). With the hurried development of flexible cloud computing technology and services, it is routine for users to control over the cloud storage services to share data with others in a friend circle such as Google Drive and Dropbox.

Fig. 1 Cloud Computing

Cloud computing is shortly referred as “Cloud”. It is way of delivering on demand services and resources. Everything from the data centers, servers, bandwidth,

*Corresponding author **Ashish Kumar** is working as Assistant Professor and **Sangita B. Chavan** is a M.E. Scholar

services, applications over internet and greatest thing about it we have to pay as per use of services and resources. It has provided elastic resources for scale up and down quickly and easily to meet the demand of business. As per your business need you can demand public, private and hybrid cloud.

When we are using the word "Moving to Cloud", means we have shifted existing services or data to cloud computing but whenever moving information to cloud information can be very sensitive (Organization business profile, financial information, client records, personal information) and need to be restricted only authentic organization and friends. But restriction to sensitive information in shared data in cloud is very big challenge. Sometimes need to migrated data from one cloud to other cloud for outsourcing and share it for cloud searching, so that it very big challenge to provide the sensitive data security in cloud. It mostly becomes very tedious task for security in big data environment and information in cross cloud.

One of the solutions for providing authenticity to sensitive data is self-expiration time and fined-grain access control. The sensitive and shared information should be destruct itself after expiration time provided by user and also providing re-encryption technique for providing full lifecycle privacy to the sensitive information.

One of the techniques for protecting data from unauthorized access is to store the sensitive information in the encrypted form. But the disadvantage for encrypting data is that the user cannot share his/her sensitive encrypted data at a fine-grained level. When the data holder wants to share data with someone, the information owner should have known the exactly one wants to share his/her sensitive information.

Literature survey and related work

There are many techniques available for protecting information in cloud and each technique has its own advantages and disadvantages. Cloud computing has been providing various and versatile services for sharing information over the internet for electronic business as well for personal use from anywhere and anytime. The main task is providing protection to shared data.

Traditional Encryption

This is one way to protecting shared information on cloud by encrypted data. There are so many disadvantages to this traditional encryption are easily decrypted and we cannot shared the encrypted data in fine-grained level. Also very difficult task during sharing the information, data owner should know the information of his/her. In traditional way of encryption is the technique for one to one encryption is done only (Jinbo Xiong *et al*, 2014).

Attribute Based Encryption (ABE)

Attribute Based encryption has so many advantages over the traditional way encryption. ABE has supported flexible one to many encryption instead of one to one encryption like traditional technique. It also provides fine-grained access control for sharing encrypted data to cloud. This scheme of encryption provides powerful and efficient data security as compare to traditional way of encryption.

It is based on the fuzzy identity-based encryption. There are two flavors of ABE such as KP-ABE and cipher text-policy ABE (CP-ABE). In CP-ABE, the cipher text is related with the access structure while the private key contains a set of attributes. In KP-ABE, when a user made a secret request, the trusted authority determined which combination of attributes must appear in the cipher text for the user to decrypt (Jinbo Xiong *et al*, 2014).

Secure Self Destruction Scheme (SSDS)

It is one of the familiar methods for achieving security for the sensitive data is deletion of sensitive information after its expiration whenever data was used. In this scheme data is encrypted into cipher text, after which is associated and extracted to make it incomplete for resist against brute-force attack and traditional cryptanalysis. Then both extracted cipher text and decryption key are distributed into the DHT (Distributed Hash Table) network for implementing self-destruction after updating period of DHT (Jinbo Xiong *et al*, 2014).

Time-Release Encryption (TRE)

The owner of sensitive information has rights to specify limited period of time or should not release before the particular time. It is one of the interesting encryption scheme in which encryption key is associated with the predefined release time and receives only after constructing decryption key with time instance.

Time-Specific Encryption (TSE)

Time Specific Encryption is provides time intervals such that cipher text can only be decrypted in the particular interval. This technique is used in many applications such as internet programming contest, electronic sealed bid auction etc. It is extension of Time Release Encryption. In TSE the time server is broadcast the time instant key (TIK), the information owner can encrypt data into time interval and decrypt cipher text if time instance key is valid in the interval.

Motivation

As the state of art, sharing sensitive information on cloud, require huge amount of security. There are so many techniques available for providing security to

shared data but each method has some limitations to achieve the highest amount of security. The sensitive shared data is motivated to add extra security to existing method.

KP-TSABE Scheme

KP-TSABE is secure self-destructing scheme for data sharing in cloud computing for achieving powerful and efficient privacy of shared data between authentic users and organizations. The following diagram shows the system model for KP-STABE.

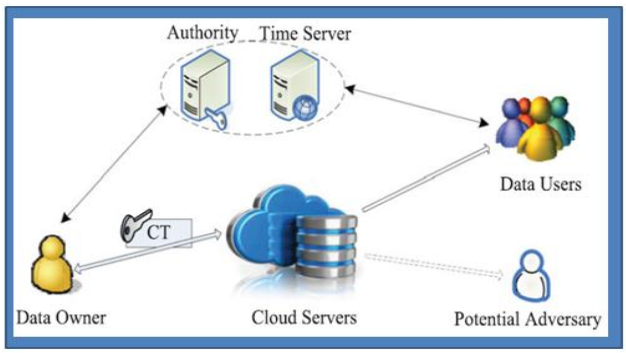

Fig. 2 System Model KP-STABE (Jinbo Xiong *et al*, 2014)

KP-STABE has various advantages overs the other security techniques of shared data.

- KP-STABE provides the user-defined authorization period and provides constraints on the sensitive data cannot be read before the particular release time and its expiration time.
- KP-STABE does not require the ideal assumption of "No attacks on VDO (Vanishing data objects) before its expires"
- KP-STABE has provided the fine-grained access control during the authorization period and its make sensitive data self-destruction after expiration of time without human intervention.
- Proxy re-encryption key provides the full lifecycle security.

In system model primarily focus on the achieving fine-grained access control during the authorization period of shared data in the cloud and also how to achieve the self-destruction scheme of data after its expiration owner defined time.

Conclusion

The electronic business is rapidly growing and cloud computing is modern step for electronic business for providing on demand service with pay as per use facilities. The shared data contains the sensitive information and need to provide full lifecycle privacy to sensitive data. There are so many schemes available but each one have own merits and demerits. KP-STABE provides the highest amount of security and fine-grained access control. Also re-encryption adds security level for shared data in cloud computing.

Acknowledgment

I would like to sincere thanks to the peoples who support and help.

References

Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen (2014), A Secure Data Self-Destructing Scheme in Cloud Computing, *IEEE Transaction on Cloud computing*, 2(4) pp. 448-458.

B. Wang, B. Li, and H. Li, (2014), Oruta: Privacy-preserving public auditing for shared data in the cloud, *IEEE Transactions on Cloud Computing* , 2(1), pp 43-56.

J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma (2014 Priam: Privacy preserving identity and access management scheme in cloud, KSII Trans. Internet Inf. Syst., 08(01), pp 282-304.

J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, (2014), A full lifecycle privacy protection scheme for sensitive data in cloud computing, *Peer-to-peer network Appl.*

P. Jamshidi, A. Ahmad, and C. Pahl (2013), Cloud migration research: A systematic review, *IEEE Trans. Cloud Comput.* 01(02), pp 142-157.

Biography

Author 1: Sangita B. Chavan is pursuing Master of Engineering with specialization in Computer network from Raisoni College of Engineering Ahmednagar under Savitribai Phule Pune University, Pune. She is working as Lecturer in Government Polytechnic Ahmednagar.

Author 2: Prof. Ashish Kumar is working as Assistant Professor in G. H. Raisoni college of engineering and Management, Ahmednagar.