A Review on Cloud Key Management Framework with Email Searching Using SC-PRE

Prof. A. K. Hase[1], P.M.Gund[2]

[1] Assistant Professor, Computer Engineering Department, PREC Loni, Maharashtra, India
[2] Student, Computer Engineering Department, PREC Loni, Maharashtra, India

ABSTRACT

Generally, every web based application required users credentials such as, username and password to preserve their identity. From both credentials password is more secure entity to preserve user's sensitive data. Also data owner encrypts their before outsourced it on cloud. As there is huge growth in the use of web application as well as outsourcing of data the number of passwords for web applications and data encryption keys for outsourcing data also get an exclusive growth. Hence, data storage exceeds the management limit of user's passwords and encryption keys. Many types of solutions have been proposed in the literature for data outsourcing keys unable to meet the requirements (i.e., privacy & confidentiality of keys, search privacy on identity attributes tied to keys and owner controllable authorization over his shared keys) regarding security of outsourcing keys.

Keyword : - *SC-PRE, search privacy, key management, keys outsourcing*

1. INTRODUCTION

Outsourcing of data is the common trend in information technology and other industries. Many business organizations outsourced their data for managing a business and serving internal and external customer. At other side there is extreme growth in the web development users are attracted towards the web application such as, online banking, shopping (i.e. Amazon, snapdeal etc.), GoogleDrive for online management of documents. To serve all these facilities of web application user primarily have to create their accounts in which their all activity logs get saved as well as security is maintained for all kind of online transactions. With growth in the use of web applications the numbers of password and encryption keys also get increased. Key management is very tedious task as user has multiple accounts for different web applications. However, the weak and shared passwords across accounts make them easy to be compromised, which in turn leaks more passwords related to private and sensitive data. According to the analysis from literature survey 14% of student's uses web based password managers to maintain and manage their passwords and encryption keys. A password manager enables them to select a unique password for different application sites (i.e. for web applications). In the year of 2011, Lastpass is the most successive web based password manager used by millions of users. As per the analysis of paper [2], 85% of peoples outsourced their data as well as encryption keys to the cloud have privacy problems. There is a promising solution used to preserved privacy of outsource keys is the encryption of keys before outsource them. This is due to two situation such as, user do not fully trust the service providers because there is no governance about how keys can be used by them and whether the key owner can actually control their keys on their own and they may trust the service providers, but keys could be disclosed if there exists an misbehaving internal employee or broken server. Solution for this issue is to encrypt outsourced keys as like encrypting outsourcing data. It is promising solution to maintain trust and to ensure key owner's control over their own privacy. Key encryption is minor different than the usual data encryption as key encryption is made on different privacy requirement such as, identity attribute, key attributes etc. In this paper, we proposed cloukeyBank approach with implementation of Searchable Conditional proxy Re- encryption (SC-PRE). It is cryptographic primitive which integrates the techniques of hidden vector encryption (HVE) and proxy re-encryption (PRE). The proposed SC-PRE also solves existing problems of key tuple encryption. In this we do not required to encrypt each tuple. Firstly, each tuple is divided into multiple attribute groups in terms of dependence relationship between attribute groups. A dual authorization token is included to achieve minimum information leakage in the process of privacy and owner controllable authorization. User with appropriate token will get access to the keys for retrieving data. CloudKeyBank provider not able to see an encrypted data stored in the key database but it can provide an efficient query search over an encrypted data by evaluating the query against each encrypted tuple. Our security analysis proves that the cloudkeyBank can efficiently support to the search privacy, key privacy and owner controllable authorization.

In the below sections we are going to discuss about related workdone for the proposed research area. We refer some existing research paper for completing this task. It is given as follow:

2 RELATED WORK

.

2.1 H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proc. 18th Int. Conf. Data Eng., 2002, pp. 216–227

H.Hacigumus, B.Lyer et al [1], proposed a technique to protect data from service providers if providers themselves not be trusted. They explore the techniques to execute SQL queries over an encrypted data. In this paper proposed strategy process much of SQL queries without decrypting the data. The remainder required for query processing as well as data decryption is placed at client side. The technique deploys the "coarse index" which allows the partial execution of SQL query on the provider side. In this paper the service provider retains the responsibility to manage the persistence of the data. Therefore, client does not require managing data persistence, thus the continuous to benefits from the system management service of the database service providers. To guarantee privacy and access authorization of outsourced data, data owners employ different cryptographic techniques to encrypt data so as to implement different goals of privacy protection. An experimental result only guarantees the confidentiality and privacy of keys but does not consider the key authorization and the different privacy requirements of sensitive attributes in key tuples.

2.2 X. Tian, X. Wang, and A. Zhou, "DSP re-encryption a flexible mechanism for access control enforcement management in DaaS, in Proc. IEEE Int. Conf. Cloud Comput., 2009, pp. 25–32.

X. Tian and X. Wang [2], introduced a challenging issue of access control management by the database service providers (DSP). They proposed an approach to implement the flexible access control enforcement management by applying a DSP re-encryption mechanism. In the proposed method user does not required much computations. User can use their private key to decrypt all authorized data tuples. In this approach dynamic policies are update and manage whenever a revocation operation takes places. Moreover in this paper a new architecture still satisfies the secure performance of the confidentiality and can reduce the computation complexity of the client by eliminating the public catalog of tokens. In this paper subsequent researches under the new architecture are on how to design the efficient query transformation function in the client, the additional mechanisms such as the integrity and query guarantee in the DSP and the efficient implementation of role-based and the secret share based DSP re-encryption mechanisms.

2.3 J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in Proc. 12th Int. Conf. Practice Theory Public Key Cryptography, 2009, pp. 357–376

J. Shao, z. Cao et al [3], discussed about C-PRE scheme. It is conditional proxy re-encryption where only ciphertext satisfying a specific condition set by one user can be transformed to the proxy and then decrypted by another user. Author extended the C-PRE method the MC-PRE to satisfy multiple conditions. It supports AND gates on conditions. Problem with this system is it cannot support CCA-secure C-PRE schemes with anonymous conditions or supporting more expressive predicates.

2.4 M. Li, S. C. Yu, N. Cao, and W. Liu, "Authorized private keyword search over encrypted data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 383–394

M. Li, S. Yu et al.[4], addressed the problem of APKS i.e. authorized private searches over an encrypted PHR's in the cloud computing where multiple PHR owners encrypt their health records along with a keyword index to allow searches by multiple users in the public domain. To limit the exposure of sensitive patient health information from unrestricted query capabilities they proposed a scalable, fine-grained authorization framework where users obtain their search capabilities from local trusted authorities according to their "eligible attributes". There are two approaches have been proposed in this paper as solutions for APKS over encrypted PHR based on HPE. The proposed solutions also enjoy the advantages of supporting multi-dimensional multi-keyword query, search capability delegation and efficient revocation.

2.5 N. Shang, F. Paci, M. Nabeel, and E. Bertino, "A privacypreserving approach to policy-based content dissemination," in Proc 26th Int. Conf. Data Eng., 2010, pp. 944–955.

N. Shang, et al [5], introduced document broadcasting approach. It is based on access control policies specifying which users can access which documents, or subdocuments. This approach is supported by new group key management scheme which is secure and allows qualified subscribers to efficiently extract decryption keys for the portions of documents they are allowed to access, based on the subscription information they have received from the document publisher. It can efficiently manages the joining and leaving of subscribers with security guarantee. Furthermore, they were planning to focus on scalability and optimization issues.

2.6 M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public clouds," IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, pp. 2268–2280, Sep. 2014

M. Nabeel et al [6], proposed based on two layers of encryption which gives assures data confidentiality from cloud and delegate the enforcement of fine-grained access control to the cloud. They addressed a challenging issue of decomposing access control policies i.e. ACP. In cloud technology security and privacy are the major concerns. Encryption assures the confidentiality of data against cloud. The previous approaches of encryption not sufficient to support the enforcement of fine-grained organizational access control policies. The proposed approach is based on a privacy preserving attribute based key management scheme. It preserves users privacy at the time of enforcing attribute based ACPs. A single layer encryption (SLE) approach is introduced by them to enforce access control via encryption. SLE addressed all the limitations of existing techniques but still requires enforcing all the ACPs by fine-grained encryption.

2.7 X. X. Tian, L. Huang, Y. Wang, C. F. Sha, and X. L. Wang, "DualAcE: Fine-grained dual access control enforcement with Multi-privacy guarantee in DaaS," Secure Commun. Netw., vol. 8, no. 8, pp. 1494–1508, 2015

X. Tian, L. Huang et al [7], proposed attribute based encryption. It is implemented for fine-grained access control in DaaS. It supports data privacy, policy privacy and key privacy issues. The proposed approach gives the privacy guarantee against any of the malicious parties, such as only the curious DSP or malicious user. The proposed scheme provides guarantee of multi-privacy such as, identity attribute privacy, data privacy and attributed conditions privacy in ACP. The proposed approach provides the guarantee of any malicious parties. For the flexible attribute set combination they also introduced ASBE. In further future work, they were planned to develop hierarchy-based administrator domain and create efficient grant mechanism for accomplishment of distributed access control.

2.8 M. Li, S. C. Yu, N. Cao, and W. Liu, ”Authorized private keyword search over encrypted data in cloud computing,” in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 383–394.

M. Li, S. Yu et al [8], focused on “multi-owner” setting. Data in encrypted format were outsourced by data owner and it can be searched and retrieved by multiple users. With the encrypted data there is a challenging issue of search keyword. In this paper, they addressed the problem of authorized private keyword searches over encrypted data where multiple data owners encrypt their records along with a keyword index. Multiple users can search encrypted records on cloud. A scalable, fine-grained authorization framework is also proposed by them to restrict exhibition of sensitive information which occurred due to unbounded capabilities of query. Two novel solutions have been proposed in APKS based on HPE over an encrypted data. APKS enhances search efficiency using attribute hierarchy. The proposed solution supports the multi-dimensional range query, search capability delegation and revocation.

2.9 G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proc. 12th Annu. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–44.

G. Ateniese et al [9], proposed atomic proxy re-encryption application. In this semi-trusted proxy converts a ciphertext for one user into a ciphertext for other user without seeing the underlying plaintext. They predicted that the proposed approach is faster and secure re-encryption. They have used bilinear maps to improve re-encryption schemes.

3. SYSTEM ARCHITECTURE

CloudKeyBank architecture consists of four entities.

1. Key owner: Key owner is data encryption key owner who outsources his/her encrypted key database (Key DB) to the CloudKeyBank provider. After that the encrypted key database (EDB) stored in CloudKeyBank provider can be accessed anywhere and anytime with minimum information leakage such as the size of Key DB. The key owner mainly completes the following three tasks: 1) Constructing the customized access control policy (ACP). 2) Depositing Key DB by using DepositKey protocol. 3) Distributing authorized Query tokens to the delegated users.

2. CloudKeyBank provider: CloudKeyBank provider completes the two tasks: 1) To enforce the privacy of identity attributes in the Search attribute group, he/she can perform search query directly by evaluating the submitted Query token against the encrypted key tuples in EDB; 2) To enforce the key authorization he/she can transform an encrypted key into the authorized re-encrypted key under the corresponding Delegation token stored in Authorization Table (AuT).

3. Trusted client: Trusted client is the primary privacy enforced component in CloudKeyBank framework. It mainly consists of two protocols: Deposit Key and Withdraw Key.

4. User: Two types of users can be included in proposed system Key owner and Collaboration group. Key owner corresponds to an individual user who deposits all his keys to CloudKeyBank provider and accesses them by himself. Collaboration group corresponds to a group of users where the key owner can share his/her keys with other users within the same collaboration group. By submitting the private key and authorized Query token, a delegated user can withdraw an authorized key by using Withdraw Key protocol under the support of privacy enforced access control policy.

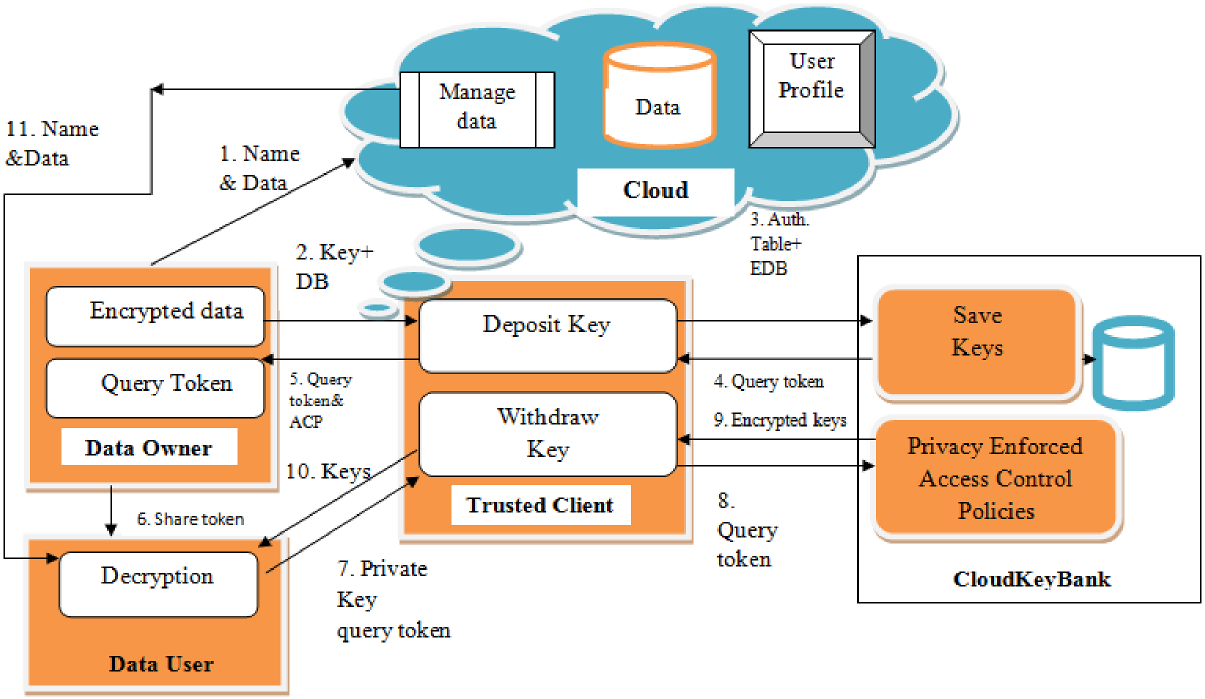

Figure-1: System Architecture

3. PROBLEM FORMULATION

There is huge growth in outsourcing of data in encrypted format. Encryption keys have to be preserved on cloud hence there is need of efficient key management which is a complex task as there is vast growth in keys as outsourcing data storage exceeds the management limit of users. Also there is need of such system which can preserves the privacy & confidentiality of keys, search privacy on identity attributes tied to keys and owner controllable authorization over his shared keys.

4. CONCLUSIONS

Multiple methods have been proposed in the literature survey regarding to outsourcing of data which are unable to meet the security requirements of outsourced keys. Therefore, in this system we identified the problem of security requirements for outsourcing keys such as, to preserve confidentiality and privacy of keys, owners controllable authorization and Search privacy on identity attributes tied to keys. For efficient key management we introduced cloudkeyBank framework. It is represented by implementing novel scheme SC-PRE and comparative analysis of security requirements of key outsourcing. In experimental analysis, we have show that proposed solution can be a worth solution for previously discussed security problems.

5. REFERENCES

[1] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, “Executing SQL over encrypted data in the database-service-provider model,” in Proc. 18th Int. Conf. Data Eng., 2002, pp. 216–227

[2] X. Tian, X. Wang, and A. Zhou, “DSP re-encryption a flexible mechanism for access control enforcement management in DaaS, in Proc. IEEE Int. Conf. Cloud Comput., 2009, pp. 25–32.

[3] J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in Proc. 12th Int. Conf. Practice Theory Public Key Cryptography, 2009, pp. 357–376

[4] M. Li, S. C. Yu, N. Cao, and W. Liu, "Authorized private keyword search over encrypted data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 383–394

[5] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public clouds," IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, pp. 2268–2280, Sep. 2014

[6] N. Shang, F. Paci, M. Nabeel, and E. Bertino, "A privacypreserving approach to policy-based content dissemination," in Proc 26th Int. Conf. Data Eng., 2010, pp. 944–955.

[7] X. X. Tian, L. Huang, Y. Wang, C. F. Sha, and X. L. Wang, "DualAcE: Fine-grained dual access control enforcement with Multi-privacy guarantee in DaaS," Secure Commun. Netw., vol. 8, no. 8, pp. 1494–1508, 2015

[8] M. Li, S. C. Yu, N. Cao, and W. Liu, "Authorized private keyword search over encrypted data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 383–394.

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. 12th Annu. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–44.

[10] Xiuxia Tian, Ling Huang, Tony Wu, Xiaoling Wang ,"CloudKeyBank: Privacy and Owner Authorization Enforced Key Management Framework", IEEE transaction on knowledge and data engineering, dec.2015,vol.27, no.12