International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

A CloudKeyBank: Privacy and Owner Authorization Enforced Key Management Framework

Darshan Chavan, Prof. P. M. Yawalkar

[1]*PG Student, Department of Computer Engineering, MET's institute of Engineering, Nashik, Maharashtra 422003*
[2]*Professor, Department of Computer Engineering, MET's institute of Engineering, Nashik, Maharashtra 422003.*

Abstract - *With the limited computing power cloud permit users to outsource their data. However, a security issue has been always obstacle to the use of computing outsourcing. Recently, there is huge growth in the use of number of security passwords for web based application and encryption keys required to securely outsource the data. User encrypts the data using encryption before uploading it on cloud and provides access rights to the other user i.e. shared data with other authorized users of cloud. While uploading data to the cloud data owner also have to outsource their password and data encryption keys to CSP. Such outsourcing of password and encryption keys attracts attention of many users with security and privacy point of view. Users don't have fully trust on CSP as they don't have guidance of how to access and manage user's keys. This is the main reason behind that user worried to outsource their important information on cloud. Previously existed systems are not much intelligent to preserve data integrity, privacy policy of searching etc. To make efficient management of user private data as well as to securely preserve user's data encryption keys on cloud there is need of such system which provides the guarantee of security and privacy to the end user for their outsourcing data and for proper key management. Bloom filter is space-efficient probabilistic data structure designed to specify whether an element is present or not in the set. It is rapid and memory efficient strategy which we contribute in our proposed work. It can save search space and time of searching as it does not require too many transactions to the database as frequent data stored in cache.*

Key Words: SC-PRE, search privacy, key management, keys outsourcing.

1. INTRODUCTION

In web development software and the databases are preserved on central server instead of installed on the desktop system. It is accessed over network. In this era, web applications are straight forward way to take the benefit for enhancing organizations efficiency and productivity. Web development deploys 'n' number of applications such as, social networking (Facebook, twitter, linkend), shopping sites (Amazon, eBay, snapdeal etc) and data storages such as, google drive. To preserve user's identity this site provides user registration and login facility so that only authorized user can get access to further content of site. User belongs to number of sites for various purposes hence he has to maintain their password for every web application. Recently, users are attracted to store their data on cloud server to make proper management of it. Users save their data on cloud in encrypted format for privacy point of view, for this task user also has to maintain multiple of data encryption keys. According to the survey, around 14 percent of students use web based password managers to manage their password. Password managers enables user to choose complex and unique password for multiple different web-based applications. Generally user refers to centralized key management providers as they want relief from vast concern of memorization and management. Password replacement technique introduced in [2], it provides miner security benefits beyond traditional password. Many users do not trust on centralized key management providers as they don't have guidance of how to access and manage user's keys. This is the main reason behind that user worried to outsource their important information on cloud. And the other hand some service providers exposes the keys if any employee misbehave with them. There are many conventional scenario supports for some security requirement, most emerged technology ASP i.e. application service provider provides software as service to client over an internet. Some re-encryption techniques address the problem of enforcing access control such as DSP makes the system more usable. DSP-re-encryption technique satisfies the security confidentiality and reduces the computation complexities. Encryption of key is same as the encryption of data tuple before upload it on cloud server. It must be promising solution which uses identity attributes and key attributes for encryption. As compared to identity attribute privacy requirements of key attribute is higher. Encryption of key like data tuple provides the confidentiality and privacy assurance but does not provides authorization for key and some other sensitive information as well as attribute in key tuple privacy[12][13]. Searchable symmetric key

encryption technique is used for search keyword encryption [14] [15]. It is also used for hierarchical prediction encryption [26]. Another technique is encrypting identity attribute used to provide control on access for key. There is challenging problem is to find an efficient key encryption scheme to encrypt key tuples in such way that different privacy requirement of precise attributes in the tuples can be satisfied. In this research we are going to contribute search using bloom filter. Using bloom filter we can reduce multiple transactions to the database. Therefore, performance of proposed system can be improved by decreasing the space and time.

2.RELATED WORK

In this section we discussed about existing techniques used to preserve privacy data and user authorisation. In this literature survey we also focus on key management technique proposed and utilised in previous systems as follow:

2.1 *SQL Over Encrypted Data*

DAAS is "Database as a service" concept of storing outsourcing data on cloud. Data owner stores the data in encrypted format using some cryptographic techniques for privacy preservation [2]. In[3], a privacy preservation technique is discussed by Tracey Raybourn, this technique is known as bucketisation encryption. This technique partitioned the encrypted attributes into querytable bucket or table. Bucketisation solves the problem of usually required a tradeoff in which greater security is achieved. OPES is order Preserving Encryption Scheme which directly applied on an encrypted data [4]. Equality, range queries and MIN, MAX and COUNT queries directly processes over an encrypted data. It is efficient encryption technique for avoiding data misuse. OPES has limitation on numeric data encryption. Authenticated index structures based on various cost metrics is proposed by F. Li, M. Hadjieleftheriou et al. for cryptographic operations and index maintenance. This technique formulates the problem of query freshness. For index maintenance B+ tree approach is implemented. But this technique provides less support for privacy leakage [5]. Whereas, previous discussed topics provides the confidentiality guarantee and privacy for data tuples. A group Key management scheme is discussed in [7], allows an efficient access to extract the decryption key for specific portion that permitted for them on the basis of subscription information. The problem of enforcing access control in DSP to make more utilization of system DSP-reencryption concept is suggested [8]. Two types of combination namely ASBE scheme and DSP re-encryption is introduced in [9] for flexible dual fined-grained access control enforcement mechanism. These techniques work against efficient key management. Another techniques discussed in [7] [9], have only focus on achieving identity and authorization privacy of users. To provide compressive protection for outsourced medical data there are two techniques combined namely, digital watermarking and binning in paper [10].

2.2 *Searching an encrypted data*

There are many techniques and algorithms are available to perform searching on encrypted data. SSE is Searchable symmetric encryption and PKES public encryption with keyword search discussed in [11] and [12]. SSE supports the collective search and basic Boolean queries on outsourced symmetrically encrypted data. This scheme supports both structural and textual data with basic Boolean queries. To provide proof of security remote searching techniques discussed in [11]. Remote searching techniques have many advantages such as; they are more secure, controlling support, hidden search and isolation. A new generalized identity based encryption approach known as predicate encryption is proposed by j. Katz, A. Sahai and B. Waters in [12]. In predicate encryption privacy keys are correlated with predicates and cipher-texts are identified with attributes. For any supported query predicate token is produced in public key systems that supporting query on encrypted data. Hidden Vector encryption is technique used for conjunctive query search over an encrypted data. It is essentially anonymous IBE scheme as they construct a bilinear group with a composite order. In [5], this work is extended to support predicate encryption to disjunction and inner product. HVE is hidden vector encryption scheme provides ciphertext associated with a binary attribute vector and k-key associated with vector [14]. There is condition for decryption of ciphertext such that k-key have to satisfy the predicate of key. This technique is used to access fined-grained control on an encrypted data. Predicate encryption is mechanism which gives master secret key owner fine-grained control over access for encrypted data [15]. A novel technique to realize a tag-based dual system encryption in prime-order groups HVE scheme is introduced in[16], which is based on bilinear maps (pairings), provides efficiency advantages in that it requires O(1)-sized private keys and O(1) pairing evaluations for data decryption.

2.3 *Proxy re-encryption*

M. Blaze introduced Divertible Protocols and Atomic Proxy Cryptography scheme. Both are the security properties. Atomic Proxy Cryptography is extension for existing public key cryptography. Previous schemes encrypt the data without granting the ability to decrypt it. Also there exist some systems that re-encrypt the data without granting ability to decrypt it [17]. PRE is proxy re-encryption scheme which re-encrypts the ciphertext from

sender. It then re-ciphertext decrypted under the private key of receiver. Two types of proxy encryptions are available namely, unidirectional and bidirectional. From both of this unidirectional scheme is most trustworthy as asymmetric proxy functions are involved in it. In unidirectional proxy encryption scheme [18] do not require any delegator for revealing their secret keys to anyone in order to permit proxy to re-encrypt their ciphertexts. Identity based proxy encryption is proposed in [19], to identify the problem in identity based proxy re-encryption while transferring ciphertext from one identity to another one. Multiple different schemes are proposed for proxy re-encryption, in that some PRE schemes work against chosen ciphertext attacks. CCA-Secure Proxy Re-Encryption is introduced by J. Shao in [21], a semi-trusted proxy can transform the ciphertext under one's public key into another ciphertext that can decrypt by other user. Due transformation scheme of proxy it can be used in many applications for example in encrypted mail forwarding. CCA is chosen ciphertext attack that work against security issues. CCA –secure and collusion resistant unidirectional PRE scheme implemented to solve the problem of ciphertext attacks. Searchable public key encryption scheme with designated testers (dPEKS) is implemented to keyword guessing attacks [22] as there exist some vulnerable to keyword guessing attacks by malicious servers. This because an outer attacker can make the use of server as a test oracle to verify the correctness of the keyword that guessed by attackers.

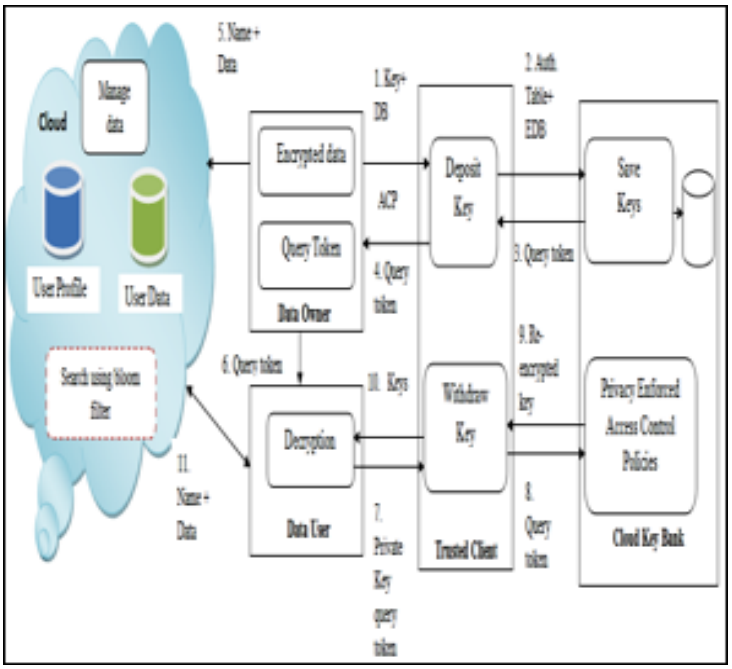
2.4 Bloom Filters

Generally, bloom filter is defined as the probabilistic data structure used to test whether the element is the member of a set. Bloom filters has 100% recall rate as, there is more

possibilities of false positive matches than false negative matches. It is concept based on hashing. Bloom filters has fixed or constant time complexity for adding and determining whether the element is present or not. Many cases there is need to perform quick look-up for deciding how to respond for incoming request. It is the compact representation of membership in set. In this, incremental result will automatically halt after getting fixed number of results.

According to literature survey analysis, we examined that there is need of such technique which can efficiently preserve the privacy & confidentiality of outsourced keys. A system which can enable owner controllable authorization, key management etc.

3.SYSTEM ARCHITECTURE



4.CONCLUSIONS

In this survey paper of efficient management of encryption keys and user password, we have identified some problem in previous systems such as encrypting identity attributes and other related identity conditions in the access control policy achieves the identity and related condition privacy of users, but it does not consider key authorization based on the identity attributes in key tuples and query authorization on submitted search query. Therefore, in outsourced keys storage, a challenging problem is to find an encryption scheme which can encrypt the key tuples in a way that the different privacy requirements of sensitive attributes in the key tuples can be satisfied. According our analysis in this paper, SC-PRE scheme can efficiently achieve security requirements that are identified as challenging issues in previous systems.

REFERENCES

[1] 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.

[2] [2] 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.

[3] Tracey Raybourn ,"Bucketisation Technique for Encrypted Databases:Quantifying the impact of Query Distribution",a thesis of master of science, May 2013

[4] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc ACM SIGMOD Int. Conf. Manag. Data, 2004, pp. 563–574.

[5] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in Proc ACM SIGMOD Int. Conf. Manag. Data, 2006, pp. 121–132

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

[7] 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.

[8] X. X. Tian, X. L. Wang, and A. Y. Zhou, "DSP Re-encryption based access control enforcement management mechanism in DaaS," Int. J. Netw. Security, vol. 15, no. 1, pp. 28–41, 2013.

[9] 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

[10] Bertino, B. C. Ooi, Y. Yang, and R. H. Deng, "Privacy and ownership preserving of outsourced medical data," in Proc 21th Int. Conf. Data Eng., 2005, pp. 521–532

[11] X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, Oakland, California, USA, May 2000, pp. 44–55.

[12] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. 27th Annu. Int. Conf. Adv. Cryptol. Theory Appl. Cryptograph. Techn., vol. 4965, pp. 146–162, 2008.

[13] D. Cash, Stanislaw, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Proc 33th Int. Conf. Crypography Conf., 2013, pp. 353–373.

[14] V. Iovino and G. Persiano, "Hidden-vector encryption with groups of prime order," in Proc. Int. Conf. Pairing-Based Cryptography, 2008, vol. 5209, pp. 75–88.

[15] Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Proc. Theory Cryptography Conf., 2009, vol. 5444, pp. 457–473.

[16] J. Hwan Park, K. Lee, W. Susilo, and D. Hoon Lee, "Fully secure hidden vector encryption under standard assumptions," Inf. Sci., vol. 232, pp. 188–207, 2013

[17] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., 1998, pp. 127–144.

[18] 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

[19] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288–306

[20] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy Re-encryption," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 185–194.

[21] 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.

[22] H. S. Rhee, W. Susilo, and H.-J. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," IEICE Electronics Express, vol. 6, no. 5, pp. 237–243, 2009.