International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

A Survey on Cloud Key Bank Privacy and Owner Sanction Enforced Key Management Framework

Mr. Malle Naveen Kumar[1] & Mr. U. Balashivudu[2]

[1]B-Tech Dept. of CSE Mahatma Gandhi Institute of Technology

Mail Id: - naveen.malle2710@gmail.com

[2]Assistant professor Dept. of CSE Mahatma Gandhi Institute of Technology

Mail Id: - balashivudu@mgit.ac.in

Abstract

Explosive magnification in the number of passwords for web predicated applications and encryption keys for outsourced data storage well exceed the management limit of users. Consequently outsourcing keys (including passwords and data encryption keys) to professional password managers (veracious-but-curious accommodation providers) is magnetizing the attention of many users. However, subsisting solutions in traditional data outsourcing scenario are unable to simultaneously meet the following three security requisites for keys outsourcing: 1)Confidentiality and privacy of keys; 2)Search privacy on identity attributes tied to keys 3)Owner controllable sanction over his/her shared keys. In this paper, we propose Cloud Key Bank, the first coalesced key management framework that addresses all the three goals above. Under our framework, the key owner can perform privacy and controllable sanction enforced encryption with minimum information leakage. To implement Cloud Key Bank efficiently, we propose an incipient cryptographic primitive denominated Searchable Conditional Proxy Re-Encryption (SC-PRE) which coalesces the techniques of Obnubilated Vector Encryption (HVE) and Proxy Re-Encryption (PRE) seamlessly, and propose a concrete SCPRE scheme predicated on subsisting HVE and PRE schemes. Our experimental results and security analysis show the efficiency and security goals are well achieved.

Keywords: - Key owner, Cloud Key Bank provider, trusted client, User.

1. INTRODUCTION

With the rapid deployment of web applications such as online banking, shopping, convivial networks and data storage (e.g., Amazon S3 and Google Drive), managing the ever-growing number of passwords and data encryption keys is becoming an immensely colossal

encumbrance for many users. Key Bank provides investment management, retail, business, private and commercial banking, consumer finance, wealth management, and investment banking products and accommodations to individuals and companies throughout the Amalgamated States and, for certain businesses, internationally. With over 1,014 branches in over 14 states and offices in 31 states, Key Bank uses Cloud's Commission to incentivize and pay 7,900 retail and business banking employees predicated on overall customer contentment and incipient customer acquisitions.

2. RELATED WORK

Subsisting system

Explosive magnification in the number of passwords for web predicated applications and encryption keys for outsourced data storage well exceed the management limit of users. Consequently outsourcing keys (including passwords and data encryption keys)to professional password managers (veracious-but-curious accommodation providers) is magnetizing the attention of many users. However, subsisting solutions in traditional data outsourcing scenario are unable to simultaneously meet the following three security requisites for keys outsourcing: 1)Confidentiality and privacy of keys; 2)Search privacy on identity attributes tied to keys; 3)Owner controllable sanction over his/her shared keys.

Disadvantage

Cloud Key Bank provider is a veracious-but-curious inside assailant who is curious about key values in ki (Key confidentiality) and identity values in ~xi (Identity confidentiality and Amiability privacy), but can veraciously provide efficient database operations given minimum information leakage. The minimum information leakage may include leakage on the total size of the Key DB and o desultory tuple identifier (e.g. the identifier indi for tuple to expedite the query efficiency), but never the direct exposure of plaintext keys or identities. The maleficent utilizer is an outside assailant who wants to derive keys of the delegated utilizer and thus impersonate him/her to do illicit actions (Key privacy and Key sanction). The Cloud Key Bank provider or the assailant in the middle may derive the private intent of the utilizer from his/her submitted search query (Search privacy). The malignant utilizer may impersonate the licit utilizer to submit search query in terms of the kenned background cognizance such

as the possible search keywords (Query sanction).

Proposed system

We propose Cloud Key Bank, the first coalesced key management framework that addresses all the three goals above. Under our framework, the key owner can perform privacy and controllable sanction enforced encryption with minimum Information leakage. To implement Cloud Key Bank efficiently, we propose an incipient cryptographic primitive designated Searchable Conditional Proxy Re-Encryption (SC-PRE) which coalesces the techniques of Obnubilated Vector Encryption (HVE) and Proxy Re-Encryption (PRE) seamlessly, and propose a concrete SCPRE scheme predicated on subsisting HVE and PRE schemes. Our experimental results and security analysis show the efficiency and security goals are well achieved.

Advantage

The keys have high sensitivity and need to be obnubilated from the veracious-but-curious accommodation provider and malevolent assailants. This involves confidentiality and privacy of keys – only the sanctioned users can derive the shared keys of the key owner through the sanctioned decryption computation. The keys are always stored with many sensitive identity attributes (in the Search attribute group in lieu of the access control policy) of key owners and are probed predicated on them. This involves search privacy on identity attributes – the veracious-but-curious key accommodation provider cannot derive any identity attribute tied with keys from the submitted search query, but can evaluate the query from the encrypted key database correctly. The keys have vigorous ownership because they are habituated to bulwark many other sensitive information of the key owner. This involves owner controllable sanction including key sanction and query sanction – only the key owner can designate and control in a fine-grained way who has the rights to access his/her shared keys through sanction on key attributes (key sanction) and sanction on submitted search query (query sanction).

3. IMPLEMENTATION

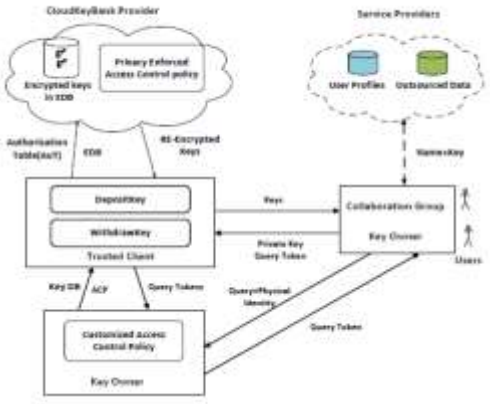

Fig:-1 System Architecture

Key owner

Key owner can be the password owner or data encryption key owner who outsources his/her encrypted key database (Key DB) to the Cloud Key Bank provider. After that the encrypted key database (EDB) stored in Cloud Key-Bank provider can be accessed anywhere and anytime with minimum information leakage such as the size of Key DB. The key owner mainly consummates the following three tasks: 1) Constructing the customized access control policy (ACP) in terms of his/her practical keys sharing requisites; 2) Depositing Key DB by utilizing Deposit Key protocol under the fortification of ACP; 3) Distributing sanctioned Query tokens to the delegated utilizer predicated on the user's registered information such as the wanted query and physical identity.

Cloud Key Bank provider

Cloud Key Bank provider can be any professional password manager such as Last Pass who provides privacy enforced access control on EDB. The Cloud- KeyBank provider mainly consummates the following 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 sanction he/she can transform an encrypted key into the sanctioned re-encrypted key under the corresponding Delegation token stored in Sanction Table (AuT).

Trusted client

Trusted client is the primary privacy enforced component in Cloud Key Bank framework. It mainly consists of two protocols: Deposit Key and Withdraw Key. Deposit Key protocol provides Key DB encryption, token generation (including Query token and Delegation token). Withdraw key protocol provides the re-encryption of encrypted keys and the decryption of re-encrypted keys.

Utilizer

There are two kinds of users in Cloud Key Bank framework: Key owner and

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

Collaboration group. Key owner corresponds to an individual utilizer who deposits all his keys to Cloud Key Bank provider and accesses them by himself. Collaboration group corresponds to a group of users where the key owner can apportion his/her keys with other users within the same collaboration group. By submitting the private key and sanctioned Query token, a delegated utilizer can withdraw a sanctioned key by utilizing Withdraw Key protocol under the fortification of privacy enforced access control policy (i.e. AuT in our solution)

4. EXPERIMENTAL RESULTS

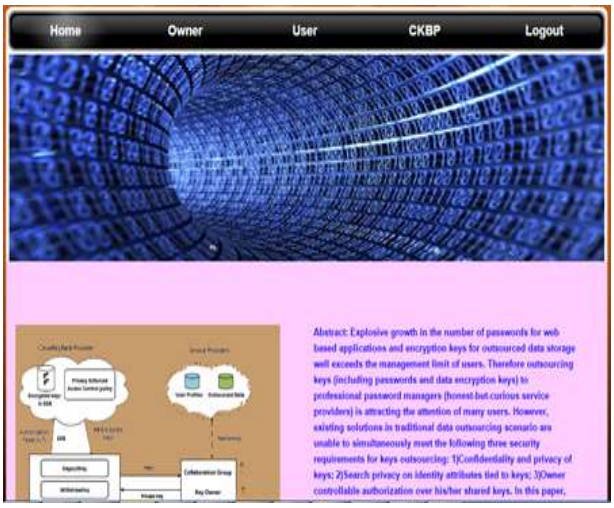

Fig:-2 Home Screen Page

Fig:-3 Authentication and Authorization

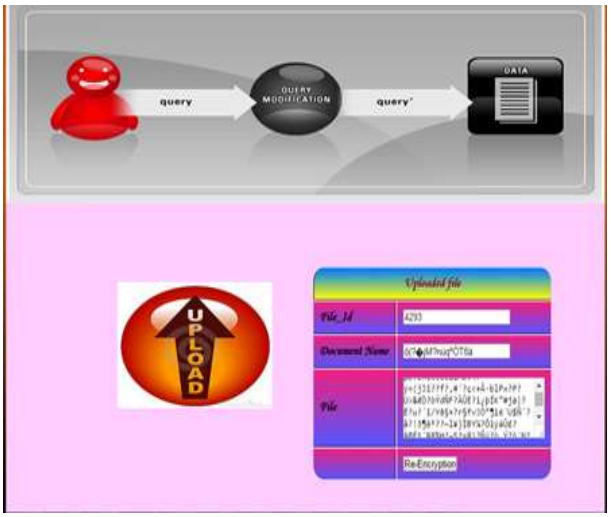

Fig:-4 Encrypted File Data

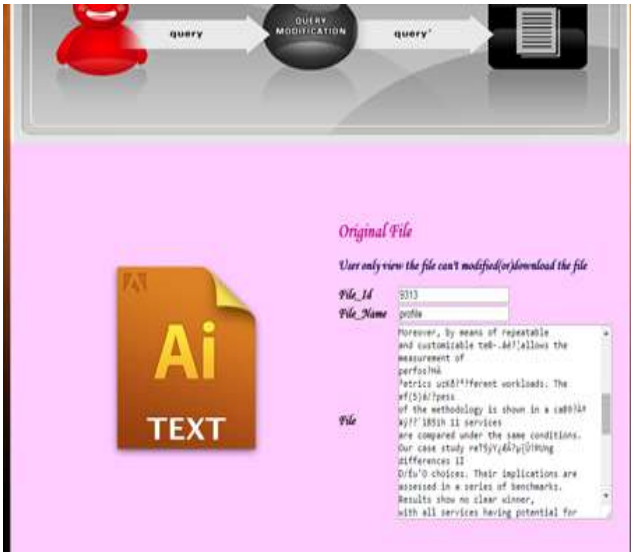

Fig:-5 Decrypted File Data

5. CONCLUSION

To solve the identified critical security requisites for keys outsourcing, we present Cloud Key Bank, the first amalgamated privacy and owner sanction enforced key management framework. To implement Cloud Key Bank, we propose an incipient Cryptographic primitive SC-PRE and the corresponding concrete SC-PRE scheme. The security comparison and analysis prove that our solution is ample to fortify the identified three security requisites which are not be solve in traditional outsourced scenario. From the performance analysis, we can optically discern that our solution is not so efficient because it requires several seconds to answer a query on a database only 200 passwords.

6. 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] 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