International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

Secret Key Management Framework by Using a Cloud Key for Owner and Privacy Authorization

[#1] Mr. Karusala Dathanandana, [2] K.Mohanrao

1 PG Scholar, Dept of CSE, Prakasam Engineering College, Kandukur, Prakasam(Dt), AP, India.

2 Associate professor Professor , Dept of CSE, Prakasam Engineering College,Kandukur, Prakasam(Dt), AP, India

Abstract: Explosive growth in the number of passwords for web based applications and encryption keys for outsourced data storage well exceeds the management limit of users. Therefore outsourcing keys to professional password managers (honest-but-curious service providers) is attracting the attention of many users. However, existing solutions in traditional data outsourcing scenario are unable to simultaneously meet the following three security requirements for keys outsourcing: 1)Confidentiality and privacy of keys; 2)Search privacy on identity attributes tied to keys; 3)Owner controllable authorization over his/her shared keys. In this paper, we propose CloudKeyBank, the first unified key management framework that addresses all the three goals above. Under our framework, the key owner can perform privacy and controllable authorization enforced encryption with minimum information leakage. To implement CloudKeyBank efficiently, we propose a new cryptographic primitive named Searchable Conditional Proxy Re-Encryption (SC-PRE) which combines the techniques of Hidden Vector Encryption (HVE) and Proxy Re-Encryption (PRE) seamlessly, and propose a concrete SCPRE scheme based on existing HVE and PRE schemes.

Keywords: Encryption, Privacy, Key Management, Proxy.

I. INTRODUCTION

The rapid deployment of web applications such as online banking, shopping, social networks and data storage, managing the ever-growing number of passwords and data

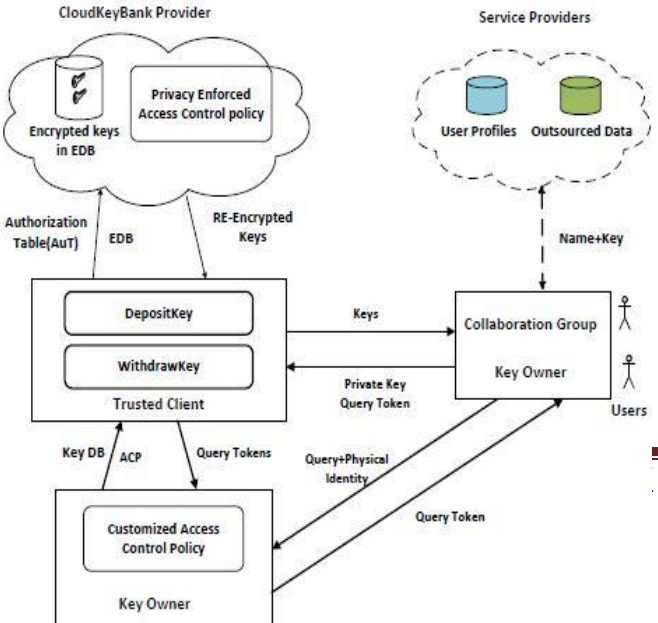
encryption keys is becoming a big burden for many users. However, the weak and shared passwords across accounts make them easy to be compromised, which in turn leaks more passwords related to private and sensitive data. As pointed out in the survey6, privacy problems are the main concern of cloud users in outsourced data storage, which is also true for outsourced keys storage. The privacy of their keys, which mainly involves two situations: 1) they 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; 2) they trust the service providers, but keys could be disclosed if there exists an misbehaving internal employee or broken server. Therefore encrypting key tuples just like encrypting normal data tuples before outsourcing seems to be a promising solution to maintaining trust and ensuring the key owners' control over their own privacy.

The privacy requirements of key attributes in the Key attribute group is higher than that of identity attributes in the Search attribute group, because the resulted information leakage by the former is much larger than that by the latter. Therefore, based on the different sensitive attributes in key tuples, we identify that the following three critical security requirements need to be achieved for secure keys outsourcing. First. The keys have high sensitivity and need to be hidden from the honest-but-curious service provider and malicious attackers. Second. The keys are always stored with many sensitive identity attributes (in the Search attribute group instead of the access control policy) of key owners and are searched based on them. Third. The keys have strong ownership because they are used to protect many other sensitive information of the key owner. However, most of the currently proposed approaches in traditional data outsourcing data scenario just support one or two of the three identified security requirements to some extent. Encrypting key tuples like encrypting data tuples in an all or nothing way can guarantee the confidentiality and privacy of keys, but does not consider the key authorization and the different privacy requirements of sensitive attributes in key tuples.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

Encrypting search keywords (identity attributes in key tuples) based on searchable symmetric encryption or hierarchical predicate encryption can guarantee the search privacy on key tuples, but does not consider the key authorization and the dependence relation between identity attributes and key attributes. Encrypting identity attributes and related identity conditions in the access control policy achieves the identity and related condition privacy of users, but 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. To efficiently solve the identified secure problems above, to the best of our knowledge, we are the first to explore and present CloudKeyBank, an unified key management framework with enforced privacy and owner

- The CloudKeyBank provider who stores the encrypted key database will not be able to see the content of the key at anytime even if he/she knows all Delegation tokens of the delegated users. Both the delegated user and the CloudKeyBank provider cannot derive the private key of key owner from the submitted Query token, but the CloudKeyBank provider still can perform efficient search queries by evaluating the Query token from each encrypted key tuple.



II. SYSTEM ARCHITECTURE

As shown in Fig.1, CloudKeyBank architecture consists of four entities: Key owner, CloudKeyBank provider, Trusted client and Users.

1. 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 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) in terms of his/her practical keys sharing requirements; 2) Depositing Key DB by using DepositKey protocol under the support of ACP; 3) Distributing authorized Query tokens to the delegated user

Fig.1. System Architecture.

based on the user's registered information such as the wanted query and physical identity.

2. CloudKeyBank provider: CloudKeyBank provider can be any professional password manager such as LastPass who provides privacy enforced access control on EDB. The CloudKeyBank provider mainly completes 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 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: DepositKey and WithdrawKey. As is shown in Fig.1, Service providers, such as web based application providers and outsourced data storage providers are the part in the dotted cloud. In this paper we assume the secure communication (protecting the security of transferred name and key) between users and service providers is based on HTTPS and outsourced data stored at these service providers are encrypted under data encryption keys. In this paper we only focus on how to achieve the privacy and owner controllable authorization of keys stored in CloudKeyBank provider, while do not consider the privacy of outsourced data protected by the keys.

Enc. It takes as input the public pk of key owner, a tuple, vector of key attributes and vector of identity attributes. The encryption algorithm (Enc) based on HVE and PRE outputs the ciphertext CT of key tuple.

III. SC-PRE BASED CLOUDKEYBANK FRAMEWORK

In this section, based on known schemes HVE and PRE, we present a concrete SC-PRE scheme which provides the privacy and authorization enforced encryption support for our CloudKeyBank framework by distributing its eight polynomial algorithms.

Setup denoted as Setup(□) ->params. It takes the security parameter as input and outputs system parameters params.

KeyGen. It takes as input the number of identity attribute-value pairs . The key generation algorithm (KenGen) outputs a public and private key pair (pk; sk) for the user.

QuTGen. It takes as input the private key sko of key owner and vector of identity attributes. The query token generation algorithm (QuTGen) outputs a query token for subsequent privacy search query on encrypted Key DB and query authorization on submitted queries.

DelTGen. It takes as input the private key sk of key owner and the public key pk du of the delegated user. The delegation key generation algorithm (DelTGen) outputs the delegation token that is computed from the partial parameters of sk and pk.

Search. It takes as input the tuple ciphertext CT under public key pk and key owner's query token, and outputs the encrypted key ek on the condition that succeeds by evaluating against the hidden vector in encrypted tuple CT, otherwise outputs □.

ReEnc is a conditional encryption algorithm. It takes as input the result of Search algorithm and the delegation token of the delegated user. The re-encryption algorithm (ReEnc) transforms encrypted key ek into re-encrypted key rek ; otherwise it outputs □ if the result of Search algorithm is □.

Dec. Taking as input the private key sk and the re-encrypted key rek, the decryption algorithm (Dec) outputs plaintext . In terms of the customized access control policy of key owner, sk may be sk of the key owner or skdu of the delegated user.

IV. CONCLUSION

To solve the identified critical security requirements for keys outsourcing, we present CloudKeyBank, the first unified privacy and owner authorization enforced key management framework. To implement CloudKeyBank, we propose a new cryptographic primitive SC-PRE and the corresponding concrete SC-PRE scheme.

V. FUTURE WORK

The main reason for inefficiency is that SC-PRE belongs to one kind of public encryption which is inefficient in common by comparing to the symmetric encryption. That is what we want to solve in our future work where we will introduce searchable symmetric encryption, bloom filter based index in one server, and access policy enforcement in another server to support scalable operations on encrypted key database.

VI. REFERENCES

[1] J. Bonneau, C. Herley, P. C. van

Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Proc of 33th IEEE Symposium on Security and Privacy, pp. 553-567, 2012.

[2] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data. In 2000 IEEE Symposium on Security and Privacy,IEEE Computer Society Press, pp.44C55, Oakland, California, USA, May 2000.

[3]D.Boneh, G.Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search, Advances in Cryptography, EUROCRYPT' 04 , LNCS 3027, pp.506-522, Springer, Berlin, Germany, May2004.

[4] X.Boyen and B.Waters, Anonymous hierarchical identity-based encryption (without random oracles). Proceeding of CRYPTO'06, 2006.

[5] J. Katz, A. Sahai, and B. Waters, Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, Proc. Theory and Applications of Cryptographic Techniques 27th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT'08), vol. 4965, pp. 146-162, 2008.

[6]D. Boneh and B. Waters, Conjunctive, Subset, and Range Queries on Encryted Data, Proc. Conf. Theory of Cryptography (TCC'07), vol. 4392, pp. 535-554, 2007.

[7]E. Shi and B. Waters, Delegating Capabilites in Predicate Encryption Systems, Proc. Int'l Colloquium Automata,

Languages and Programming (ICALP'08), vol. 5126, pp. 560-578, 2008.

[8] V. Iovino and G. Persiano, Hidden-Vector Encryption with Groups of Prime Order, Proc. Int'l Conf. Pairing-Based Cryptography (Pairing'08), vol. 5209, pp. 75-88, 2008.

[9] E. Shen, E. Shi, and B. Waters, Predicate Privacy in Encryption Systems, Proc. Theory of Cryptography Conf. (TCC'09), vol. 5444, pp. 457-473,2009.

[10] J.Hwan Park. Efficient Hidden Vector Encryption for Conjunctive Queries on Encrypted Data. IEEE Transactions On Knowledge And Data Engineering, 23(10):1483-1497,2011.