ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Efficient Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage: A Survey

Niraj Jaywant Bankar, Prof. Kore Kunal Sidramappa

P.G. Student, Department of Comp Engineering, SPCOE Otur, Pune, India

Professor, Department of Comp Engineering, SPCOE Otur, Pune, India

ABSTRACT: The ability of specifically offering encoded information to various clients through open distributed storage might enormously ease security worries over coincidental information leaks in the cloud. A key test to outlining such encryption plans lies in the proficient administration of encryption keys. The desired adaptability of imparting any gathering of chosen records to any gathering of clients requests diverse encryption keys to be utilized for various archives. On the other hand, this similarly suggests the need of safely disseminating to clients countless for both encryption and seek, and those clients will need to safely store the got keys, and present a just as expansive number of catchphrase trapdoors to the cloud to perform look over the shared information. The suggested requirement for secure correspondence, stockpiling, and many-sided quality plainly renders the methodology unrealistic. In this paper, we address this viable issue, which is generally dismissed in the writing, by proposing the novel idea of key aggregate searchable encryption (KASE) and instantiating the idea through a solid KASE plan, in which an information owner just needs to disseminate a solitary key to a client for sharing an extensive number of reports, and the client just needs to present a Single trapdoor to the cloud for questioning the common records. The security examination and execution assessment both affirm that our proposed plans are provably secure and for all intents and purposes productive.

KEYWORDS: Searchable encryption, data sharing, cloud storage, data privacy

I. INTRODUCTION

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization. However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets(e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a cloud storage is often called the cryptographic cloud storage. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption(SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data. Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored in the literature. First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends In a social network application, or sharing a business document with certain colleagues on a cloud drive)usually demands different encryption keys to be used for different files. However, this implies the number of keys that need to be distributed to users, both for them to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels, but also be securely stored and managed by the users in their devices. In addition, a large number of trapdoors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical.

II. LITERATURE SURVEY

1 Multi-user Searchable Encryption

There is a literature on searchable encryption, including SSE schemes [5]–[8] and PEKS schemes [9]–[15]. In contrast to those existing work, in the context of cloud storage, keyword search under the multi-tenancy setting is a common scenario. In such a scenario, the data owner would like to share a document with a group of authorized users and each user who has the access right can provide a trapdoor to perform the keyword search over shared document, namely, the “multi-user searchable encryption” (MUSE) scenario. Some recent work [6], [13]–[15], [19] focus to such a MUSE scenario, although they all adopt single key combined with access control to achieve the goal.

2 Multi-Key Searchable Encryption

In the case of a multi-user application, considering that the number of trapdoors is proportional to number of documents to search over (if the user provides to the server a keyword trapdoor under every key with which a matching document might be encrypted), Popa [20] firstly introduces the concept of multi-key searchable encryption (MKSE) & puts forward the first feasible scheme in 2013.

3 Key-aggregate Encryption for Data Sharing

Data sharing systems based upon cloud storage have attracted much attention recently [1]–[4]. In particular, [4] consider how to reduce the number of distributed data encryption keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

IV. EXISTING METHODOLOGY

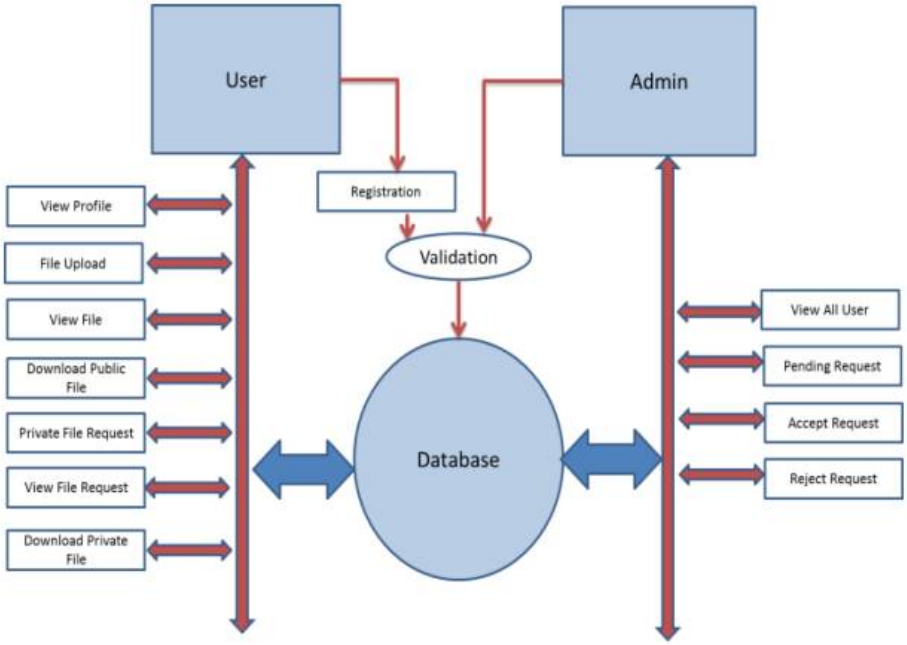

Figure 1 : Generate floe of System

System setup When an organization submits a request, cloud will create a database containing four tables. Moreover, it assigns an administrator account manager. Then, the data sharing system will work under the control of manager. To generate system parameters params, manager runs the algorithm KASE.Setup and updates the field parameters.

User registration When adding a new member, manager assigns UserID, UserName, and password and then stores the necessary information into the table user.

User login Like most popular data sharing products (e.g., Dropbox and citrix), our system relies on a password verification for authenticating users. To further improve the security, multi-factor authentication or digital signatures may be used when available.

Data uploading User upload file like PDF file, word file, Text File ,image etc. Uploading file contain file, File name, file description. File may be public file or private file. While uploading file public key and private key generated automatically by using function Randomize string and Randomize number. One user send file to all other user by simply share file as public for no authority ner can encrypt the keys using his/her private key and store them into the table.

Keyword Search User views all uploaded file by other user and itself. It display information of file name, file description, share as public or private and name of user those are uploaded a file. User can search the specific file just simply search the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

name of file. User download public file without authentication of owner of file, but user need private key while downloading private file.

Data retrieving File request contain the information of requested file by user. It contain user name, file name, public key of file and message. User can only request file which are private because it need private key for download.

V. CONCLUSION

Considering practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute large number of keys to users to enable them to access his/her documents, for the first time we propose concept of key-aggregate searchable encryption (KASE) and construct a KASE scheme. Both analysis and evaluation result confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage. However, if a user wants to query over documents shared by multiple owners, he have to generate multiple trapdoors to the cloud. How to reduce number of trapdoors under multi-owners setting is a future work.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.
[2] R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2013/508, 2013.
[3] D. Boneh, C. Gentry and B. Waters. "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", CRYPTO'05, pp. 258C275, 2005.
[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.
[7] Boneh, Dan, et Brent Waters. «Conjunctive, Subset, and Range Queries on Encrypted Data.» Theory of Cryptography Conference. Springer, 2007. 535-554.
[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012. [9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
[10] Golle, Phillipe, Brent Waters, et Jessica Staddon. «Secure Conjunctive Keyword Search over Encrypted Data.» Applied Cryptography and Network Security (ACNS '04). 2004. 31- 45.
[11] Chase, Melissa, et Sherman Chow. «Improving Privacy and Security in Multi-Authority Attribute-Based Encryption.» ACM Conference on Computer and Communications Security. 2009.
[12] Goyal, Vipul, Omkant Pandey, Amit Sahai, et Brent Waters. «Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.» ACM Conference on Computer and Communications Security. 2006. 89-98.
[13] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.
[14] Ostrovsky, Rafail, Amit Sahai, et Brent Waters. «Attribute-based encryption with non-monotonic access structures.» ACM Conference on Computer and Communications Security. 2007. 195-203.
[15] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490- 502, 2012.
[16] Juels, Ari, et Burt Kaliski. «PORs: proofs of retrievability for large files.» ACM Conference on Computer and Communications Security. ACM Press, 2007. 584-597.
[17] Park, Dong Jin, Kihyun Kim, et Pil Joong Lee. «Public Key Encryption with Conjunctive Field Keyword Search.» Information Security Applications. Springer, 2005. 73-86.
[18] Shacham, Hovav, et Brent Waters. «Compact Proofs of Retrievability.» ASIACRYPT. Springer, 2008. 90-107
[19] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249-255, 2013.
[20] D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts", International journal of information security, 12(4): 251-265, 2013