ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON CRYPTOGRAPHIC CLOUD STORAGE WITH KEY AGGREGATE SEARCHABLE ENCRYPTION

Pallavi Vijay Nichal*, Prof. P. L. Ramteke
Student of Master of Engineering in (CS & IT) HVPM's college of Engineering and Technology Amravati, India
Associate Professor in Department of (CSE) HVPM's College of Engineering and Technology Amravati, India

DOI: 10.5281/zenodo.47039

ABSTRACT

Cloud is a new way to store large amount of data. In cloud computing, data owners host their data on cloud servers and users can access the data from cloud servers. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. 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.Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

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

INTRODUCTION

The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over inadvertent data leaks in the cloud. A key challenge to designing such encryption schemes lies in the efficient management of encryption keys. The desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. However, this also implies the necessity of securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data. The implied need for secure communication, storage, and complexity clearly renders the approach impractical. In this paper, we address this practical problem, which is largely neglected in the literature, by proposing the novel concept of keyaggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

In a KASE scheme, the owner only needs to distribute a single key to a user when sharing lots of documents with the user, and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner. However, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting is a future work. Moreover, federated clouds have attracted a lot of attention nowadays, but our KASE cannot be applied in this case directly. It is also a future work to provide the solution for KASE in the case of federated clouds.

By proposing the novel concept of key aggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large

number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former. To support searchable group data sharing the main requirements for efficient key management are twofold:

1) A data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files
2) The user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. To the best of our knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy both requirements (the key-aggregate cryptosystem [4], which has inspired our work, can satisfy the first requirement but not the second).

OBJECTIVES

1) We design a secure data sharing scheme, for dynamic groups in an untrusted cloud.
2) A user is able to share data with others in the group without revealing identity privacy to the cloud.
3) It supports efficient user revocation and new user joining.
4) More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation.

LITERATURE SURVEY

1. Multi-user Searchable Encryption

There is a rich literature on searchable encryption, including SSE schemes [3][5] and PEKS schemes [6][7]. In contrast to those existing work, in the context of cloud storage, keyword search under the multi-tenancy setting is a more 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 the shared document, namely, the "multi-user searchable encryption" (MUSE) scenario. Some recent work [4], [7], [9] focus to such a MUSE scenario, although they all adopt single-key combined with access control to achieve the goal. In [4], [9], MUSE schemes are constructed by sharing the document's searchable encryption key with all users who can access it, and broadcast encryption is used to achieve coarse-grained access control. In [8], attribute based encryption (ABE) is applied to achieve fine-grained access control aware keyword search. Key aggregate searchable encryption can provide the solution for the latter, and it can make MUSE more efficient and practical.

2. Multi-Key Searchable Encryption

In the case of a multi-user application, considering that the number of trapdoors is proportional to the number of documents to search over (if the user provides to the server a keyword trapdoor under each key with which a matching document might be encrypted), Popa [10] firstly introduces the concept of multi-key searchable encryption (MKSE) and puts forward the first feasible scheme in 2013. MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user. approach of MKSE inspires us to focus on the problem of keyword search over a group of shared documents from the same user in the multiuser applications, and the adjust process in MKSE also provides a general approach to perform keyword search over a group of documents with only one trapdoor. However, the adjust process of MKSE needs a delta generated from both user's key and SE key of the document, so it does not directly apply to the design of a concrete KASE scheme.

3. Key-aggregate Encryption for Data Sharing

Data sharing systems based on cloud storage have attracted much attention recently [1][2]. In particular,

Chu et al. [2] consider how to reduce the number of distributed data encryption keys. To share several documents with different encryption keys with the same user, the data owner will need to distribute all such keys to him/her in a traditional approach which is usually impractical. Aiming at this challenge, a keyaggregate Encryption (KAE) scheme for data sharing is proposed to generate an aggregate key for the user
to decrypt all the documents.

CONTRIBUTIONS

More specifically, our main contributions are as follows.

1) We first define a general framework of keyaggregate searchable encryption (KASE) composed
of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. We then describe both functional and security requirements for designing a valid KASE scheme.

2) We then instantiate the KASE framework by designing a concrete KASE scheme. After providing
detailed constructions for the seven algorithms, we analyze the efficiency of the scheme, and establish its security through detailed analysis.

3) We discuss various practical issues in building an actual group data sharing system based on
the proposed KASE scheme, and evaluate its performance. The evaluation confirms our system
can meet the performance requirements of practical applications.

CONCLUSION

In this paper we study the different papers regarding privacy preserving for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Data sharing is an important functionality in cloud storage. We show how to securely, efficiently, and flexibly share data with oyhers in cloude storage. we address this challenge by proposing the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former.

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] 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.
[3] X. Song, D.Wagner, A. Perrig. “Practical techniques for searches on encrypted data”, IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[4] 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.
[5] 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.
[6] D. Boneh, C. G, R. Ostrovsky, G. Persiano. “Public Key Encryption with Keyword Search”, EUROCRYPT 2004, pp. 506C522, 2004.
[7] 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.
[8] C. Dong, G. Russello, N. Dulay. “Shared and searchable encrypted data for untrusted servers”, Journal of Computer Security, pp. 367-397, 2011
[9] 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.
[10] R. A. Popa ,N. Zeldovich. “Multi-key searchable encryption”. Cryptology ePrint Archive, Report 2013/508, 2013.