Key-Aggregate Searchable Encryption (KASE) Through trapdoor for Group Data Sharing via Cloud Storage

Prof. Mugdha Rane[1], Shruti Kokate[2], Jyoti Sonawane[3], Pranita Panchal[4] , Meenkshi[5], Priya Nalawade[6]

[12345]*Information Technology Department, Savitribai Phule Pune University*
Address

[12345] Bharati Vidyapeeth's College Of Engineering For Women,Pune

Abstract

Data distribution is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible. The innovation is that one can aggregate any set of secret keys and make them as compact as a single key, but surrounding the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be expediently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

Keywords—Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

1 Introduction

However, this also implies the requirement 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 disguised need for secure communication, storage, and complication clearly renders the approach unworkable.

In this paper, we address this practical problem, which is largely unkempt in the literature, 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.

2 Literature Survey

Key-Aggregate Cryptosystemfor Scalable Data Sharing in Cloud Storage

In this article, we show how to, efficiently, securelyand flexibly share data with others in cloud storage. The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over unintended data leaks in the cloud.

A key challenge to designing such encryption schemes lies in the efficient management of encryption keys.

The desired elasticity of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents.

We describe new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated.

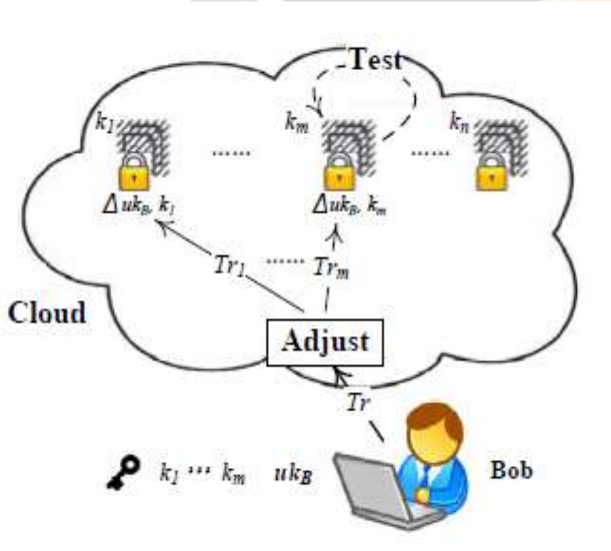
Practical Techniques for Searches on Encrypted Data.

In this paper, we designate our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of critical advantages. They are provably secure: they provide provable confidentialityfor encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an uninformed word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server.

3 System Overview

We consider a cloud computing architecture by mergingwith an example that a company uses a cloud to enable its staffs in the same collection or section to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Fig.

Fig: System Architecture



Cloud is operated by CSPs and provides priced profuse storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to [3], [7], we assume that the cloud server is truthful but enquiring. That is, the cloud server will not spitefully delete or modify user data due to the protection of data auditing schemes [17], [18], but will try to learn the content of the stored data and the identities of cloud users.

Group manager takes charge of system parameters generation, userrevocation, user registration, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members.

Note that, the group membership is enthusiastically changed, due to the staff notification and new employee contribution in the company.

4 Our Contributions

Revisiting previous definitions. We review existing security definitions for secure indexes, including in distinguishability against chosen-keyword attacks (IND2-CKA) [23] and the simulation-based definition in [18], and highlight some of their limitations. Specifically, we recall that IND2-CKA does not guarantee the privacy of user queries (and is therefore not asatisfactory notion of security for constructing SSE schemes) and then highlight (and fix) technical issues with the simulation-based definition of [18]. We address both these issues by proposing new game-based and simulation-based definitions that provide security for both indexes and trapdoors.

New definitions. We introduce new adversarial models for SSE. The first, which we refer to as non- adaptive, only considers adversaries that make their search queries without taking into account the trapdoors and search outcomes of previous searches. The second—adaptive—considers adversaries that choose their queries as a function of previously obtained trapdoors and search outcomes. All previous work on SSE (with the exception of oblivious RAMs) falls within the non-adaptive setting. The insinuation is that, contrary to the natural use of searchable encryption described in these definitions only guarantee security for users that perform all their searches at once. We address this by introducing game-based and simulation-based definitions in the adaptive setting.

New constructions. We present two constructions which we prove secure under our new definitions. Our first scheme is only secure in the non-adaptive setting, but is the most efficient SSE construction to date. In fact, it achieves searches in one communication round, requires an amount of work from the server that is linear in the number of documents that contain the keyword (which is optimal), requires constant storage on the client, and linear (in the size of the document collection) storage on the server. While the construction in also performs searches in one round, it can induce false positives, which is not the case for our construction. Additionally, all the constructions in require the server to perform an amount of work that is linear in the total number of documents in the collection.

5 Conclusion

We have pronounced new techniques for remote searching on encrypted data using an untrusted server and provided proofs of security for the resulting crypto systems. Our techniques have a number of critical advantages: they are provably secure; they support controlled and hidden search and query segregation; they are simple and fast (More specifically, for a document of length , the encryption and search algorithms only need stream cipher and block cipher operations); and they introduce almost no space and communication overhead. Our scheme is also very elastic, and it can easily be extended to support more advanced search queries. We conclude that this provides a powerful new building block for the construction of secure services in the untrusted infrastructure.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. 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 decrease the number of trapdoors under multi-owners setting is a future work. More- over, 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.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Com- puting”, Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing”, Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. “Mona: secure multi- owner data sharing for dynamic groups in the cloud”, IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182- 1191.

[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 con- structions”, In: Proceedings of the 13th ACM conference on Com- puter and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen. “Computationally efficient searchable symmetric encryption”, Secure Data Management, pp. 87-100, 2010.

[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 Encryp- tion with Keyword Search”, EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang, P. Lee. “Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System”, In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11] J. Li, Q. Wang, C. Wang. “Fuzzy keyword search over encrypt- ed data in cloud computing”, Proc. IEEE INFOCOM, pp. 1-5, 2010.

[12] C. Bosch, R. Brinkma, P. Hartel. “Conjunctive wildcard search over encrypted data”, Secure Data Management. LNCS, pp. 114- 127, 2011.

[13] C. Dong, G. Russello, N. Dulay. “Shared and searchable en- crypted data for untrusted servers”, Journal of Computer Security, pp. 367-397, 2011.

[14] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.