ISSN 2395-1621

A Survey on Group Data Sharing using Key-Aggregate Searchable Encryption (KASE) Technique in cloud

[#1]Amruta Nerlekar, [#2]Ankita Patil, [#3]Prof. Rugraj Purohit

[#123]Department of Computer,

Savitribai Phule Pune University

[123]Alard College of Engineering and Management Marunji, Pune-411057

ABSTRACT

It is required to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that for security one has to sacrifice functionality. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. Now we proposed 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 essential advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that when only the ciphertext is given the untrusted server cannot learn anything about the plaintext ; 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 arbitrary word without the user's authorization; they also support unseen queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length , the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Index Terms: **Cloud storage, data sharing, key-aggregate encryption, and patient-controlled encryption.**

ARTICLE INFO

Article History

Received: 28th November 2016

Received in revised form :

28th November 2016

Accepted: 30th November 2016

Published online :

2nd December 2016

I. INTRODUCTION

Private-key storage outsourcing permits clients with either limited resources or limited expertise to store and allocate large amounts of symmetrically encrypted data at low cost. Since regular private-key encryption prevents one from searching over encrypted data, clients also fail the ability to selectively retrieve segments of their data. To address this, Several techniques have been proposed for provisioning symmetric encryption with search capabilities to address this; the resulting concept is normally called searchable encryption. DARPA identified the area of searchable encryption, which is the technical advances that can be used to balance the need for both privacy and national security in information aggregation systems.

By secure index we can provisioning symmetric encryption with search capabilities. An index is a data structure that stores document collections while supporting efficient keyword search, i.e., given a keyword, the index returns a pointer to the documents that contain it. Informally, an index is "secure" if the search operation for a keyword *w* can only be performed by users that possess a "trapdoor" for *w* and if the trapdoor can only be generated with a secret key. Without knowledge of trapdoors, the index leaks no information about its contents. As shown by Goh in one can build a symmetric searchable encryption scheme from a secure. Index as follows: the client indexes and encrypts its document collection and sends the secure index together with the encrypted data to the server. If anybody wants to search for a keyword *w*, the client should generates and sends a trapdoor for *w* which the server uses to run the search operation and recover pointers to the appropriate (encrypted) documents. Symmetric searchable encryption can be achieved in its full generality and with optimal security using the work of Ostrovsky and

Goldreich. More specifically, using these techniques any type of search query can be achieved (e.g., conjunctions or disjunctions of keywords) without leaking *any* information to the server, not even the "access pattern" (i.e., which documents contain the keyword). This strong privacy assurance, however, comes at the cost of a logarithmic (in the number of documents) number of rounds of interaction for each read and write. Also in this paper, the authors show a 2-round solution, but with significantly larger square-root overhead. Therefore, the earlier mentioned work on searchable encryption efforts to reach more efficient solutions (typically in one or two rounds) by weakening the privacy guarantees.

II. LITERATURE SURVEY

[1] Rongxing Lu, Xiaodong Lin, Xiaohui Liang†, and Xuemin (Sherman) Shen "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing"

As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

[2]Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing"

In this paper, they propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

[3]Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing 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 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.

[4]Dawn Xiaodong Song David Wagner Adrian Perrig"Practical Techniques for Searches on Encrypted Data"

In this paper, they describe 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 crucial advantages.

[5]R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions Private-key storage outsourcing"

In this paper they begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

III. SYSTEM OVERVIEW

We consider a cloud computing architecture by merging with an example that a company uses a cloud to enable its staffs in the same group or department 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.

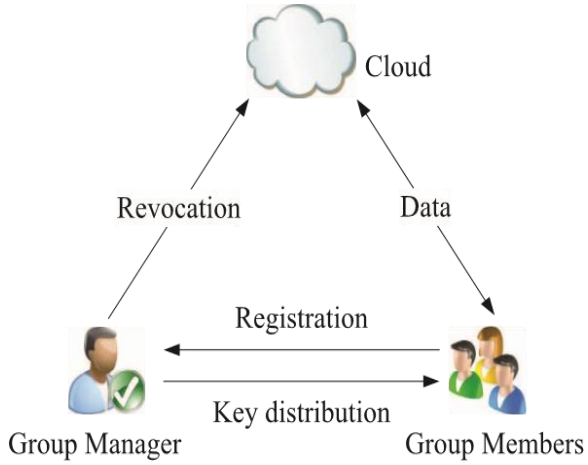

Fig.1 System Model

Cloud is worked by CSPs and provides valued plentiful storage services. However, the cloud is not fully reliable by users since the CSPs are very likely to be outside of the cloud users' reliable domain. Similar to [3], we assume that the cloud server is honest but interested. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, 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, user registration, user revocation, and revealing the actual identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, In our system we have to assume that the other parties are fully trusted to the group manager.

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, group members role is played by the staff. Note that, the group membership

is dynamically changed, due to the staff resignation and new employee participation in the company.

IV. OUR CONTRIBUTIONS

In modern cryptography, a fundamental problem we often study is about leveraging the secrecy of a small piece of knowledge into the ability to perform cryptographic functions (e.g. encryption, authentication) multiple times. In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size.

We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called *master-secret key*, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

With our solution, Alice can simply send Bob a single aggregate key via a secure e-mail. Bob can download the encrypted photos from Alice's Dropbox space and then use this aggregate key to decrypt these encrypted photos. The scenario is depicted in Figure 2.

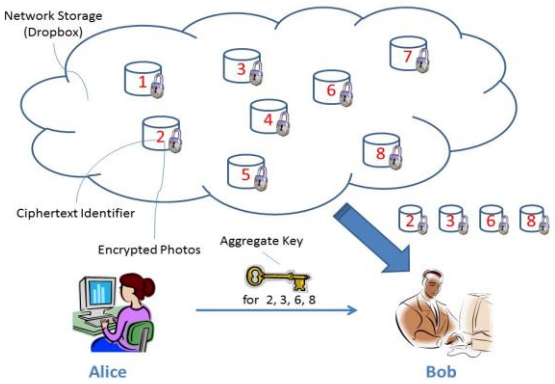

Figure 2 System Scenario

Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key.

The sizes of ciphertext, public-key, master-secret key and aggregate key in our KAC schemes are all of constant size. The public system parameter has size linear in the number of ciphertext classes, but only a small part of it is needed each time and it can be fetched on demand from large (but non-confidential) cloud storage.

V. CONCLUSION

In this paper we have described new techniques by using an untrusted server and provided proofs of security we are resulting crypto systems for remote searching on encrypted data. Our techniques have a number of essential advantages: they are provably secure; they support controlled and hidden search and query isolation; they are simple and fast (More specifically, length of document, 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 flexible, and it can simply be extended to support more advanced search queries. We concluded that this provides a powerful new building block for the construction of secure services in the untrusted infrastructure.

REFERENCES

[1] 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.

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

[3] 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.

[4] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[5] 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.

