International Journal of Research

Available at https://edupediapublications.org/journal

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Key aggregate Searchable Encryption (KASE) for Group Data Sharing through Cloud Storage

Jasim Mohammed Kadhim
NIZAM COLLEGE (AUTONOMOUS) OSMANIA UNIVERSITY, HYDERABAD.

amerjaber7818@Gmail.com

Abstract- 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 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.

Keywords: Aggregate key cryptosystem, Cloud storage, data sharing, key-aggregate encryption. Diffe Hellman key exchange technique.

1. INTRODUCTION:

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented

applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.
The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

2. System Objective

The Goal of the framework is to give best answer for the Current issue is that Alice scrambles records with unmistakable open keys, yet just sends Weave a solitary (steady size) unscrambling key while sharing the documents figure content class list likewise extensive when a same client shares various records class list stay consistent i.e no variety in class list. Since the decoding key ought to be sent by means of a safe channel and kept mystery, little key size is constantly alluring. Utilizing The general population key Cryptosystem (open key Encryption calculation)

Issue DEFINITION:-

The testing issue is the means by which to successfully same client share numerous scrambled documents in this manner class record stays same (steady). Obviously clients can download the individual or mass scrambled documents from the capacity, unscramble them, then send them to others for sharing, however it loses the estimation of distributed storage. Clients ought to have the capacity to assign the entrance privileges of the sharing information to others so they can get to these information from the server straightforwardly

SCOPE:-

We Can ensure clients' information protection is a focal inquiry of distributed storage. With more scientific instruments, cryptographic plans are getting more flexible and regularly include different keys for a solitary application. In this paper, we consider how to "pack" mystery keys in broad daylight key cryptosystems which bolster appointment of mystery keys for various figure content classes for various client and a solitary figure content class file stays steady for same client in distributed storage. Regardless of which one among the force set of classes, the representative can simply get a total key of consistent size.

PROBLEM TESTIMONIAL

=There is a rich literature on searchable encryption, including SSE schemes and PEKS schemes. 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 focus to such a MUSE scenario, although they all adopt single-key combined with access control to achieve the goal.
In 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 attribute based encryption (ABE) is applied to achieve fine-grained access control aware keyword search. As a result, in MUSE, the main problem is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered.

Consistent size decoding key require pre-characterized various leveled relationship. The

altered order is utilized. In that there is stand out path in which we can segment the record. On the off chance that we need to give out access rights in view of something else (e.g. taking into account report sort or affectability of information) we will need to take a gander at all the low-level classes included, and give a different decoding key for each [2]. More number of decoding key was utilized [1].

3. RELATED WORK

SYMMETRIC-KEY ENCRYPTION WITH COMPACT KEY AGGREGATE CRYPTOSYSTEM

The proposed system style AN economical public-key encoding theme that supports versatile allocation. In this scheme any set of the cipher texts (produced by the encoding scheme) is rewrite by a constant-size secret writing key (generated by the man of affairs of the master-secret key). We solve this downside by introducing a special sort of public-key encoding known as keyaggregate cryptosystem (KAC). In KAC, users encrypt a message not solely underneath a public-key, but additionally underneath AN symbol of cipher text known as category. Such that cipher texts are any classified into completely different categories. The owner of the key holds a master-secret called Master secret key [5].

The master-secret can be wont to extract secret keys for various categories. More significantly, the extracted key have can be AN combination key that is as compact as a secret key for one category, but aggregates the power of the many such keys, such that the decryption power for any set of cipher text categories. By this solution, Alice can merely send Bob a single combination key via a secure channel like email. Bob can transfer the encrypted photos from Alice's Drop box house and then use this combination key to rewrite these encrypted pictures.

4. PROPOSED STRUCTURE

In this paper, 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.

To support searchable group data sharing the main requirements for efficient key management are twofold. First, 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. Second, 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.

We first define a general framework of key aggregate 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.

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.

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.

5. CONCLUSION

In this paper outsourcing of data to cloud server through system with secure way. For the security of information we tend to ar exploitation various cryptography procedure ar utilized. One of the strategies for key total cryptosystem for era of mystery key with totally distinctive arrangement of mystery keys. In this paper we ar anticipated considered progressed diffie writer key trade for era of mystery with different arrangement of mystery keys. Utilizing this key the learning proprietor or client can figure and change keep information into cloud. By performing encoding and decipherment of information we tend to ar exploitation progressed XOR cryptography strategy. By executing those systems we give mystery and classification of data.

REFERENCES

[1] H.Fareesa Firdose , R.Deepthi Crestose Rebekah,"A Key Aggregate Construction with Adaptable Offering of Information in Cloud " [2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, Privacy- Preserving Public Auditing for Secure Cloud Storage, IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.

[3] S.Kamara and K.Lauter,—Cryptographic Cloud Storage,Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.

[6] 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.

[7] M. Chase and S. S. M. Chow, Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, in ACM Conference on Computer and Communications Security, 2009, pp. 121–130

[8] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[10] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp.89–98.

JASIM MOHAMMED KADHIM
MSCIS From NIZAM COLLEGE
(AUTONOMOUS) OSMANIA
UNIVERSITY, HYDERABAD.
9676941886, jasimmohammed549@gmail.com