A Study on Aggregate Trapdoor for Group Data Sharing Via Could Storage

[1]M. Sowjanya,[2]T.Neetha

[1]M.Tech Student, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, India[2]Associate Professor, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, India

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: Asymmetric, Cloud storage, Data Sharing, Encryption, Key Aggregate.

INTRODUCTION:

Nowadays the storage in the cloud has materialized as a capable answer for suitable and on-demand accesses to huge amounts of information shared over the Internet. Business users are being paying attention by cloud storage due to its several benefits, including lower cost, better agility, and improved resource utilization. Everyday users are also sharing private data, such as photos and videos, with their friends through social network applications based on cloud.

On the other hand, while benefiting from the expediency of sharing data through cloud storage, users are also gradually worried about accidental data reveal by the cloud. Such data revealing, will be performed by malicious opponent or a mischievous cloud operator, can habitually direct to severe violation of private data or confidential data regarding bussiness. To speak about users anxiety over possible data reveal in cloud storage, a general approach is for the data owner to encrypt all the data before uploading them in to the cloud, such that presently the encrypted data may be get back and decrypted by individuals who contains the decryption keys. Such cloud storage is often called the cryptographic cloud storage .Though; the encryption of data builds it demanding for users to search and then preferable retrieve only the data including the 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 retrieving data matching a keyword, the user will send the matching keyword to the cloud to react for the search over the encrypted data. Even though merging a searchable encryption Scheme with cryptographic cloud storage can accomplish the essential security needs of a cloud storage, executing such a system for large scale application relating huge number of users and large number of files may still be delayed by realistic issues relating the well-organized management of encryption keys, which, to the finest of our knowledge. Primarily, the want for selectively sharing encrypted data with different users usually demands different encryption keys to be used for different files. On the other hand, this involves the number of keys that need to be spread to users, both for them to search over the encryped files and to decrypt the files, will be relative to the number of such files. Such a large number of keys must not only be spread to users via secure channels, but also be securely stored and handled by the users in their devices. The implicit requirement for secure communication, storage, and computational difficulty may cause system ineffectiveness.

RELATED WORK:

They consider the problems that arise in a naive attempt to add security to such a system. They argue above that they want to allow the patient to produce their own decryption key. But here in this case, how the patient can allow others to access their record is a question. So, clearly their does not want to give their entire key, because if other recipient who got their entire key can modify or read all the parts of her record. The patient can grant access to a category easily and even without knowing what types of files are already exists that might ultimately be included in it. But, the hierarchy is fixed in that there is only one way in which they can partition the record. If they want to give out the access rights based on something else like example based on document type or sensitivity of data, they have to take care of all the low level categories involved, and they has to provide a separate decryption key for each. Example like giving a access to a lab report to all X-rays would require giving separate keys for Cardiologic X-rays, Dental X-rays and Mental Health Xrays.

PROPOSED SYSTEM:

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 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:

The conclusion of this paper is as follows. To share the data in a secure way, the required tool is encryption. Asymmetric key encryption is a more secure way to share the data than symmetric key encryption because it uses two keys, public key and private key. Among these two keys, either of the keys is used for encryption and decryption.

REFERENCES:

[1] L. Hardesty, “Secure computers aren’t so secure,” MIT press, 2009.

[2] 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.

[3] 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.

[4] 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

[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] D. Boneh, R. Canetti, S. Halevi, and J. Katz, “ChosenCiphertext Security from Identity-Based Encryption,” SIAM Journal on Computing (SIAMCOMP), vol. 36, no. 5, pp. 1301–1328, 2007.

[8] D. Boneh, X. Boyen, and E.-J. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” in Proceedings of Advances in Cryptology - EUROCRYPT ’05, ser. LNCS, vol. 3494. Springer, 2005, pp. 440–456.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. “Public Key Encryption 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: PairingBased Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.