IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 72-76
www.iosrjournals.org

A Paper On secure multi-owner group data search by using aggregate key

Salman Mujawar
(*RSCOE, University of Pune, Pune, Maharashtra India*)

Abstract: *The ability of specifically imparting scrambled information to distinctive clients through open distributed storage might significantly ease security worries over incidental information spills in the cloud. A key test to outlining such encryption plans lies in the productive administration of encryption keys. The sought adaptability of offering any gathering of chose reports to any gathering of clients requests distinctive encryption keys to be utilized for diverse archives. Notwithstanding, this likewise infers the need of safely dispersing to clients a substantial number of keys for both encryption and look, and those clients will need to safely store the got keys, and present a just as extensive number of keyword trapdoors to the cloud with a specific end goal to perform seek over the mutual information. The suggested requirement for secure correspondence, stockpiling, and many-sided quality obviously renders the methodology unreasonable. In this paper, we address this viable issue, which is to a great extent dismissed in the proposing so as to write, the novel idea of key aggregate searchable encryption (KASE) and instantiating the idea through a solid KASE plan, in which an information proprietor just needs to convey a solitary key to a client for sharing countless, and the client just needs to present a solitary trapdoor to the cloud for questioning the mutual reports. The security examination and execution assessment both affirm that our proposed plans are provably secure and for all intents and purposes effective.*

Keywords: cloud *storage , data sharing, , data privacy, Searchable encryption,*

I. Introduction

Considering the down to earth issue of security safeguarding information sharing framework in light of open cloud stockpiling which obliges an information proprietor to convey a substantial number of keys to clients to empower them to get to his/her reports, we interestingly propose the idea of key-aggregate searchable encryption (KASE) and develop a solid KASE plan. Both investigation and assessment results affirm that our work can give a successful answer for building down to earth information sharing framework in light of open cloud stockpiling. In a KASE plan, the proprietor just needs to appropriate a solitary key to a client when offering heaps of archives to the client, and the client just needs to present a solitary trapdoor when he inquiries over all records shared by the same proprietor. In any case, if a client needs to inquiry over reports shared by numerous proprietors, he must create different trapdoors to the cloud. The most effective method to lessen the quantity of trapdoors under multi-proprietors setting is a future work. In addition, united clouds have pulled in a considerable measure of consideration Now a days, yet our KASE can't be connected for this situation straightforwardly. It is additionally a future work to give the answer for KASE on account of combined clouds.
There is a rich writing on searchable encryption, counting SSE plans [1]–[8] and PEKS plans [9]–[15]. As opposed to those current work, in the setting of distributed storage, keyword search under the multi-tenancy setting is a more normal scenario.

II. Literature Survey

2.1) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing
AUTHORS**:** Shucheng Yu, Cong Wang

Cloud computing transforms the way information technology(IT) is expended and oversaw, promising enhanced Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies basedon data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption .Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

2.2) Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing.
AUTHORS: Rongxing Lu

Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme basedon the bilinear pairing techniques. 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.

2.3) Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud
AUTHORS**:** Xuefeng Liu

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users.Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from anuntrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we 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.

2.4) Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage
AUTHORS**:** Cheng-Kang Chu, Sherman S. M. Chow

Data sharing 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 cipher texts such that efficient delegation of decryption rights for any set of cipher texts 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. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently 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.

III. Existing System

The data before exchanging them to the cloud, such that later the mixed data may be recoup and decoded by the people who have the unscrambling keys. Such disseminated stockpiling is every now and again called the cryptographic conveyed stockpiling. In any case, the encryption of data makes it striving for customers to request and after that particularly recoups only the data containing given vital words. A normal course of action is to use a searchable encryption (SE) plan in which the data proprietor is obliged to scramble potential conclusive words and exchange them to the cloud together with encoded data, such that, for recuperating data planning a watchword, the customer will send the contrasting enchantment word trapdoor with the cloud for performing chase over the mixed data.

2.4) Disadvantages

1. 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.

2. 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.

2.5) Proposed System

We address this test by proposing the original thought of key-aggregate chase skilled encryption (KASE), and instantiating the thought through a strong KASE arrangement. The proposed KASE arrangement applies to any disseminated stockpiling that sponsorships the searchable social event data sharing handiness, which infers any customer may particularly grant a get-together of picked files to a get-together of picked customers, while allowing the later to perform vital word look over the past. To support searchable social event data sharing the guideline essentials for efficient key organization are two.

3.2.1) Advantages:

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.

3.2.2) Disadvantages:

KASE scheme has only one key is used for data access & searching hence it becomes challenging to maintained security on that single key.

IV. System Architecture

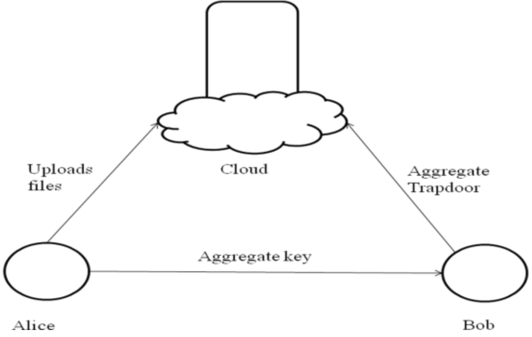

Figure. The system model

2.6) Modules

4.1.1) Setup

This algorithm is run by the cloud service provider to set up the scheme. On input of a security parameter and the maximum possible number n of documents which belongs to a data owner, it outputs the public system parameter prams.

4.1.2) Keygen

This algorithm is run by the data owner to generate a random key pair.

4.1.3) Encrypt

This algorithm is run by the data owner to encrypt the document and generate its keywords' cipher texts. For each document, this algorithm will create for its searchable encryption key. On input of the owner's public key and the file index, this algorithm outputs data cipher text and keyword cipher texts.

4.1.4) Extract

This algorithm is run by the data owner to generate an aggregate searchable encryption key for delegating the keyword search right for a certain set of documents to other users. It takes as input the owner's master-secret key and a set which contains the indices of documents, then outputs the aggregate key.

4.1.5) Trapdoor

This algorithm is run by the user who has the aggregate key to perform a search. It takes as input the aggregate searchable encryption key and a keyword, then out- puts only one trapdoor.

4.1.6) Test

This algorithm is run by the cloud server to perform keyword search over an encrypted document. It takes as input the trapdoor and the document index , then outputs true or false to denote whether the document contains the keyword.

V. Conclusion

Considering the pragmatic issue of security saving information sharing framework taking into account open cloud stockpiling which obliges an information proprietor to appropriate a substantial number of keys to clients to empower them to get to his/her records, we surprisingly propose the idea of key-aggregate searchable encryption (KASE) and develop a solid KASE plan. Both examination and assessment results affirm that our work can give a powerful answer for building functional information sharing framework taking into account open cloud stockpiling. In a KASE plan, the proprietor just needs to disperse a solitary key to a client when imparting loads of reports to the client, and the client just needs to present a solitary trapdoor when he inquiries over all records shared by the same proprietor. On the other hand, if a client needs to question over archives shared by different proprietors, he must produce various trapdoors to the cloud. The most effective method to decrease the quantity of trapdoors under multi-proprietors setting is a future work. Additionally, unified clouds have pulled in a great deal of consideration these days, yet our KASE can't be connected for this situation specifically. It is additionally a future work to give the answer for KASE on account of united clouds.

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]. 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 multiowner 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 constructions”,In: Proceedings of the 13th ACM conference on Computer 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 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: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11]. J. Li, Q. Wang, C. Wang. “Fuzzy keyword search over encrypted 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 encrypted 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.

[15]. 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.

About Author

Salman Mujawar received B.E degree in Computer Engineering from Shivaji University, Kolhapur ,India in 2014 and pursuing ME degree in Computer Science and Engineering from Rajarshi Shahu College of Engineering, Pune, India.