Volume 2, Issue 11, November-2015, pp. 867-871 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Key-Aggregate Crypto System for Reliable Outsourced Data among Public Cloud

[1]SHOBAN DEVARAPALLI, [2]R.MADHURI DEVI

[1]M.Tech (CSE), Priyadrshini Institute of Technology & Management

[2]AssociateProfessor (Dept.of CSE), Priyadrshini Institute of Technology & Management

Abstract— The capacity of in particular sharing encrypted data with divergent to clients through public cloud storage may truly ease security trouble, by plausibility data uncover in the cloud. A key test to plan such encryption thought lies in the very much sorted out administration encryption keys. The favored adaptability of distributing any attaining so as to gather reports with any gathering of clients weight distinctive encryption keys to be utilized for diverse archives. Then again, this includes the need of safely disseminating to clients by a substantial number of keys for both encryption and seeks, and those clients need to advance to store the got keys. The aberrant requirement for secure correspondence, storage, and many-sided quality plainly cause the outlandish methodology. In this paper, we focus on this viable issue, by recommending the novel idea of key aggregate searchable encryption (KASE) and instantiating the thought through a genuine KASE plan, in which a data proprietor needs to share out a solitary key to a client for disseminating an extensive number of reports, and the client needs to display a solitary trapdoor to the cloud for scrutinizing the mutual archives.

Keywords—data sharing, Searchable encryption, data privacy, cloud storage

1 INTRODUCTION

These days the storage in the cloud has appeared as a fit response for suitable and on interest gets to immense measures of data shared over the Web. Business clients are being focused by cloud storage because of it's few advantages, including lower cost, better nimbleness, and enhanced asset usage. Regular clients are likewise sharing private data, for example, photographs, and recordings, with their companions through informal organization applications in view of the cloud. Then again, while profiting from the convenience of sharing data through cloud storage, clients are likewise biting by bit stressed over unplanned data uncover by the cloud. Such data uncovering, will be performed by a vindictive adversary or an evil cloud administrator, can frequently direct to the serious infringement of private data or secret data with respect to business. To talk about client's uneasiness over conceivable data uncover in cloud storage, a general methodology is for the data proprietor to encode all the data before transferring them into the cloud, such that in no time the encrypted data might get back and unscrambled by people who contains the decoding keys. Such cloud storage is frequently called the cryptographic cloud storage [6].Though; the encryption of data manufactures it requesting for clients to look and after that best recover just the data including the given keywords. A typical arrangement is to utilize a searchable encryption (SE) plan in which the data proprietor is required to scramble potential keywords and transfer them to the cloud together with encrypted data, such that, for recovering data coordinating a keyword, the client will send the coordinating keyword to the cloud to respond for the hunt over the encrypted data.

Despite the fact that combining a searchable encryption Plan with cryptographic cloud storage can fulfil the fundamental security needs of a cloud storage, executing such a framework for substantial scale application relating immense number of clients and huge number of documents

might even now postponed by practical issues relating the very much sorted out administration of encryption keys, which, to the finest of our insight. Essentially, the need for specifically sharing encrypted data with diverse clients more often than not requests distinctive encryption keys to be utilized for diverse records. Then again, this includes the quantity of keys that should be spread to clients, both for them to seek the encrypted records and to unscramble the documents, will be in respect to the quantity of such documents. Such a substantial number of keys must not just be spread to clients by means of secure channels, additionally, be safely put away and took care of by the clients in their gadgets. The verifiable prerequisite for secure correspondence, storage, and computational trouble might bring about framework insufficiency.

In this paper, we propose the novel idea of key aggregate searchable encryption (KASE) and instantiating the idea through a solid KASE technique. The proposed KASE plan identifies with any cloud storage those backings the searchable gathering data sharing element, which implies any client, might want to disseminate a gathering of documents which are specific with a gathering of close clients while allowing the last to complete keyword look over the prior. To keep up searchable gathering data sharing the principle requirements for effective key administration are twofold. Fundamentally, a data proprietor needs to allow a solitary aggregate key (rather than a gathering of keys) to a client for sharing any number of records. Ensuing, the client needs to present a solitary aggregate trapdoor to the cloud for performing keyword look over any amount of shared documents. KASE plan can guarantee both solicitations.

2. RELATED WORK:

1) Primarily we describe a common structure of keyaggregate searchable encryption (KASE) collected from several polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. We then explain both functional and security requirements for scheming a valid KASE scheme.

2) We then instantiate the KASE skeleton by Scheming a concrete KASE scheme. After giving the full structure for the algorithms, we analyze the effectiveness of the scheme, and set up its saftey through detailed analysis.

2.1 Searchable Encryption:

Searchable encryption schemes categorized into two categories, i.e., searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS). Both SSE and PEKS can be described as the tuple SE= (Setup, Encrypt, Trapdoor(Trpdr),Test):

1. **Setup**(1^{λ}): This algorithm is run by the owner to set up the scheme. It takes as input a security parameter 1^{λ} and outputs the necessary keys.
2. **Encrypt**(l;n): This algorithm is run by the owner to encrypt the data and generate its keyword ciphertexts. It takes as input the data n, owner's necessary keys including searchable encryption key l and data encryption key, outputs data ciphertext and keyword ciphertexts Cn.
3. **Trpdr**(l;x): This algorithm is run by a user to generate a trapdoor Trd for a keyword w using key l.
4. **Test**(Trd, Cn): This algorithm is run by the cloud server to perform a keyword search over encrypted data. It takes as input trapdoor Trd and the keyword ciphertexts Cn, outputs whether Cn contains the specified keyword. For exactness, it is required that, for a message n containing keyword x and a searchable encryption key l, if (Cn←-Encrypt(l;n) and Tr ←Trpdr(l;x)), then Test(Trd, Cn)=true.

3. THE KEY-AGGREGATE SEARCHABLE ENCRYPTION (KASE) CONSTRUCTION:

In this paper, we propose the novel approach of Key-aggregate searchable encryption (KASE) as a enhanced solution, as depicted in Fig.1(b). , in KASE, seeta needs to issue a single aggregate key, instead of $\{k_i\}^{m}_{i=1}$ for sharing m documents with Ram, and ram needs to issue a single aggregate trapdoor, instead of $\{ Tr_i \}^{m}_{i=1}$, to the cloud server. The cloud server can utilize this aggregate trapdoor and some public data to carry out keyword search and revisit the result to Ram. As a result, in KASE, the delegation of keyword search right can be achieved by sharing the single aggregate key.

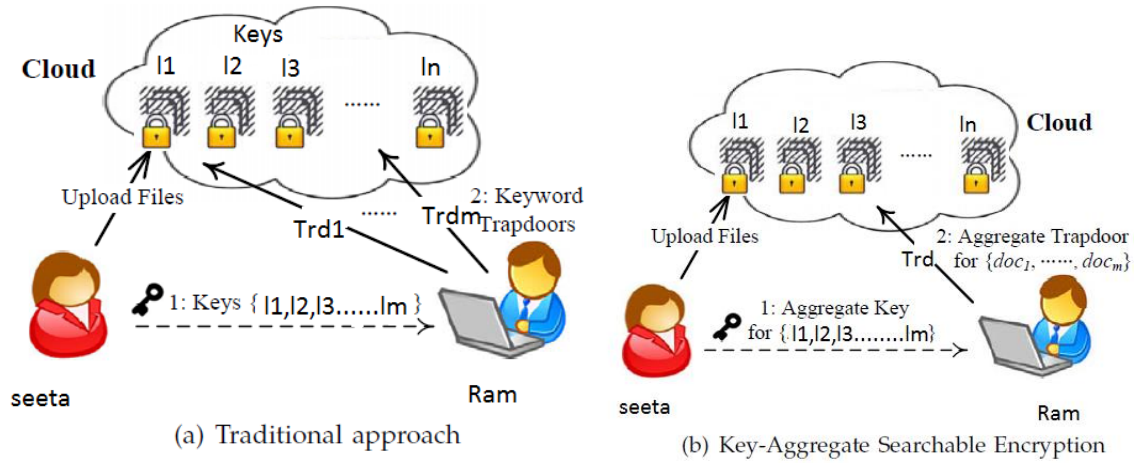
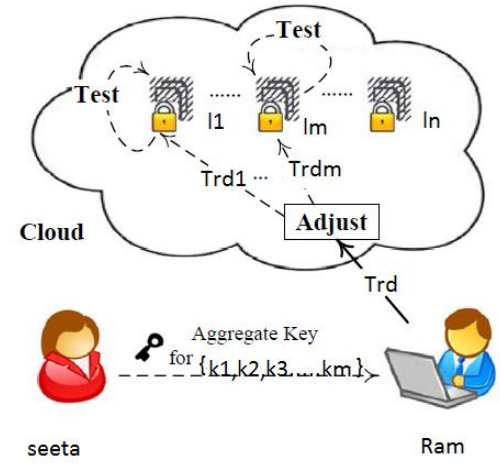


Fig 1.Keyword Search in group data sharing system

To design a key-aggregate searchable encryption method under which any subset of the keyword ciphertext from any set of documents is searchable with a constant-size trapdoor generated by a constant size aggregate key.

Fig. 2. Framework of key-aggregate searchable encryption.



3.2 The KASE construction

The KASE construction is composed of several algorithms. Specially, to set up the method, the cloud server would generate public parameters of the system during the **Setup** algorithm, and these public parameters can be reprocess by dissimilar data owners to distribute their files. For each data owner, they should produce a public/master-secret key pair through the **Keygen** algorithm. Keywords of each document can be encrypted through the **Encrypt** algorithm with the exclusive searchable encryption key. In that case, the data owner can apply the master-secret key to produce an aggregate searchable encryption key for a group of selected documents through the **Extract** algorithm. The aggregate key can be spread securely to approve users who need to access those documents. After that, as shown in Fig.2, an certified user can create a keyword trapdoor via the **Trapdoor** algorithm using this aggregate key, and submit the trapdoor to the cloud. After getting the trapdoor, to carry out the keyword search over the particular set of documents, the cloud server will run the **Adjust** algorithm to produce the right trapdoor for each document, and then run the **Test** algorithm to test whether the document contains the keyword.

This construction is summarized in the following.

1. Setup(1^λ, n): This algorithm is run by the cloud service provider to set up the scheme. On input of a security parameter 1^λ and the maximum possible number n of documents which belongs to a data owner, it outputs the public system parameter params.

2. **Keygen**: This algorithm is run by the data owner to generate a random key pair (pk,msk).

3.**Encrypt**(pk, i): This algorithm is run by the data owner to encrypt the i-th document and generate its keywords' ciphertexts. For each document, this algorithm will create a delta ⊿i for its searchable encryption key ki. On input of the owner's public key pk and the file index i, this algorithm outputs data ciphertext and keyword ciphertexts Ci.

3. **Extract**(msk, S): This algorithm is run by the data owner to generate an aggregate searchable encryption key for hand over the keyword search right for a certain set of documents to other users. It takes as input the owner's master-secret key

msk and a set S which enclose the directory of documents, and then outputs the aggregate key kagg.

4. **Trapdoor** (kagg, x): 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 kagg and a keyword w, then outputs only one trapdoor Trd.

5. **Adjust** (params, i, S, Trd): this algorithm is run by cloud server to adjust the aggregate trapdoor to generate the right trapdoor for each different document. It takes as input the system public parameters params, the set S of documents' indices, the index i of target document and the aggregate trapdoor Tr, then outputs each trapdoor Tri for the i-th target document in S.

6.**Test**(Tr_i, i): this algorithm is run by the cloud server to perform keyword search over an encrypted document. It takes as input the trapdoor Tr_i and the document index i, then outputs true or false to denote whether the document doc_i contains the keyword w.

4. CONCLUSION & FUTURE ENHANCEMENT

Contemplating of the sensible issue of security protecting data sharing framework in light of public cloud storage which needs a data proprietor to distribute an expansive number of keys to clients to allow them to get to the records, in this proposed idea of key aggregate searchable encryption (KASE) and develop a solid KASE plan. It can give a productive answer for building useful data sharing framework in light of public cloud storage. In a KASE plan, the proprietor needs to circulate a solitary key to a client while contributing a considerable measure of reports with the client, and the client need to present a solitary trapdoor when they question overall records shared by the same proprietor. Then again, if a client needs to address over reports shared by numerous proprietors, that client must create different trapdoors to the cloud. The future improvement for this proposed work is to figure out how to diminish the quantity of trapdoors under multi-proprietors attaining so as to set the security.

REFERENCES

[1] Baojiang Cui, Zheli Liu and Lingyu Wang : Key-Aggregate Searchable Encryption for Group Data Sharing via Cloud Storage, IEEE Transactions On Computers, Vol. 6, No. 1, January 2014

[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.
[16] J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689,
Elsevier, 2010.
[17] X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures", IEEE Trans. on Parallel and Distributed Systems,
DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180, 2013.
[18] J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.
[19] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249-255, 2013.
[20] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing",
Proc. IEEE INFOCOM, pp. 525-533, 2010.
[21] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507- 525, 2012.
[22] D. Boneh, C. Gentry, B. Waters." Collusion resistant broadcast encryption with short ciphertexts and private keys", Advances in CryptologyCCRYPTO 2005, pp. 258-275, 2005.
[23] D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts", International journal of information security, 12(4):251-265, 2013.
[24] D. Boneh, B. Lynn, H. Shacham. "Short signatures from the Weil pairing", Advances in Cryptology ASIACRYPT 2001, pp. 514-532, 2001.

