International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

Smital Erande[1], V. S. Ranmalkar[2]

[1]Savitribai Pule Pune University, VACOE, Ahmednagar

[2]Professor, Savitribai Pule Pune University, VACOE, Ahmednagar

Abstract: ***Over incidental information spills in the cloud there might enormously wide security worries with various clients through open distributed storage due to the capacity of specifically scrambled information sharing. In the effective encryption keys administration, to generate such encryption plans, falsehoods is a key test. For various records, with any gathering of clients' requests for diverse encryption keys, any gathering of those documents to be utilized the fancied adaptability of sharing. In any case, for both encryption and pursuit, to clients countless the need of disseminating safely and to safely store the got keys likewise suggests those clients will have and to perform seek over the common information submit to the cloud all together a just as vast number of watchword trapdoors. The methodology is not feasible for the inferred requirement for secure stockpiling, multifaceted nature and correspondence unmistakably renders. In this paper, by idea instantiating through the plan of a solid KASE and proposing the idea of key-total searchable encryption (KASE), we address this down to earth issue. In the writing this issue was generally dis-regarded, in which countless sharing to a client, there necessities just to appropriate a solitary key an information proprietor, and the client requirements for questioning the mutual archives for presenting a solitary trapdoor to the cloud.***

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

1. Introduction

Over the Internet for giving advantageous, omnipresent and for a lot of shared information's on-interest gets to, there has developed as a promising arrangement by distributed storage. Today, taking into account distributed storage through informal organization applications, individual information, for example, photographs and recordings are imparted by a large number of clients to their companions once a day. Because of its various lower cost, better asset use and more prominent dexterity, by distributed storage the business clients are likewise being pulled in.

In any case, worried of clients about coincidental information spills in the cloud additionally progressively by means of distributed storage while getting a charge out of the accommodation of sharing information. There can as a rule lead to genuine breaks of individual protection or business mysteries because of such information spills. Over potential information spills in distributed storage to address clients' worries, all the information scrambled before transferring them to the cloud is the regular methodology for the information proprietor, such that later by the individuals who have the decoding keys, the encoded information might be recovered and unscrambled which is known as the cryptographic distributed storage. In any case, for clients to pursuit and after that specifically recover just the information containing given watchwords, the encryption of information makes it testing. To utilize a searchable encryption (SE) conspire, a typical arrangement is in which potential catchphrases are scramble by information proprietor and together with encoded information transfer them to the cloud, such that, for performing seek over the scrambled information, the client will send the relating watchword trapdoor to the cloud for recovering information coordinating a catchphrase.

The fundamental security necessities of a distributed storage can accomplish by the distributed storage in spite of the fact that joining a searchable encryption plan with cryptographic, for extensive scale applications, executing such a framework including a great many clients and by functional issues including billions of documents might in any case be blocked the effective administration of encryption keys, which, are generally overlooked in the writing to the best of our insight. Most importantly, for various records which the requirement for specifically imparting scrambled information to various clients, there as a rule requests diverse encryption keys to be utilized. Such a substantial number of keys must be safely put away and oversaw and in addition circulated to clients by means of secure channels, by the clients in their gadgets. What's more, by the clients there must be created countless and keeping in mind the end goal to perform a catchphrase seek over numerous records submitted to the cloud. Such a framework wasteful and unfeasible the inferred requirement for secure computational multifaceted nature, correspondence and capacity might render.

In this paper by proposing the novel idea of KASE, we address this test and through a solid KASE plan instantiating the idea. To any distributed storage there applies the proposed KASE plan which underpins the usefulness of searchable gathering information sharing, which implies that, any client might specifically impart the gathering of chose documents to a chose clients gathering, to perform catchphrase look over the previous while permitting the last mentioned. For proficient key administration the primary prerequisites are twofold to support searchable gathering information sharing. To start with, for sharing any number of records, an information proprietor just needs to circulate a solitary total key to a client. Second, over any number of shared records for performing watchword look, there just needs to present the client to the cloud a solitary total

trapdoor. To the best of our insight, in this paper the KASE plan proposed can fulfill both prerequisites.

Contributions: More particularly, takes after are our primary commitments.

1) For era of key, setup of security parameter, key extraction, encryption, era of trapdoor, modification of trapdoor, and testing of trapdoor, we first characterize a general KASE system which make seven polynomial algorithms. For outlining a substantial KASE plan we then portray the prerequisites of both utilitarian and additionally security.
2) After planning plan of a solid KASE, we then instantiate the KASE structure. For the seven algorithms in the wake of giving point by point developments, we build up its security through nitty gritty examination and investigate the proficiency of the plan.
3) Based on the proposed KASE plan, in building a real gathering information sharing framework we talk about different commonsense issues and assess its execution.

There is a rich literature on searchable encryption, including SSE schemes [5] [8] and PEKS schemes [9] [15]. 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 [6], [13] [15], [19] focus to such a MUSE scenario, although they all adopt single-key combined with access control to achieve the goal. In [6], [19], MUSE schemes are constructed by sharing the documents searchable encryption key with all users who can access it, and broadcast encryption is used to achieve coarse-grained access control. In [13] [18], 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. Key aggregate searchable encryption can provide the solution for the latter, and it can make MUSE more efficient and practical.

In the case of a multi-user application, considering that the number of trapdoors is proportional to the number of documents to search over (if the user provides to the server a keyword trapdoor under each key with which a matching document might be encrypted), Popa [28] firstly introduces the concept of multi-key searchable encryption (MKSE) and puts forward the first feasible scheme in 2013.

MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoors keyword in documents encrypted with different keys. This might sound very similar to the goal of KASE, but these are in fact two completely different concepts. The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user. This approach of MKSE inspires us to focus on the problem of keyword search over a group of shared documents from the same user in the multiuser applications, and the adjust process in MKSE also provides a general approach to perform keyword search over a group of documents with only one trapdoor. However, the adjust process of MKSE needs a delta generated from both users key and SE key of the document, so it does not directly apply to the design of a concrete KASE scheme.

Data sharing systems based on cloud storage have attracted much attention recently [1][4]. In particular, Chu et al. [4] consider how to reduce the number of distributed data encryption keys. To share several documents with different encryption keys with the same user, the data owner will need to distribute all such keys to him/her in a traditional approach which is usually impractical. Aiming at this challenge, a keyaggregate Encryption (KAE) scheme for data sharing is proposed to generate an aggregate key for the user to decrypt all the documents. To allow a set of documents encrypted by different keys to be decrypted with a single aggregate key, user could encrypt a message not only under a public-key, but also under the identifier of each document. The construction is inspired by the broadcast encryption scheme [27]. In this construction, the data owner can be regarded as the broadcaster, who has public key pk and master-secret key msk; each document with identifier i can be regarded as a receiver listening to the broadcast channel, and a public information used in decryption is designed to be relevant to both the owners msk and the encryption key; the message encryption process is similar to data encryption using symmetric encryption in BE, but the key aggregation and data decryption can be simply regarded as the further mathematical transformation of BE. Encrypt algorithm and BE. Decrypt algorithm respectively.

2. Literature Survey

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.

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

based on 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.

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.

With the characters of low maintenance and little management cost, cloud computing offers an effective and economical approach for data sharing in the cloud among group members. However, since the cloud is untrustworthy, the security guarantees for the sharing data become our concerns. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue. Recently, Liu et al presented a secure multi-owner data sharing scheme, named Mona, which was claimed that any group member could anonymously share data with others by exploiting group signature technique. Meanwhile, the scheme could address fine-grained access control, which means that not only the group members could use the sharing data resource at any time, but also the new users were able to use the sharing data immediately after their revocations and the revoked users will not be allowed to use the sharing data again after they are removed from the group. However, through our security analysis, the Mona scheme still has some security vulnerabilities. It will easily suffer from the collusion attack, which can lead to the revoked users getting the sharing data and disclosing other legitimate members' secrets. In addition, there is another security shortage in the user registration phase, which is how to protect the private key when distributing it in the unsecure communication channels. This kind of attack can also lead to disclosing the user's secret data.

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.

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 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. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext 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.

X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures", IEEE Trans on parallel and Distributed system DOI ieeecomputer society.org/10.1109/TPDS.2013.180,2013

Attribute-based signature (ABS) enables users to sign messages over attributes without revealing any information other than the fact that they have attested to the messages. However, heavy computational cost is required during signing in existing work of ABS, which grows linearly with the size of the predicate formula. As a result, this presents a significant challenge for resource-constrained devices (such as mobile devices or RFID tags) to perform such heavy computations independently. Aiming at tackling the challenge above, we first propose and formalize a new paradigm called Outsourced ABS, i.e., OABS, in which the computational overhead at user side is greatly reduced through outsourcing intensive computations to an untrusted signing-cloud service provider (S-CSP). Furthermore, we apply this novel paradigm to existing ABS schemes to reduce the complexity. As a result, we present two concrete OABS schemes: i) in the first OABS scheme, the number of exponentiations involving in signing is reduced from O(d) to O(1) (nearly three), where d is the upper bound of threshold value defined in the predicate; ii) our second scheme is built on Herranz et al.'s construction with constant-size signatures. The number of exponentiations in signing is reduced from O(d2) to O(d) and the communication overhead is O(1). Security analysis demonstrates that both OABS schemes are secure in terms of the unforgeability and attribute-signer privacy definitions specified in the proposed security model. Finally, to allow for high efficiency and flexibility, we discuss extensions of OABS and show how to achieve accountability as well.

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.

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when

needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3. Existing System

A. Multi-user Searchable Encryption

Counting PEKS and additionally SSE plans, on searchable encryption there is a rich writing. The watchword seek under the multi-tenure setting is a more basic situation in the connection of distributed storage as opposed to those current work. In such a situation, to impart a record to a gathering of approved clients the information proprietor might want, and over the "multi-client searchable encryption" (MUSE) situation, every client can give a trapdoor who has the entrance right to perform the watchword look.

To such a MUSE situation some late work center, in spite of the fact that to accomplish the objective with access control they all receive single-key consolidated. With all clients by sharing the record's searchable encryption key who can get to it, MUSE plans are developed, and to accomplish coarse-grained access control telecast encryption is utilized. To accomplish fine-grained access control mindful catchphrase seek characteristic based encryption (ABE) is connected. Subsequently, in MUSE, how to control which clients can get to which documents is primary issue, though There is not considered how to minimize trapdoors and shared the quantity of keys. The answer for the last can give by key total searchable encryption, and it can be make more pragmatic and effective for MUSE.

B. Multi-Key Searchable Encryption

On account of use which has a multi-client, to look over considering that there is relative the quantity of trapdoors to the quantity of archives, The idea of multi-key searchable encryption (MKSE) was presented by Popa.

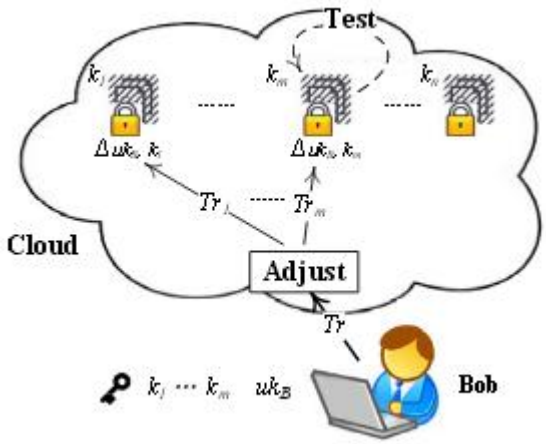

Figure 1: Multi-Key Searchable Encryption

In 2013 he advances the primary plausible plan. For giving a solitary catchphrase trapdoor to the server by a client permits by MKSE, yet in records encoded with various keys, to hunt down that trapdoor's watchword still permits the server. To the objective of KASE this may sound fundamentally the same, however these are indeed two unique ideas totally. From the same client in the multiuser applications over a gathering of shared records, there spotlight on the issue of catchphrase inquiry by this methodology of MKSE which rouses us, and to perform watchword seek over a gathering of documents with one and only trapdoor a general approach additionally gives by the change process in MKSE. In any case, the MKSE's change handle needs. From both client's vital and SE key of the archive a delta created, so to the outline of a solid KASE plan it doesn't specifically apply.

4. Proposed System

From both the encryption of multi-key searchable plan and also the key-total information sharing plan, there draws its bits of knowledge the configuration of our KASE plan. In particular, rather than numerous autonomous keys, all together to create a total searchable encryption key, we adjust the thought displayed in. With a specific file of record each searchable encryption key is related, and into the result of open keys installing the proprietor's expert mystery key which is connected with the archives, the total key is made. Over various archives, with a specific end goal to actualize catchphrase look utilizing the total trapdoor. To deliver a balanced trapdoor, the cloud server can utilize this procedure for each record.

A. The KASE Framework

This Framework is made out of seven algorithms by The KASE frameworks. In particular, to set up the plan, the general population parameters of the framework would create by the cloud server through the Setup algorithm, and by various information proprietors these open parameters can be reused to share their documents. An open/expert mystery key pair ought to create by him/her for every information proprietor, through the Keygen algorithm. With the interesting searchable encryption key, by means of the Encrypt algorithm the watchwords of every record can be scrambled. At that point, to create a total searchable

encryption key, by means of the Extract algorithm the expert mystery key can be utilized by information proprietor for a gathering of chose documents. To approved clients who need to get to those records the total key can be circulated safely. After that, as appeared in Fig.2, through the Trapdoor algorithm a watchword trapdoor can create utilizing this total key by an approved client, and for the cloud there present the trapdoor. The cloud server will pursue getting the trapdoor over the predetermined arrangement of archives for performing the catchphrase look.

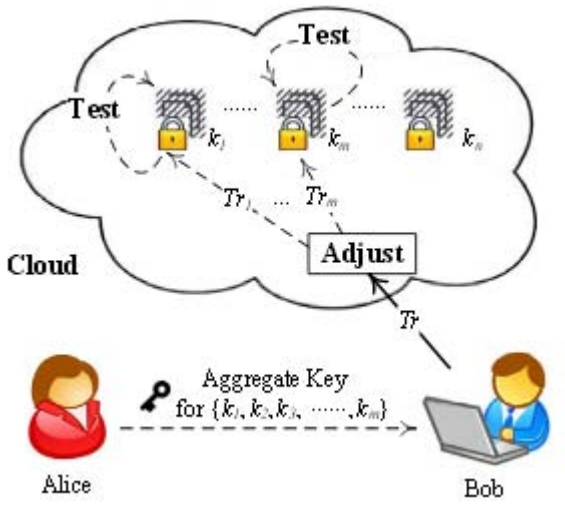

Figure 2: Framework of key-aggregate searchable encryption.

For every record the privilege trapdoor produce by the Adjust algorithm, and after that for testing whether the archive contains the watchword, run the Test algorithm.

5. Conclusion

In proposed plan, when imparting bunches of documents to the client, there just needs to disseminate a solitary to a client key for the proprietor and when client questions over all archives shared by the same proprietor, he just needs to present a solitary trapdoor. Be that as it may, over records shared by numerous proprietors if a client needs to inquiry, for the cloud he should produce various trapdoors. The future work is that, under multi-proprietors setting, how to diminish the quantity of trapdoors. Besides, a great deal of consideration have pulled in by combined mists these days, yet for this situation specifically our KASE can't be connected. To give the answer for KASE is additionally a future work on account of united mists.

6. Acknowledgment

Author would like to take this opportunity to express our profound gratitude and deep regard to my (Project Guide name), for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of huge help throughout my project work. His perceptive criticism kept me working to prepare this project in a much better way. Working under him was an extremely knowledgeable experience for me.

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.