Group Data Searching And Sharing Using Key Aggregate Cryptosystem

[1] Wakchaure Sonali Pandharinath.
ME Student, Dept. of Computer Engineering.AVCOE, Sangamner, Pune University,Maharastra,India
[2] Sonkar Shrinivas K.
Assistant Professor, Dept. of Computer Engineering.AVCOE, Sangamner, Pune University,Maharastra,India

ABSTRACT

A Searchable encryption can be defined as Store data externally in encrypted format. It can be easily search by user and most important that to allow others to search data without having access to plaintext. Data leaks in the cloud are the major security problem. In searchable encryption data owner encrypt some keywords and then upload them in the cloud with the encrypted data. In previous systems, it is noticed that sharing encrypted data with different users may contain the different encryption keys that are used for different files. Therefore, number of keys may imply problem as that are needed to be distributed to users for encryption as well as decryption of the cloud data. Also to perform a keyword search over many files large number of trapdoors must be generated by users and submitted to the cloud. Hence, existing systems are less secure communication, storage, and computational complexity which may cause system inefficiency. To overcome these problems we are studying about the KASE i.e. Key-Aggregate Searchable Encryption.

Keywords: Encryption, searchable data, trapdoors, Key-Aggregate Searchable Encryption (KASE) .

I. INTRODUCTION

Cloud storage can be defined as storing data online in the cloud. Cloud storage provides the benefits of convenient and on-demand greater accessibility, reliability, strong protection for data backup and archival. Key-aggregate searchable encryption (KASE) to address the problem of privacy preserving in public cloud storage in which data owner required to distribute huge number of keys to other users to enable the access to their data. This scheme can be implies on any cloud system which supports the functionality of searchable group data sharing [1] . User can generate multiple trapdoors if user wants to query over documents shared by multiple owners. It also studies about the broadcast encryption (BE) scheme[2]. It encrypts the message of user who is listening on a broadcast channel and any user from same subset can decrypt the message using private key.

. In searchable group data sharing scheme, data owner can share group of files with the selected group of users. For that data owner needs to distribute single key to the user for sharing the group of files and instead of group of trapdoors user only needs to submit single aggregate trapdoor to perform keyword searching over the group of any number of files. KASE system can be satisfying the basic requirements of the key-aggregate cryptosystem [5]. In cloud system overall cost of data storage is less as it does not require maintaining and managing expensive hardware. With enjoying these benefits user also worried about data leaks in the cloud. Therefore, data leakage would be a major security violation because of an accidental, or due to a malicious hacker attack. To address data leak problem in cloud cryptographic cloud storage [7] system is referred. In which data owner firstly encrypt all the data before storing on cloud in such way that only user whom having decryption keys can be decrypt or fetch the data.

In searchable encryption (SE) scheme, owner of data encrypt some keywords and keep them with encrypted data in cloud. Furthermore, to retrieve that data keyword matching is done by sending the keyword trapdoor to the cloud to search particular encrypted data. This technique achieves basic security to the data in cloud. Practically, it is not efficient as there are millions of users and billions of files are contained by the large application.

To the best of our knowledge, in large system different users requires different encryption keys for different files. However, in such system resulting number of keys required to encrypt as well as decrypt the files. Such large number of keys cannot securely manage and stored in cloud system. Therefore such system implies as inefficient and impractical for communication, storage and computational complexities.

II. LITERATURE SURVEY

Baojiang Cui, Zheli Liu and Lingyu Wang [1], proposed key-aggregate searchable encryption (KASE) to address the problem of privacy preserving in public cloud storage in which data owner required to distribute huge number of keys to other users to enable the access to their data. This scheme can be implies on any cloud system which supports the functionality of searchable group data sharing. In searchable group data sharing scheme, data owner can share group of files with the selected group of users. For that data owner needs to distribute single key to the user for sharing the group

of files. And instead of group of trapdoors user only needs to submit single aggregate trapdoor to perform keyword searching over the group of any number of files.

S. Yu, C. Wang, K. Ren, and W. Lou [2],This system provides the solution for the problem of fine-grainedness, scalability, and data confidentiality of access control in cloud storage. To address these problems access policies are created based on data attributes. This paper proposed attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption techniques to achieve their goal.

R. Lu, X. Lin, X. Liang, and X. Shen [3], in this secure provenance *SP* scheme based on the bilinear pairings in cloud computing model. This scheme is used provide security and trusted evidences for data forensics in cloud computing. Provable security techniques are used to check the validity of the security. Trusted evidences for data forensics are provided by the secure provenance *SP* scheme.

X. Song, D.Wagner, A. Perrig [4], paper proposed the proofs of security with the help proposed cryptographic scheme. It supports searching functionality without losing the confidentiality of the data. This technique is secure for encryption as it provides control searching over the data. This system handles the hidden searches as well as query isolation over the cloud data. This system also supports random-access decryption in which the length of each word also needs to be stored with the word. For Searching process encrypted Index is used when data size is large.

R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky [5],This paper stronger security technique that is Searchable Symmetric Encryption (SSE). In this technique user can store data on remote server and can access it privately. To extend the searching ability authors were also proposed multi-user SSE. In this system user least the data from large dataset, Single-database PIR used to retrieve data from a server containing unencrypted data. For the secure modifications new documents can be added to the previous document collection.

S. Kamara, C. Papamanthou, T. Roeder [6], this paper proposed stronger security technique that is Searchable Symmetric Encryption (SSE). In this technique user can store data on remote server and can access it privately. To extend the searching ability authors were also proposed multi-user SSE. SSE is adaptive security than chosen-keyword attacks (CKA2). This system uses inverted index approach. SSE has capability to describe leakage of a database which contains two tables over word and file identifiers.

D. Boneh, C. G, R. Ostrovsky, G. Persiano[7],In this author refers mechanism called *Public Key Encryption with keyword Search*. In this user sends the key to server to identify that all messages are containing some specific keyword without learning extra information. This system is based on IBE construction.This approach is for users who own their data and they wish to upload that data to a third-party database in which they may not trust. The system is based on a variant of the Computational Diffie-Hellman problem.

C. Dong, G. Russello, N. Dulay [8], in this system user has its own key which is used to encrypt and decrypt the data. Therefore it does not require any trusted server for accessing the data. This encryption system is based on proxy cryptography in which users share data via an un-trusted data storage server. In this server is hosted by a third party. Proxy cryptography is build upon the El Gamal encryption scheme. To securely encrypt keywords, keyword encryption scheme is also obtained by proxy encryption scheme. This scheme allows user revocation straightforwardly.

F. Zhao, T. Nishide, K. Sakurai [9], data sharing scheme based on attribute-based cryptosystems is proposed by authors. It is fine-grained as well as flexible for cloud storage. This scheme decreases the data leakage from keyword search process also user revocation and key updating can be easily achieved. In this system server recalculate the hash values then match it with the keyword to retrieve the encrypted data.

J. W. Li, J. Li, X. F. Chen, et al. [10], this author gives the information about fuzzy keyword search method in a multi-user system. It maintains the keyword privacy over the encrypted data. Also gram-based technique is utilized to construct the storage-efficient fuzzy keyword sets. Furthermore, to improve the search efficiency a symbol-based trie-traverse searching scheme is proposed. This system allows outsourcing cryptographic access control mechanism and also relives the cost at user side. It supports the Interface between users and public cloud.

Z. Liu, Z. Wang, X. Cheng, et al [11],To construct a multi-user searchable encryption model in hybrid cloud new concept of coarse-grained access control is proposed in this paper. In this development, two schemes are introduced as:

1. Broadcast Encryption (BE) and
2. Single-user searchable encryption scheme.

C. Wang, Q. Wang, K. Ren, and W. Lou [12],In this paper, privacy-preserving public auditing system is introduced for providing security to the data stored in cloud. This paper also utilizes homomorphic linear authenticator and random masking for efficient auditing process. This system supports multiple auditing tasks with efficient handling. To extend

our main result into a multi-user setting bilinear aggregate signature technique is proposed in this paper. TPA brings in new vulnerabilities towards user data privacy.

D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al.[13],In this paper, efficient broadcast encryption scheme is proposed. In this scheme size of secret key and ciphertext is constant. Selective CCA secure is proved by assuming BDHE and universal one-way hash function. This system also maintains the two parallel sets of system parameters. For selective CPA identity-based broadcast encryption is proposed in this paper. Session key is produced by formalizing s broadcast encapsulation. GBDHE and knowledge of exponent assumptions are considered for adaptive CCA security.

D. Boneh, B. Lynn, H. Shacham [14],To provide a level of security similar to 320-bit DSA signatures, authors proposed a signature scheme whose length is approximately 160 bits. This signature scheme is based on Weil pairing. To construct a DDH oracle which denote the subgroup generated by two different sets Weil pairing is used.
M. Li, W. Lou, K. Ren[15], In this paper two important security issues are discussed:

1. Secure and dependable distributed data storage
2. fine-grained distributed data access control

This paper inspires novel and practical designs of secure, dependable, and privacy enhanced WBANs.

D. Boneh, C. Gentry and B. Waters [16],In this paper public key broadcast encryption systems for stateless receivers is introduced. In this for any subset receiver ciphertexts and private keys are of constant size. This generalized scheme gives a tradeoff between public key size and ciphertext size.

R. A. Popa, N. Zeldovich [17], In this paper, multi-key search is introduced in cryptographic scheme to overcome the problem arise with single search token. This system provides the guarantee of security under variants of the Bilinear Decisional Diffie-Hellman and External Diffie-Hellman assumptions, as well as in the random oracle model.

III. PROPOSED SYSTEM

This system will be secure as encryption technique is involved. Also it is efficient as aggregate key for multiple documents are shared with group of user. Which is not case in existing system Decryption key should be sent via a secure channel and kept secret e.g. email hence data will be secure. This system will be efficient public-key encryption scheme which supports flexible delegation for searching also. Searching over encrypted data is performed efficiently since important public information is retrieved and mapped with the document in encryption format.
searching is performed based on the index. Similarity search is performed on the number of document. It reduces the searching time and then retrieve the document. Various phases are use to design system like setup, key generation, encrypt, search, decrypt, share key phase. In this scheme user only need to share single key over the number of document and decrypt document using that single key.

IV. CONCLUSION

In this paper, we reviewed the existing systems papers of sharing the data securely in the cloud. The existing systems based on key encryption may suffer from certain problems such as; these systems are impractical and inefficient as they may require many keys over the cloud data for encryption as well as decryption. Therefore in this paper we are analyzing these problem and aims to overcome them by proposing a novel system called as KASE. In this system, we define general framework for KASE system. Then we describe functional and non-functional requirements of KASE scheme. After describing the KASE scheme we establish its security by detailed analysis.

REFERENCES

1. Baojiang Cui, Zheli Liu_ and Lingyu Wang Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

2. 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.

3. 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

4. X. Song, D.Wagner, A. Perrig. “Practical techniques for searches on encrypted data”, IEEE Symposium on Security and Privacy,IEEE Press, pp. 44C55, 2000.

5. 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.

6. 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.

7. D. Boneh, C. G, R. Ostrovsky, G. Persiano. “Public Key Encryption with Keyword Search”, EUROCRYPT 2004, pp. 506C522,2004.

8. C. Dong, G. Russello, N. Dulay. “Shared and searchable encrypted data for untrusted servers”, Journal of Computer Security, pp. 367-397, 2011.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. D. Boneh, B. Lynn, H. Shacham. “Short signatures from the Weil pairing”, Advances in Cryptology ASIACRYPT 2001, pp. 514-532, 2001.

15. M. Li, W. Lou, K. Ren. “Data security and privacy in wireless body area networks”, Wireless Communications, IEEE, 17(1): 51-58, 2010.

16. D. Boneh, C. Gentry and B. Waters. “Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys”, CRYPTO’05, pp. 258C275, 2005.

17. R. A. Popa ,N. Zeldovich. “Multi-key searchable encryption”. Cryptology ePrint Archive, Report 2013/508, 2013.