© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Cloud Group Data Sharing using Key-Aggregate Searchable Encryption (KASE) Scheme

Shweta Lambhate[*1], Sachin Patil[#2]

[*1]Computer Department, Pune University, Ahmednagar, Maharashtra, India
[#2]Computer Department, Pune University, Pune, Maharashtra, India

ABSTRACT

Cloud computing is latest technology widely serving client oriented applications. It has the capability of sharing selective encrypted data via public cloud storage with multiple users which may ease security over accidental data leaks in the cloud. Efficient key management is important in encryption schemes. For sharing multiple documents with different groups in cloud, separate encryption keys are needed. Security is required by owner to distribute large number of keys for encryption and searching, and by users to store received keys. Users have to submit equal number of trapdoors to the cloud for search operation. In such case features of security, storage and complexity are required at its best performance.

Key-Aggregate Searchable Encryption (KASE) scheme addresses to the problem of storage management and security in group data sharing on cloud. Through this scheme only single key is distributed by owner to user for sharing multiple documents, and user also required to submit single trapdoor to receive shared documents. KASE scheme is efficient and secure as resulted by security analysis tests.
Keywords: Searchable Encryption, Data Sharing, Cloud Storage, Data Privacy

I. INTRODUCTION

Cloud computing is recent trend in IT infrastructure which enables organizations to consume resources of computing as a utility and organise data storage model which keeps data accessible and available for shared pool of configurable devices on-demand with coherence environment, low cost and least management efforts. However large data sharing leads to advertent data confidentiality problems. Many security schemes are generated against potential data leaks from which encryption is common approach. In cryptographic cloud storage, data owner before uploading files encrypts them such that only the person with decryption key can retrieve shared documents. This approach becomes impractical for key management and secure storage to implement with large scale cloud applications. Also searching and retrieving selective data from large number of encrypted files is challenging for user. Searchable Encryption (SE) [3] is solution for this problem in which owner encrypts keywords and uploads it along with encrypted data so that user can retrieve shared data by providing keyword trapdoor to cloud.

Based on this SE concept many schemes are introduced later. SSE scheme [3]-[6] and PEKS scheme [7]-[13] considered SE construction for sharing data in single owner and user environment and performed secure search on remote server by submitting search query on keyword provided by owner. Further system for sharing of data with group of multiple authorised users such that any user from the group with access rights can provide trapdoor on cloud to search for keyword on shared data is constructed. This scenario of Multi-user searchable Encryption scheme [4],[11]-[14] used single key with access control.

To reduce complexity of increase in number of trapdoors proportional to number of files shared, Popa [16] introduced Multi-key SE scheme. So that single trapdoor

is provided by user and server gets capability to search for that trapdoor's keyword in shared documents even their encryption keys are different. Further to reduce number of encryption keys Chu et al. [2] introduced concept of Key aggregate Encryption which flexibility to decrypt any number of ciphertext with constant-size decryption key. Our model further enhances this concept by providing keyword search over encrypted data to achieve goal of privacy-preserving data sharing and efficient cloud storage.The below subsections will give information about general concepts in cloud computing used in rest of the paper. Different encryption schemes and their operations are described.

A. Broadcast Encryption (BE) scheme:

In this scheme, data owner as broadcaster encrypts content and sends it over broadcast channel to subset S of users. Users from S listening for shared data decrypts received documents using private key. Broadcasting is such that only qualified users can decrypt contents.

B. Searchable Encryption(SE) scheme:

Data owner encrypts data and provide search queries on cloud. Users submit proper search query to get access to selective documents and decrypt them through private key.

Two importance concepts in SE are:

1) Multi-user Searchable Encryption (MUSE): It works under multi-tenancy operations where data owner shares documents with group of users and users can receive them by submitting trapdoor for keyword search on shared contents. It advances the single user SSC and PEKS schemes.

2) Multi-key Searchable Encryption (MKSE): A single trapdoor for multiple different keys is provided which reduces the number of trapdoors used for each document separately.

The rest of the paper is arranged as follows: we describe the overview of related work in section 2 which include prior systems, algorithms, pros and limitations of them. Section 3 gives conclusion along with future research.

II. METHODS AND MATERIAL

Related Work

A. *D. Boneh, G. Di Crescenzo, R. Ostrovskyy and G. Persianoz, "Public Key Encryption with keyword Search", 2004:* In this paper the problem in public cloud system to search for encrypted data through encryption key is examined. Keyword as search query for email gateway is firstly introduced. Without learning contents of shared data gateway can search for specific keyword and verify qualified document to route document accordingly. This PEKS scheme can also enable server to identify all publicly encrypted documents of owner by other users containing the same keyword given by owner without decryption of data. Gateway test is performed to match encrypted keywords of sender and word of receivers choice, no more information is learned by the gateway. PEKS system implies Identity Based Encryption (IDE) scheme where owner encrypts data such that user having required attributes can only decrypt the shared document. This system considered only single owner and user condition for performing keyword search over multiple shared documents.

B. *R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions", 2006:* The problem of SSC scheme used for single user i.e. owner is considered in this paper. In prior system only the owner of data could submit search queries and perform search over encrypted data outsourced to other party. The construction in this paper extended the work of searchable symmetric encryption to be used for multi-user environment, where searching can be performed by arbitrary group of parties instead of only owner. Contrary to the prior system which guaranteed security for clients performing all searches at once, this scheme ensured security constraints for any number of practical searches by different users. Two SSE constructions are introduced as 1. Non-Adaptive Secure Construction (SSE-1) 2. An Adaptively Secure Construction (SSE-2). Multiple secure searching is achieved through SSC-2 where search queries are considered as function of previously obtained search results and trapdoors. In both constructions the work performed

by server is constant with respect to size of data over each returned document.

C. *F. Zhao, T. Nishide, and K. Sakurai, "Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control", 2012:* Searching all keyword index in cloud storage to match with given keyword and decrypt them is not practically feasible. Narrowing the scope of search results to user's decryptable file's group using Attribute Based Encryption (ABE) and CP-ABE to minimise information leakage and reduce searching complexity in multi-user cryptographic cloud storage environment is introduced in this paper. This system only search for related documents which user can decrypt and so is more efficient. The flexibility of specifying the access rights for individual users in case of user revocation is provided known as fine grained access control. The Ciphertext-Policy Attribute Based Encryption (CP-ABE) and Attribute Based Signature (ABS) access structure computation are used for providing differential access rights.

D. *Z. Liu, Z. Wang, X. Cheng, C. Jia and Ke Yuan, "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", 2013:* The complexity of maintaining massive authentication information for dynamic insertion and removal of users in fine grained access control scheme is resolved in this paper. Two schemes: 1. Identity Based Broadcast encryption (IBBE) for simplified access control by using single random value for addition or revocation of users and management of keys and 2. SUSE scheme for secure two phase operation without private cloud or trusted centre by using Pseudo Random Permutation (PRP) function, gives practical implementation of MUSE system. Two phase operation is performed for encryption of keywords and generating trapdoors. BE scheme directly imply security for re-encrypted trapdoor and symmetric key, and SUSE scheme ensures security of keyword ciphertext and encrypted files. This system is efficient against 1. External adversaries as trusted centre only respond to identified users by Coarser-Grained Access Control and 2. Internal adversaries as PRFs of SSC scheme is provably secure.

E. *R. A. Popa and N. Zeldovich, "Multi-Key Searchable Encryption", 2013:* The system provided flexibility to user for searching over multiple documents which he/she can access say n, with different encryption keys. One search token is provided by user to server instead of n tokens. The user have to provide some public information and token for word to search and the system server then by using this information calculates token for different keys (adjust function) and get all documents with matching word even their encryption keys are different. Only single user and multi-key condition is considered in this paper. This scheme ensures data confidentiality in client-server architecture against attack on server as the encrypted data is only stored on server and encryption and decryption functions are performed on client machine. Data security is guaranteed as no third party key generation is included instead it is provided by client itself.

C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", 2014: To share multiple documents with same user, the data owner needed to distribute equal number of keys to the user. The complexity and security aspects become more subtle and impractical in case of large number of shared documents. In this scheme only single aggregate key to decrypt all documents is provided by owner i.e. compression of secret key. A public-key cryptosystem is introduced which produce constant-size cipher-texts leading to limited secure storage application. The user encrypts data under public key and ciphertext class which is identifier of ciphertext. But predefined bound of ciphertext classes number can limit the encryption scope. This scheme is more efficient than hierarchical relationship i.e. all key-holders sharing similar set of privileges just for reducing space. The delegation of decryption rights to users is main advancement of this scheme although keyword search operation is not provided which is main requirement for privacy preserving data sharing on public cloud storage.

III. CONCLUSION

In this paper we addressed the problem of privacy preserving data sharing system in cloud storage and studied different searchable encryption technics with multi-user and multi-key schemes with aggregation of multiple attributes to reduce storage complexity and

improve efficiency of search over shared data. Secondly, we studied model for Key-Aggregate Searchable Encryption scheme, a practical system for efficient management of encryption keys for sharing large number of documents with users.

The KASE scheme considers single owner multi-user condition, but querying search over documents shared by multiple owners will require multiple trapdoors to be submitted by users. Multi-owner document sharing through single trapdoor can be future work.

IV. ACKNOWLEDGMENT

We would like to thank all authors of research papers referred in this paper for their work. It was very helpful and knowledge gaining for further future research to be done in this field.

V. REFERENCES

[1] B. Cui, Z. Liu and L. Wang, "*Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage*", IEEE TRANSACTIONS ON COMPUTERS, Volume: PP, Issue: 99, Year: 2015

[2] 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.

[3] X. Song, D.Wagner, A. Perrig. "*Practical techniques for searches on encrypted data*", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[4] 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.

[5] P. Van,S. Sedghi, JM. Doumen. "*Computationally efficient searchable symmetric encryption*", Secure Data Management, pp. 87-100, 2010.

[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] 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.

[9] J. Li, Q. Wang, C. Wang. "*Fuzzy keyword search over encrypted data in cloud computing*", Proc. IEEE INFOCOM, pp. 1-5, 2010.

[10] C. Bosch, R. Brinkma, P. Hartel. "*Conjunctive wildcard search over encrypted data*", Secure Data Management. LNCS, pp. 114-127, 2011

[11] C. Dong, G. Russello, N. Dulay. "*Shared and searchable encrypted data for untrusted servers*", Journal of Computer Security, pp. 367-397, 2011.

[12] 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.

[13] 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.

[14] 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.

[15] D. Boneh, C. Gentry and B. Waters. *"Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys"*, CRYPTO'05, pp. 258C275, 2005.

[16] R. A. Popa ,N. Zeldovich. *"Multi-key searchable encryption"*. Cryptology ePrint Archive, Report 2013/508, 2013.

[17] 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.

[18] 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.