IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Survey on Leakage-Resilient KASE for Group Data Sharing with Auxiliary Input via Cloud Storage

Payal Bhagat[1], Amar Buchade[2]

M.E. Student, Computer Engineering, Pune Institute of Computer Technology, Pune, India[1]

Assistant Professor, Computer Engineering, Pune Institute of Computer Technology, Pune, India[2]

Abstract: As cloud computing becomes popular, more and more sensitive information are being centralized into the cloud nowadays. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task because all the data which we outsource are in encrypted format. In this paper, we have discussed a few approaches for sharing data on cloud with minimal usage of key. We also discuss few data searching technique over encrypted data. While enjoying the advantage and convenience of cloud storage for data sharing, users are becoming more worried about careless leak of data in the cloud. To address this problem we studied various leakage models.

Keywords: Auxiliary Input, Key Aggregate, Leakage Resilient, Searchable.

I. INTRODUCTION

Storage on cloud is a solution for accessing large amounts of data and sharing with various users by means of internet. Nowadays, a number of users are mainly sharing a large number of various kinds of documents, which are considered to be under various categories like photos, videos and documents via various social networking based applications on daily basis. There are various benefits of using cloud storage like lesser cost, greater agility, availability and better utilization of resource has caused attraction of plenty more number of business users toward using the cloud storage.
While enjoying the advantage and convenience of cloud storage for data sharing, users are becoming more worried about careless leak of data in the cloud. To overcome the users problem of possible leak of data in cloud storage, the data owner can encrypt the data before sending them to the cloud is a popular approach, so that later the data may be decrypted and retrieved by users who have the decryption keys. But still, the data encryption makes it difficult for users to search given keywords and then retrieve only selected data matching keywords. We also studied various searchable encryption technique which provide searching over encrypted data.

By combining a cryptographic cloud storage with searchable encryption technique can achieve the basic requirements security. However, different encryption keys must be used for different files when sharing selective encrypted data with different users. This suggest that number of keys required to be distributed to users will be equivalent to the number of files. Such a large number of keys must be securely stored and managed by the users in their devices and only to be distributed to users via secure channels. To perform a keyword search over many files a large number of trapdoor must be generated by users and submitted to the cloud. To address this challenge we studied various approaches which can improve the cloud storage functionality by securely storing the encrypted data and providing searchable encryption to facilitate the need searching over encrypted data.

Majority of the devices on cloud are mobile devices, and the stored aggregate key in it can be easily leaked. Thus, how to design a system that will be resilient to leakage is still a challenging problem. While conveniently using cloud storage for data sharing, users are becoming more worried about data leaks in the cloud. To address this problem we studied various leakage models.
Various techniques have been proposed for data sharing via cloud storage, their efficiency is to be increased by means of development of new concepts and schemes. This paper is organized as follows: Section II illustrates some of the methodologies used for data sharing and searching through cloud storage. Section III concludes the review of our work.

II. REVIEW OF LITERATURE

We studied the following related systems to discover their advantages, drawbacks and limitations. These systems are discussed below.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A. Key Aggregate Encryption for Data Sharing

Data sharing systems have received much more attention lately [3], [4], [5], [6] which is based on cloud storage. To be specific, Chu et al [6] considered many ways to reduce the data encryption keys distribution numbers. The owner of data needs to distribute all keys which are used for encryption, to share several documents with the same user in a traditional approach which is almost infeasible. Taking this challenge with aim to generate an aggregate key for the user to decrypt all the documents shared with the user, Chu et al [6] proposed a data sharing system using key-aggregate cryptosystem (KAC). This is a new cryptographic system, which allowed giving flexible decryption rights such that aggregate secret key can be used to decrypt any cipher-texts subset. The constant-size aggregate key is generated by the master secret key of data owner. In this system, different classes are created to classify the cipher-texts, and these different classes are used by data owner to generate aggregate secret keys by using master secret key. The power of many keys is aggregated as one key is compacted for one cipher-text class. Hence to share many documents, only one aggregate key is needed to be sent by the data owner to data requester in cloud.

B. Key Aggregate Searchable Encryption

Chu el at [6] proposed a system which allows efficiently assigning the rights of decryption to users who requested data, however searching over the encrypted data is not support. In the cloud based system, achieving privacy-preserving data sharing is the main objective, where keyword search is an essential requirement. By merging a cloud cryptographic storage with searchable encryption can accomplish the primary requirements of a cloud storage security. Basically the need is to selectively and efficiently share encrypted data with individual as well as multiple distinct users. This requirement generally demands different keys to be used for encryption of different data. But still, this indicate that the number of keys required will be proportional to the number of files that is needed to be shared with users to search over the encrypted files as well as to decrypt the files. While distributing such a huge number of keys care must be taken that secure channels must be used for keys distribution amongst users, as well as the keys must be stored safely and properly managed on their devices by users. To search over encrypted data keyword search must be performed over many files for which trapdoors in huge number of must be generated by users and sent to the cloud. The said need for secure storage, communication and computational complexity makes such a system impractical and inefficient. Baojiang Cui, Zheli Liu, and Lingyu Wang el at [1] proposed concept of key-aggregate searchable encryption to tackle these challenges. The proposed KASE system can be applied to any storage on cloud that have the functionality of group data sharing and searching, which means that any selected group of files may selectively shared with a group of selected users by any user, while allowing to perform keyword search over the data.

C. Multi-User Searchable Encryption (MUSE)

Multi-User Searchable Encryption (MUSE) technique was focused in some recent work [8], [9], [10], [11], [14], while to reach the objective these all adopted single key integrated with access control. In [7], [14], multi-user searchable encryption system are constructed to achieve coarse-grained access control by using broadcast encryption and documents were shared by sending searchable encryption key to all users who can access it. Attribute Based Encryption (ABE) is applied in [8], [9], [10], [11], [12], [13] to achieve searching keyword using fine-grained access control. However now in multi-user searchable encryption, control over which document can be accessed by which user is the main problem. As well as it does not consider how the number of shared keys and trapdoors can be reduced. Key aggregate searchable encryption (KASE) system can make MUSE more efficient and practical and also provide the answer for the keyword search and access control.

D. Multi-Key Searchable Encryption (MKSE)

When there is a scenario of multi-user application, we consider that when searching keyword over documents the number of trapdoor will be same as the number of documents, Popa and Zeldovich el at [15] firstly proposed the multi-key searchable encryption (MKSE) system concept and in 2013 this system was put forward. Multi-key searchable encryption allows a user to search over documents encrypted with different keys by providing a trapdoor of single keyword to the server. This requirement looks very similar to the objective of KASE, but these two techniques are completely different from each other. The objective of KASE system is distributing the aggregate key to give the keyword search right to any user in a group data sharing system, however the aim of MKSE is to ensure that using single trapdoor keyword search can be performed on cloud server over different documents belonging to a user.

E. Public-Key Encryption with Keyword Search

The difficulty in public cloud system is searching over encrypted data through encryption key. Firstly introducing search query where keyword were used for email gateway. Without knowing about the contents of data shared specific keyword can be searched by gateway and verifying satisfying document to rank documents accordingly. Public Key Encryption with Keyword Search system recognize all public key encrypted documents containing the same keyword given by data owner without decryption of data. Test over gateway is executed 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.

F. Searchable Symmetric Encryption

The problem of Searchable Symmetric Encryption (SSE) system used for single user i.e. owner is considered in this work. In previous system search queries can only be submitted by the owner of data and perform search over encrypted data outsourced to other party. The construction in this work [7] enhanced the work of searchable symmetric encryption to be used for multi-user environment, where instead of only owner searching can be performed by arbitrary group of parties. Opposite to the previous system which guaranteed security for clients performing all searches at once, this system 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.

G. Leakage Security Model

Until now, some classic leakage models have been proposed, and there are primarily three leakage models. The first model is the bounded retrieval model [18], [19], [20], in this model the bit-length of the key must be significantly higher than the total number of bits leaked over the lifetime of system, and before the whole secret is leaked we hope that the attack is detected and stopped. The second model is the continual leakage model [21], [22], [16], where the secret key should be refreshed continually where there is no leakage during the update process and it assumes that leakage is bounded in term of a fraction of the secret key size between consecutive updates. The third model which is developed from the relative leakage model [17], is the auxiliary input model [23], [24], [25], [26], which permits any non invertible function that no probabilistic polynomial time attacker can compute the actual pre-image with probability which is non-negligible. Zhiwei Wang and Lingyu Zhou el at [2] proposed a leakage resilient KAC with auxiliary input based on Chu et al.'s basic construction [6]. Where, the attacker still cannot recover any information of the master secret key, no matter how many bits are leaked from the aggregate key.

H. Leakage-Resilient KAC with Auxiliary Input

Chu et al. [6] proposed a key aggregate cryptosystem (KAC) to solve the problem of selectively sharing data by generating a single aggregate key. This is a new cryptographic system, which allowed giving flexible decryption rights such that aggregate secret key can be used to decrypt any cipher-texts subset. The constant-size aggregate key is generated by the master secret key of data owner. In this system, different classes are created to classify the cipher-texts, and these different classes are used by data owner to generate aggregate secret keys by using master secret key. The power of many keys is aggregated as one key is compacted for one cipher-text class. Hence to share many documents, only one aggregate key is needed to be sent by the data owner to data requester in cloud. But in real world, attackers can learn partial information about secret key by making many side channel attacks and observing cryptographic execution physical properties. Zhiwei Wang and Lingyu Zhou el at [2] proposed a leakage resilient key aggregate cryptosystem with auxiliary input which is based on Chu et al.'s construction [6].

III.CONCLUSION

Sharing and searching data need multiple keys to be shared in cloud which makes the system inefficient, to overcome this challenge an effective method of key-aggregate searchable encryption is provided. However in practical world, side channel attacks allow the attackers to learn partial information about secret key. So providing an leakage-resilient key-aggregate searchable encryption will make the cloud storage more secure and reliable.

ACKNOWLEDGMENT

I sincerely convey my gratitude to our Dissertation Coordinator Dr. A. S. Ghotkar and Head of Computer Engineering Department, Dr. R. B. Ingle for their support and help.

REFERENCES

[1] Baojiang Cui, Zheli Liu, and Lingyu Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transaction on Computer, vol. 65, no 8, Aug 2016.

[2] Zhiwei Wang and Lingyu Zhou, "Leakage-Resilient Key-Aggregate Cryptosystem with Auxiliary Input", 25th International Conference on Computer Communication and Networks (ICCCN), 2016.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Conf. Comput. Commun., 2010, pp. 534–542.
[4] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
[5] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
[6] C. K. Chu, S. Chow, W. G. Tzeng, J. Y. Zhou, and R. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 468–477, Feb. 2014.
[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.
[8] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," J. Comput. Security, vol. 19, pp. 367–397, 2011.
[9] F. Zhao, T. Nishide, and K. Sakurai, "Multi-user keyword search scheme for secure data sharing with fine-grained access control," in Proc. Int. Conf. Inf. Security Cryptol., 2012, pp. 406–418.
[10] J. W. Li, J. Li, X. F. Chen, C. F. Jia, and Z. L. Liu, "Efficient keyword search over encrypted data with fine-grained access control in hybrid cloud," in Proc. 6th Int. Conf. Netw. Syst.Security, 2012, pp. 490–502.
[11] J. Li and K. Kim, "Hidden attribute-based signatures without anonymity revocation," Inf. Sci., vol. 180, no. 9, pp. 1681–1689, 2010.
[12] X. F. Chen, J. Li, X. Y. Huang, J. W. Li, and Y. Xiang, "Secure outsourced attribute-based signatures," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 12, pp. 3285–3294, Dec. 2014.
[13] J. Li, X. F. Chen, M. Q. Li, J. W. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 6, pp. 1615–1625, Jun. 2014.
[14] Z. L. Liu, Z. Wang, X. C. Cheng, and , C. F. Jia, K. Yuan, "Multi- user searchable encryption with coarser-grained access control in hybrid cloud," in Proc. 4th Int. Conf. Emerging Intell. Data Web Technol., 2013, pp. 249–255.
[15] R. A. Popa and N. Zeldovich, "Multi-key searchable encryption," Cryptol. ePrint Archive, Rep. 2013/508, 2013.
[16] Mingwu Zhang, Wei Shi, Chunzhi Wang, Zhenhua Chen, Yi Mu: Leakage-Resilient Attribute-Based Encryption with Fast Decryption: Models, Analysis and Constructions. ISPEC 2013, volume 7863 of LNCS, pages 75-90, 2013
[17] Akavia A, Goldwasser S and Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks". TC- C'09, LNCS 5444, pp. 474-495, Berlin: Springer-Verlag, 2009.
[18] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Wallsh, and D. Wichs. Public-key encryption in the bounded-retrieval model. In EUROCRYPT, pages 113-134, 2010.
[19] J. Alwen, Y. Dodis, and D. Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. In CRYPTO, pages 36-54, 2009.
[20] D. Di Crescenzo, R. J. Lipton, and S. Wallsh. Perfectly secure password protocols in the bounded retrieval model. In TCC, pages 225-244, 2006.
[21] Y. Dodis, K. Haralambiev, A. Lopez-Alt, and D. Wichs. Cryptography against continuous memory attacks. In FOCS, pages 511-520, 2010.
[22] A. Lewko, Y. Rouselakis, B. Waters. Achieving Leakage Resilience through Dual System Encryption. TCC 2011, LNCS 6597, pages: 70-88, 2011.
[23] Dodis, Y., Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Public Key Encryption Schemes with Auxiliary Inputs. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 361C381. Springer, Heidelberg (2010).
[24] Tsz Hon Yuen, Sherman S. M. Chow, Ye Zhang, Siu-Ming Y-iu: Identity-Based Encryption Resilient to Continual Auxiliary Leakage. EUROCRYPT 2012: 117-134.
[25] Tsz Hon Yuen,Ye Zhang, Siu-ming Yiu, Joseph K. Liu: Identity-Based Encryption with Post-Challenge Auxiliary Inputs for Secure Cloud Applications and Sensor Networks, ESORICS 2014, Part I, LNCS 8712, pp. 130-147, 2014.
[26] Zhiwei Wang, Siu Ming Yiu: Attribute-Based Encryption Relient to Auxiliary Input, ProvSec 2015, LNCS 9451, pp. 371-390, 2015.