International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

Review on Key Based Encryption Scheme for Secure Data Sharing on Cloud

Miss. Swati V.Thakre[1], Prof. K.K.Chhajed[2], Prof.V.B.Bhagat[3]

[1]*Miss.Swati V.Thakre, P.R.Pote College Of Engineering, Maharashtra, India.*

[2] *Prof. K. K. Chhajed, Assistant Professor Department of Computer Science and Engineering, P.R.Pote College Of Engineering, Maharashtra, India.*

[3]*Prof. V. B. Bhagat, Assistant Professor Department of Computer Science and Engineering, P.R.Patil College Of Engineering, Maharashtra, India.*

Abstract: *Cloud technology is very constructive and useful in present new technological era. Cloud computing has given the users the accessibility to deploy number of files to the centralized cloud and share those with number of users. Cloud computing always comes with the hurdles of security concerns. Hence to achieve cloud data security, To enable secure and flexible data sharing in the cloud, efficient management of encryption keys are required .The data owner always needs to encrypt the files before uploading and it must decrypt before end users. This system needs secure storage of keys, but as files gets increased in number keys management becomes complex. By using Key based Encryption scheme user only need to submit aggregate key for file sharing in groups and searchable encryption and also submit aggregate trapdoor. This system provide number of benefits to multiuser and also reduce trapdoor.*

Key Word: Searchable Encryption, Cloud Computing, Aggregate Key, Data Privacy

1. INTRODUCTION

Cloud architecture can be used to allow data sharing capabilities and this can provide n number of benefits to the user. At present there is a push for IT organizations to increase their data sharing efforts. Cloud computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand [2]. There are some requirements in cloud system for sharing data securely. First, the data owner should be able to specify a set of users that are permitted to view data. Any member within the group should be able to gain access to the data anytime. The data owner should be able to add new users, revoke access rights against any member of the group over his or her shared data. Data owner or group admin, when he wants to share his data in the group he sends a key to the members of the group for data encryption [3]. And users get the access to the data with the help of any member of the group can then get the encrypted data from the cloud and decrypt the data using the key. But still this technique will not work properly if there is n number of users in the group.

While considering data privacy, we cannot rely on traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with users own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. So our aim is to develop an efficient data sharing scheme that enable complete control. This scheme also aims to enable group of users perform a keyword search over authorized encrypted files using single aggregate trapdoor generated from the single aggregate key [4].

2. AIM

To provide data storage and better data sharing in cloud, ensuring data security is important. Daily millions of user shares their data on cloud. A misbehaving cloud operator can pose serious threat of data stealing. Generally, key based encryption is used for ensuring data security.

3. LITERATURE SURVEY

Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

Author: S. Yu, C. Wang, K. Ren, and W. Lou,

In [1], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KP-ABE technique. In this paper the data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegate's tasks of data file re encryption and user secret key update to cloud servers. However, the single-owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Multi Key Searchable Encryption

Author: Raluca Ada Popa and Nickolai Zeldovich

Popa [2] firstly introduces the concept of multi-key searchable encryption (MKSE). In this scheme documents encrypted with different keys. Such scheme called as multi key search .This scheme hides the content of the document and the words one searches for, and the only information the server learns is whether some word being searched for matches a word in a document. It also provides data confidentiality in client-server applications against attacks on the server. The most challenging aspect when coming up with such a scheme is that there is no single trusted user.

Multi User Searchable Encryption

Author: R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky.

In this paper curtmola introduced rich literature on searchable encryption, including SSE schemes [3] and PEKS schemes [4]. 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 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.

Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud

AUTHORS: Xuefeng Liu, Yuqing Zhang

Xuefeng Liu et al. [5] proposed a secure multi-owner data sharing scheme, named Mona. It implies that any user in the group can securely share data with others by the untrusted cloud. The proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. This scheme provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

Author: Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou

Cheng-Kang Chu et al. [6] introduce a public-key encryption scheme called as key-aggregate cryptosystem (KAC) to securely, efficiently, and flexibly share data with others in cloud storage. In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. That means the cipher texts are further categorized into different classes. The key owner holds a master-secret key, which can be used to extract secret keys for different classes. The extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher text classes. In KAC the sizes of cipher text, public-key, master-secret key, and aggregate key are all of constant size.

3.1 Limitation of Existing System

Existing solutions are difficult to detect faults in Web applications deployed in a large scale dynamic cloud computing environment due to the following reasons:

1. Data leaks in the cloud.
2. The costs and complexities involved generally increase with the number of the decryption keys to be shared.
3. The encryption key and decryption key are different in public key encryption.
4. Large number of keys for both encryption and search.
5. Large number of trapdoor must be generated by the user and submitted to the cloud in order to perform a keyword search over many files.
6. The implied need for secure communication, storage, and complexity clearly renders the approach impractical.

4. PROPOSED SYSTEM

The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease. Any group of selected document shared with group of user's demands different encryption key to be used for different documents.so large number of key uses for both encryption and search .and also submit large number of trapdoor to the cloud in order to perform search data over shared document. This leads to key management and storage problem. This practical problem can be addressed by using Key Based Encryption scheme.

System play main three role user which is uploaded files and cloud service provider, third one is admin .user registered and added in group if group of user want to share files then encrypted before uploaded to cloud then aggregate key send to another group of user only authenticate user can decrypt files group of manager provide key to group of user then user can access files from cloud, search keyword using single trapdoor. System composed of seven polynomial algorithms for security. Parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing.

1. Setup: The cloud server will use this algorithm to initialize system parameters.
2. Keygen: Data owner uses this algorithm to generate his/her key pair.
3. Encrypt: Data owner uses this algorithm to encrypt data and generate its keyword cipher texts when uploading the i-th document.
4. Extract: Data owner uses this algorithm to generate an aggregate searchable encryption key.
5. Trapdoor: The user uses this algorithm to generate the trapdoor to perform keyword search.
6. Adjust: The cloud server uses this algorithm to produce the right trapdoor.
7. Test: The cloud server uses this algorithm to perform keyword search over the i-th document.

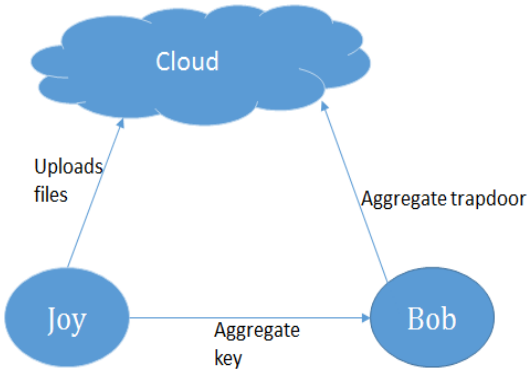

Figure 1: Framework of system

5. CONCLUSION

Key based encryption Scheme can provide an effective solution for secure and scalable data sharing system based on the cloud storage. In Key based encryption scheme, the owner only needs to distribute a single key to a user when sharing lots of documents with the user, and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner. Federated clouds are getting popular nowadays, but proposed scheme cannot be directly applied. So it is also a future scope to apply this scheme in the federated cloud environment.

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. A. Popa ,N. Zeldovich. "Multi-key searchable encryption".Cryptology ePrint Archive, Report 2013/508, 2013.Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[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] 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.

[6] 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.

[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 conferenceon 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.