Aggregation of Key with Searchable Encryption for Group Data Sharing

Mr. M. Dillibabu [1], R. Sricharan [2], R. Sibi Chakravarthy [3] M. Sandeep Kumaar [4] M. P. Nepoleon[5]
Information Technology, Panimalar Engineering College
Poonamallee, Chennai
1. Assistant Professor(IT), 2.Final Year IT, 3. Final Year IT, 4. Final Year IT, 5. Final Year IT
deenshadilli@gmail.com
charan100.sri@gmail.com
sibiitdeveloper@gmail.com
sandeep94kumaar@gmail.com
neponexz33@gmail.com

Abstract— 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.

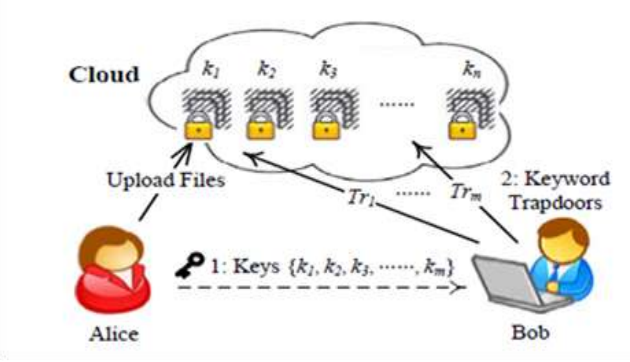
Keywords—*Multi-key searchable encryption(MKSE),Multi-user searchable encryption(MUSE).*

*****

I. Introduction

We considered the verifiability of the cloud's transformation and provided a method to check the correctness of the transformation. However, the we did not formally define verifiability. But it is not feasible to construct ABE schemes with verifiable outsourced decryption following the model defined in the existing. Moreover, the method proposed in existing relies on random oracles (RO). Unfortunately, the RO model is heuristic, and a proof of security in the RO model does not directly imply anything about the security of an ABE scheme in the real world. It is well known that there exist cryptographic schemes which are secure in the RO model but are inherently insecure when the RO is instantiated with any real hash function.

In this thesis work, firstly modify the original model of ABE with outsourced decryption in the existing to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.



In this paper we only focus on CP-ABE with verifiable outsourced

decryption . The same approach applies to KP-ABE with verifiable outsourced decryption. To assess the performance of our ABE scheme with verifiable outsourced decryption, we implement the CP-ABE scheme with verifiable outsourced decryption and conduct experiments on both an ARM-based mobile device and an Intel-core personal computer to model a mobile user and a proxy, respectively

Sender securely sends the searchable encryption keys to the receiver for all the documents. Receiver in turn must generate keyword trapdoors for all the keys.

Large number of documents will produce large number of keys and keyword trapdoors.

Thus, Storage becomes too expensive for the receiver client side device.

II. LITERATURE SURVEY

D.Boneh,B.Lynn,H.Schacham[1] in 2001 developed a paper "Short signatures from theWeil pairing". Signatures are typed and sent over a low bandwidth channel.The main disadvantage is that it adds more security to cloud.But the system is vulnerable to other attacks.J. Li, Q. Wang, C. Wang[2] presented "Achieving Secure,Scalable, and Fine-Grained Data Access Control in Cloud Computing" in 2010 addresses the challenging open issue by defining and enforcing access policies based on data attributes. It nables multiple access control.But the Searching of the data is complex. C. Bosch, R. Brinkma, P. Harte[3] in 2011 presented "Conjunctive wildcard searchover encrypted data". Which overcomes the problem of wildcard searches over encrypted data to make search queries more flexible.The main advantage is Search encrypted filters.But the Outsourcing to the cloud vendors are in jeopardy .S. Kamara, C. Papamanthou, T. Roeder[4] presented "Dynamic searchable symmetric encryption" in 2012. The main function is to enable a client to securely outsource its data to an untrusted cloud provider without sacrificing the ability to search over it.This provides Good wavelength between User and Vendor but it Cannot trust multiple owners.

X. Liu, Y. Zhang, B. Wang, and J. Yan[5] presented “MONA: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud” in 2013.This functions by securing multi owner data sharing scheme named MONA, for dynamic groups in the could.This Improves the functionality of the organizations but the disadvantage is Using Multiple Keys .

C. Chu, S. Chow,W. Tzeng, et al[6] developed ”Key-aggregate cryptosystem for scalable data sharing in cloud” in 2014 .In this,One can aggregate any set of secret key and make them compact as a single key. Single key is used here but the main disadvantage is the absence of Trapdoors.

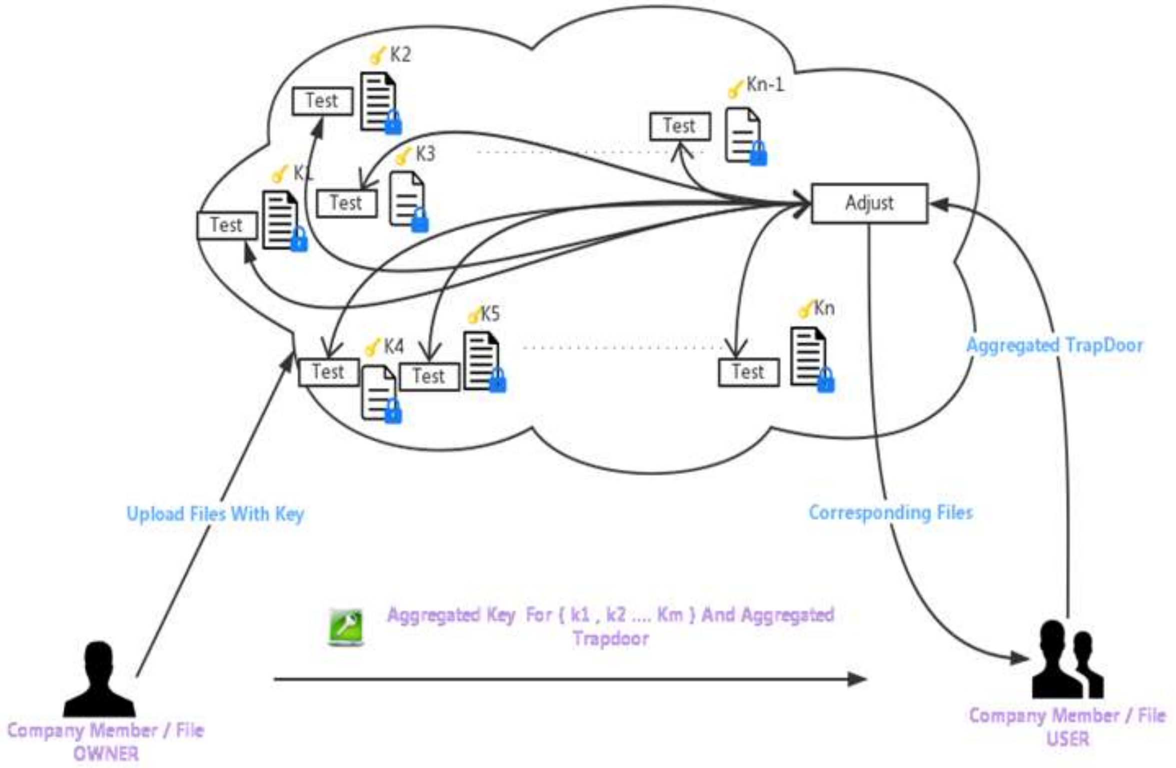
III. PROPOSED METHODOLOGY

The user, manager or CSP wants to access the admin panel. They need to register their user name and password to enter the admin panel and then manager alone will be involved in space allocation . Based on the current available space, he will request the CSP for the space to store.Cloud space provider will see the managers space request and based on it,he will provide the cloud space and group ID for the company members.The manager after getting the group ID he will create a group name and password, then he will add the company members to that group.

After getting the credentials from the manager , the group members can upload file by browsing the document.By clicking upload, the file in the server side will be read and encrypted . Finally keyword will be generated.If the owner of the document needs to share file with certain members of the group he needs to select the member name and click share. On clicking share the server side coding will collect file keys and keywords and generate aggregate key and trapdoors for members.

A company group member can get a file by using the trapdoor generated for him. On clicking search, adjust algorithm will generate different file keys and test algorithm searches the specific document’s key. If the document is present , the document will be displayed in front of the group member.

In case the member needs to access the document , he needs to download the file by entering aggregate key and by clicking download. After that original key will be displayed , file will be decrypted and downloaded in the download folder.If the manager needs to extend the space he needs to click the additional space icon and he needs to fill how many pages is required .Request will be sent to CSP for additional space , based on the requirements he will send the extended space but it will affect the managers group space with validity i.e the extended space will be available for certain period of time.After using the cloud space , if there is any dissatisfaction regarding CSP the manager can comment in the feedback box. The admin will overlook the feedback and takes action


K2
Test
Kn-1
Test
K3
K1
Test
Test
Adjust
K5
Kn
K4
Test
Test
Test
Aggregated TrapDoor
Upload Files With Key
Corresponding Files
Aggregated Key For { k1 , k2 .... Km } And Aggregated Trapdoor
Company Member / File OWNER
Company Member / File USER

1.AUTHENTICATION MODULE:

In this module , if any of the user, manager or CSP wants to access the admin panel. They need to register their user name and password to enter the admin panel.

2.CLOUD SPACE REQUEST MODULE:

In this module , manager alone will be involved . Based on the current available space, he will request the CSP for the space to store.

3.ALLOCATION SPACE MODULE:

In this module, cloud space provider will see the managers space request and based on it,he will provide the cloud space and group ID for the company members.

4.ADD MEMBERS MODULE:

In this module , the manager after getting the group ID he will create a group name and password, then he will add the company members to that group.

5.UPLOAD FILE MODULE:

After getting the credentials from the manager , the group members can upload file by browsing the document . By clicking upload, the file in the server side will be read and encrypted . Finally keyword will be generated.

6.SHARE FILE MODULE:

If the owner of the document needs to share file with certain members of the group he needs to select the member name and click share. On clicking share the server side coding will collect file keys and keywords and generate aggregate key and trapdoors for members.

7.SEARCH FILE MODULE:

In this module, a company group member can get a file by using the trapdoor generated for him. On clicking search, adjust algorithm will generate different file keys and test algorithm searches the specific document's key. If the document is present , the document will be displayed in front of the group member.

8.DOWNLOAD FILE MODULE:

In case the member needs to access the document , he needs to download the file by entering aggregate key and by clicking download. After that original key will be displayed , file will be decrypted and downloaded in the download folder.

9.ADDITIONAL SPACE MODULE:

If the manager needs to extend the space he needs to click the additional space icon and he needs to fill how many pages is required . Request will be sent to CSP for additional space , based on the requirements he will send the extended space but it will affect the managers group space with validity i.e the extended space will be available for certain period of time.

10.FEEDBACK MODULE:

After using the cloud space , if there is any dissatisfaction regarding CSP the manager can comment in the feedback box. The admin will overlook the feedback and takes action

IV. CONCLUSION

In this Proposed System An effective data sharing with aggregated key and keyword searching by using aggregated trapdoor are generated and sent to another members in a group.So overcome existing system works.

REFERENCES

[1] 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.
[2] 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.
[3] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.
[4] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114- 127, 2011.
[5] Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
[6] 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.
[7] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
[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] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.
[10] 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.
[11] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[12] 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.
[13] 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.
[14] 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.
[15] 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.