ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Secure Data Transmission in Cloud Storage Using KASE Scheme

Girish Kumar D[1], H. Mounika[2], Madhuri[3], P Anusha[4], Chandana G U[5]

Asst. Professor, Department of ISE, Ballari Institute of Technology and Management, Ballari, India[1]

B.E Student, Department of ISE, Ballari Institute of Technology and Management, Ballari, India[2,3,4,5]

ABSTRACT*:* In cloud, there is an important functionality called Data sharing. Data sharing is also concerned about the security, efficiency and flexibility for the data to share in the cloud storage. The capacity of selectively sharing encrypted data with different users via public cloud server may great ease security concerned over inattentive data leaks in the cloud. The key challenging of designing encryption scheme is lies between the efficient management of encryption keys. Here address the practical problem which is largely neglected in the literature. By proposing the novel concept of Key-aggregate searchable encryption and also instantiating the concept through concrete KASE scheme where the data owner need to distribute a single key to data user for sharing large number of documents, and the user only needs to submit a single trapdoor to cloud for querying the shared documents. A new public-key cryptosystem is introduced to produce a constant size cipher text called KASE. Based on the text methodology as a key the key is used to share the data safely. Once the sharing is completed the key aggregate differs from key aggregate cryptosystem and this process provides efficient solution than the existing system.

KEYWORDS: Cloud storage provider, out sourcing, attribute based encryption, key aggregate Crypto system.

I. INTRODUCTION

Cloud storage is merged as a promising solution for providing ubiquitous, convenient and on-demand access to large amounts of data shared over the internet. At the present days millions of users are sharing their personal data, such as images, videos and confidential documents, with their friends or any organizations through social network application based on the public cloud storage in the daily processes. Business users are also sharing their documents or group of files attached with cloud storage due to its numerous benefits, including low cost, greater agility, and better resource utilization. However while enjoying the convenience of the data sharing via cloud storage user increasingly concerned about inadvertent leaks in cloud storage. Such data leaks caused by malicious adversary, or misbehaving of the cloud operator, it leads to serious breaches of personal privacy or business secrete. To address the user concern about the data leaks a common approach is for the data owner to encrypt all the data which is to be shared before uploading them to the cloud, and later encrypted data is retrieved and decrypted by those who have the decrypted keys. This type of cloud storage is called cryptographic cloud storage. Here a common solution to employ a searchable encryption(SE) scheme in which the data owner is required to encrypt the potential keywords and upload them to the cloud together with encrypted data, then for retrieving data matching a keyword, the user need to submit the corresponding keyword trapdoor to the cloud for performing search over the encrypted data. By combining searchable encryption scheme with cryptographic cloud storage, implementing such type of system for large scale application involving millions of users and billions of files to share is hindered by practical issues involving the efficient management of encryption keys which is largely ignored in the literature. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical. So that, this project address the key challenge by proposing the concept of Key-aggregate searchable encryption (KASE), and instantiating the concept through concrete KASE scheme. This proposed KASE scheme applies in any cloud storage that supports the searchable group data sharing functionality, which means user may selectively share the group of data to the group of users by submitting the single aggregate trapdoor to the public cloud storage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

II. LITERATURE SURVEY

1. 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.

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 cipher texts such that efficient delegation of decryption rights for any set of cipher texts 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 cipher text 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.

2. 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.

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public key for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

III.EXISTING SYSTEM

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared tenancy cloud computing environment, things become even worse. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owners anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality .A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff. Drawbacks are a**)** The costs and complexities involved generally increase with the number of the decryption keys to be shared b) The encryption key and decryption key are different in public key encryption.

IV.PROPOSED SYSTEM

The design of our KASE scheme draws its insights from both the multi-key searchable encryption scheme and the key-aggregate data sharing scheme .Specifically, in order to create an aggregate searchable encryption key instead of many independent key. Each searchable encryption key is associated with a particular index of document, and the aggregate key is created using the owner's master-secret key & public keys associated with the documents. In Order to search the respected document from the cloud server, single aggregate trapdoor is submitted to the cloud server. If match occurs

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

between the shared document in cloud and requested documents, then cloud will return requested & respective documents to the user. Then user will download and decrypt the document by using the decryption keys.

V.SYSTEM ARCHITECTURE AND DESIGN

System Architecture is the functional model that describes the structure, conduct, and more perceptions of a framework. An engineering depiction is a formal portrayal and illustration of a framework, sorted out in a way that thinks about the structure of the architecture which involves framework segments, the connections (e.g. the behaviour) amongst them, and gives a platform from where the items can be attained, and frameworks built up, that will cooperate to actualize the universal framework.

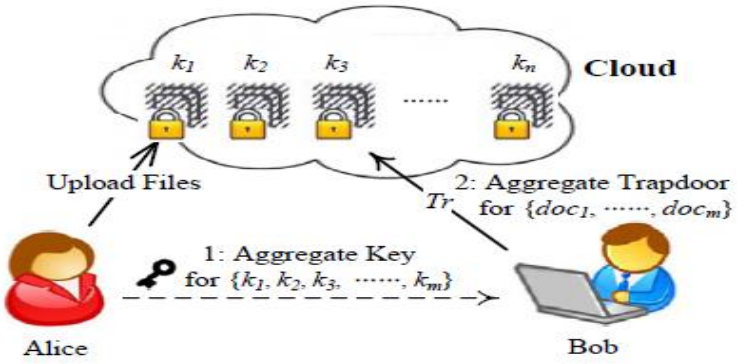


Fig: Key-aggregate Searchable Encryption

The above fig consists of a data owner who generates a single aggregate key which was created by using public key and masters secrete key for encrypting the shared documents. The produced single aggregate key is send to the data user through secure communication channel. Then data user can perform the searching over the shared documents by submitting the single aggregate trapdoor, which is created by the data users to the cloud server.
Cloud server performs some of the algorithms by using aggregate trapdoor over the collection of documents. And lastly, test algorithm is performed to ensure that the respective request has the right to access them. If the match occurs, cloud server return all the shared documents to the respective data user.

VI.EXPERIMENTAL RESULTS

1.User Registration:

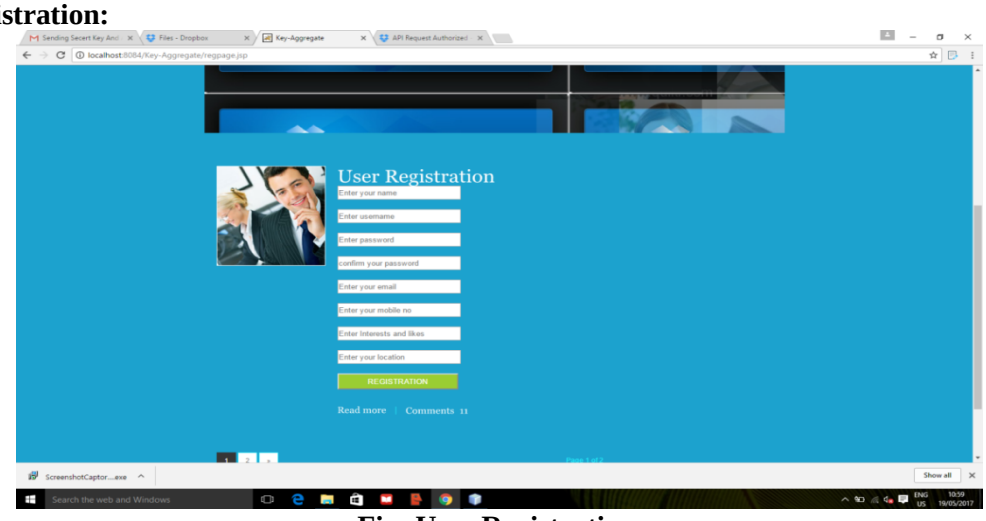


Fig: User Registration

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Registration: User can register with basic information like user name ,Email-Id, mobile number, etc...

2.Admin Login:

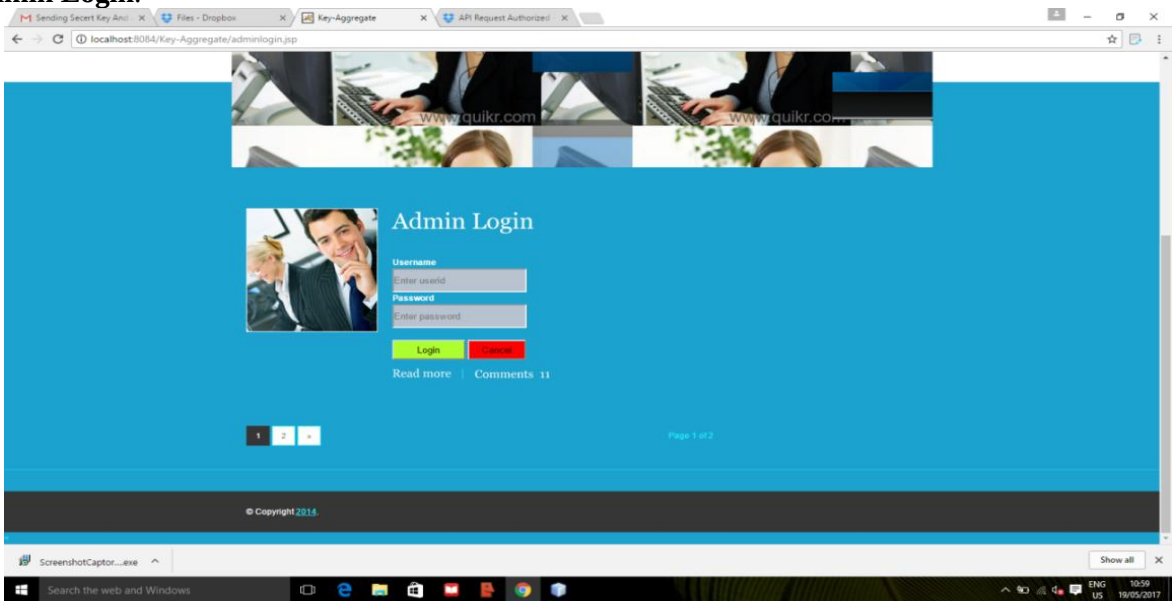


Fig: Admin Login

Admin should login with his username and password.

3.Sharing & Sending keys:

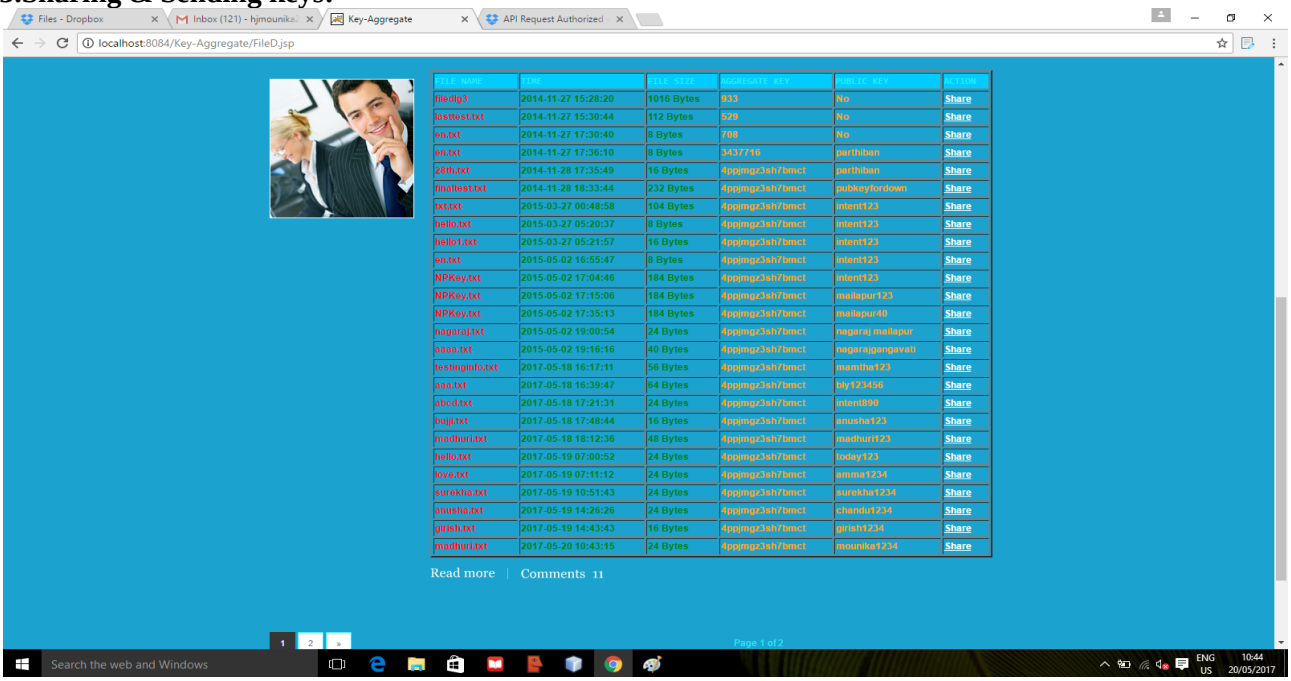


Fig: Sharing the document

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

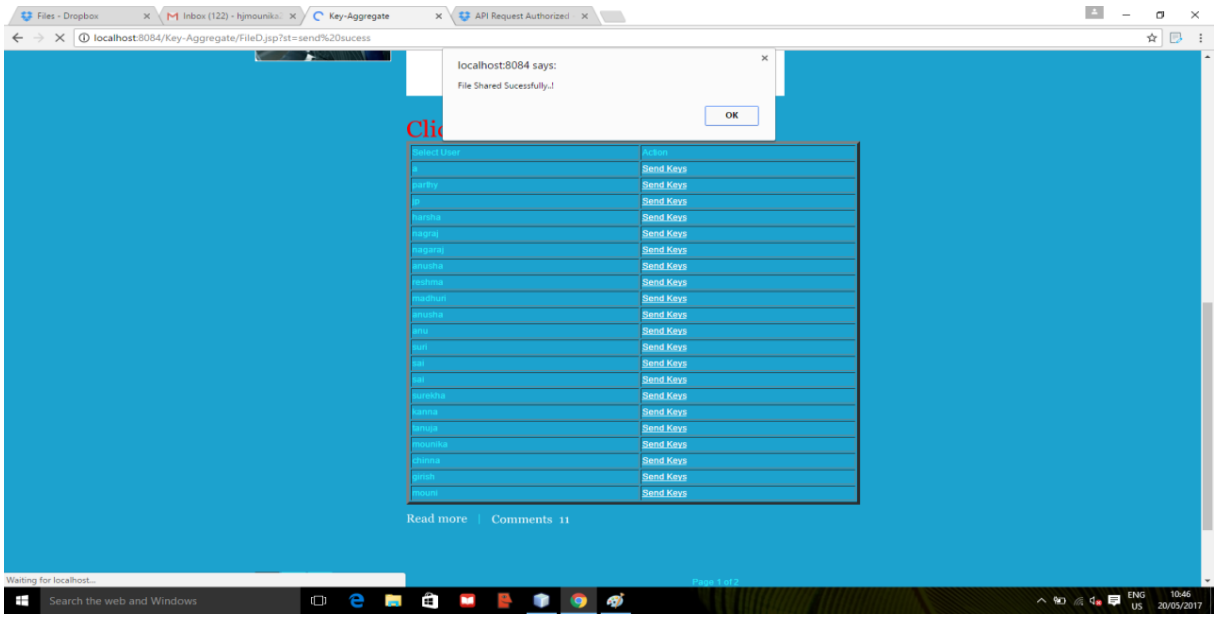
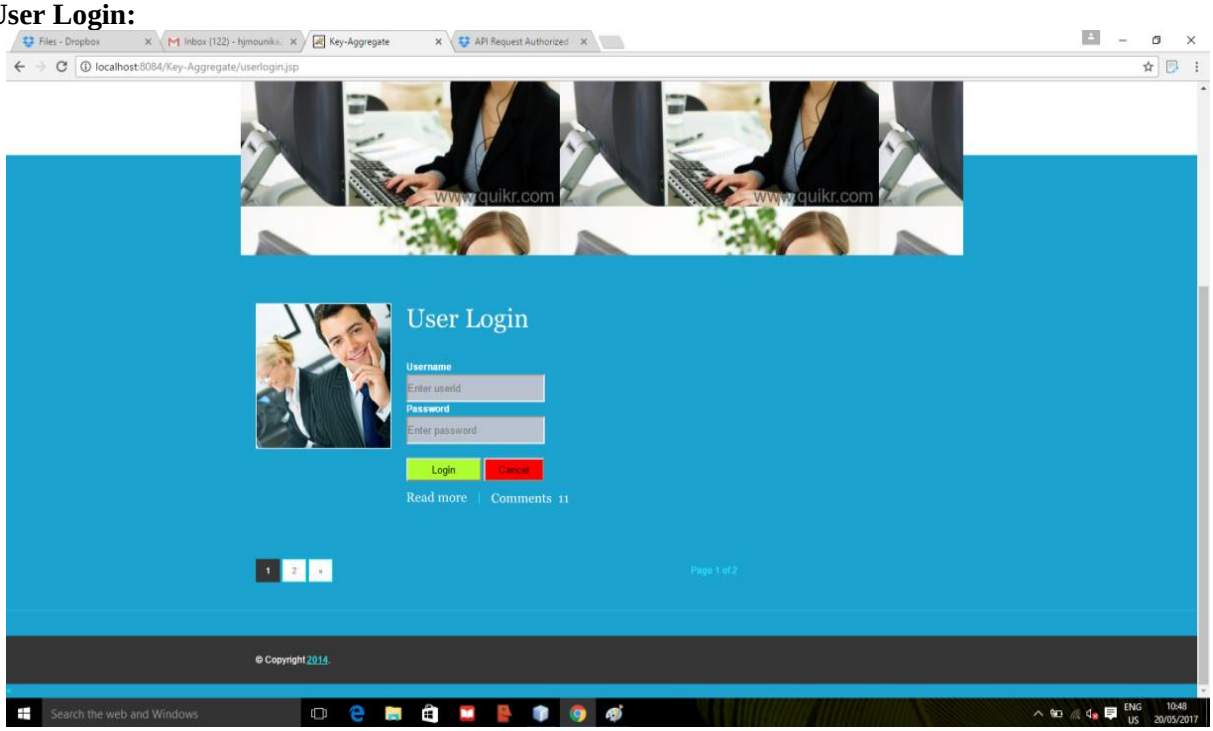


Fig: sending the keys to user

The Created document is shared to the selected user by sending the document name, aggregate key & public key to the particular user Email-Id.

4.User Login:



User should login with his username and password to download the files.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

5.File Downloading:

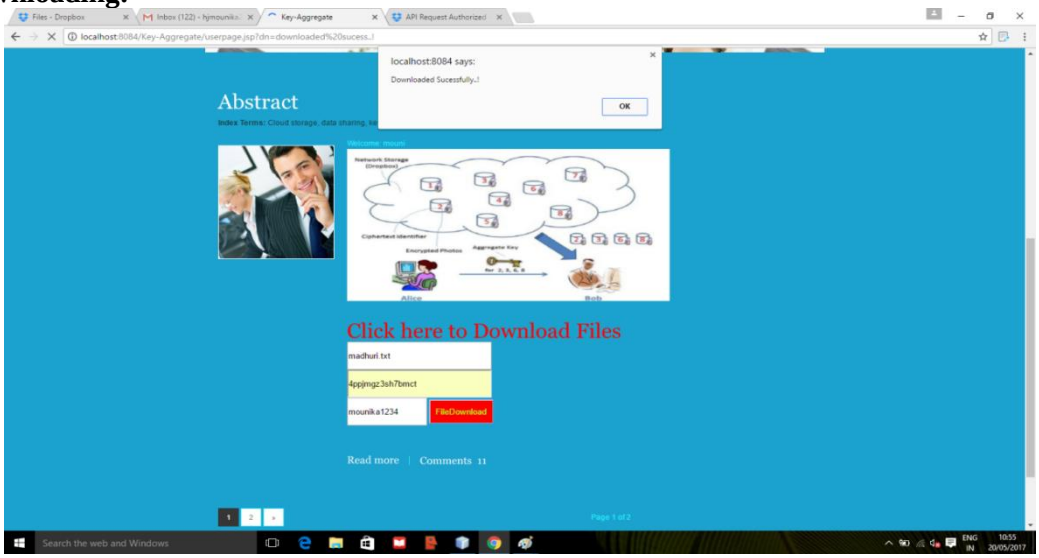


Fig: File downloading

File can be downloaded by giving the details of document name, aggregate key & public key which has been sent to the user Email-Id. Downloaded files will be stored in the drop box of D-drive.

6.Decryption:

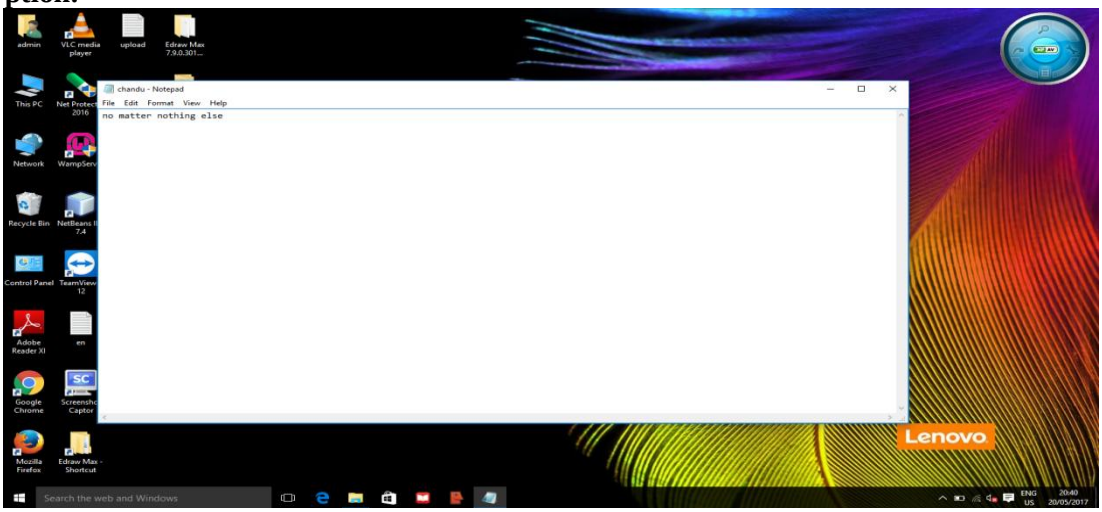


Fig: Decrypted message

User can decrypt the encrypted data by using the decryption key.

Advantages of proposed system

- ✓ To avoid inadvertent data leaks in the cloud and privacy for preserving data.
- ✓ To distribute single key to a user for sharing number of documents using KASE scheme.
- ✓ To submit a single trapdoor to the cloud for querying the shared documents.
- ✓ It is more secure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- ✓ Decryption key should be sent via a secure channel and kept secret.
- ✓ It is an efficient public-key encryption scheme which supports flexible delegation.
- ✓ To the best of our knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy requirements

VII.CONCLUSION

As here, by considering the practical problem of privacy preserving data sharing system based on public cloud storage, where the data owner distribute a large number of keys to user to enable them and to access their documents so that this particular project is proposed i.e, the concept of key aggregate searchable encryption(KASE), and implement as a concrete KASE Scheme. This project confirms both analysis and evaluation results that the work can provide an efficient data sharing system on public cloud storage. In this KASE Scheme the owner only needs to distribute a single key to a user while sharing the lots of documents with the user and user only need to submit a single trapdoor to retrieve all the shared documents from the same owner. If user wants to query the documents shared by multiple owner, they must generate multiple trapdoors to the cloud. Such that, the data user can retrieve the required respective encrypted documents which are shared by the data owners.

REFERENCES

[1] Chu, S. chow, W. Tzengetal. "Key-aggregate cryptosystem for scalable data sharing in Cloud Computing" IEEE Transactions on parallel and Distributed systems 2014, 25(2); 468-477.
[2]. Baojiang Cui, Zheli Liu_ and Lingyu Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, 2015.
[3].X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multi-owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.
[4]. 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
[5].X. Song, D. Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2014
[6]. 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.
[7] 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.
[8] X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures", IEEE Trans. on Parallel and Distributed Systems,
DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180.
[9] 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.
[10] 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.