ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

An Application for Scalable Data Sharing in Cloud Storage

Mithun V Mhatre[#1], Dr. M.Z. Shaikh[#2]

M.E Student, Dept. of Computer Engineering, Bharati Vidyapeeth's College of Engineering, Delhi, India [#1]

Principal, Bharati Vidyapeeth's College of Engineering, Delhi, India[#2]

ABSTRACT: Cloud technology is very constructive and useful in present new technological era, where aperson uses the internet and the remote servers to give and maintain data as well as applications. Suchapplications in turn can be used by the end users via the cloud communications without any installation.Moreover, the end users‟ data files can be accessed and manipulated from any other computer using theinternet services. Despite the flexibility of data and application accessing and usage that cloud computingenvironments provide, there are many questions still coming up on how to gain a trusted environment thatprotect data and applications in clouds from hackers and intruders.Cloud storage should be able to store and share data securely, efficiently, and flexibly with othersin cloud storage. The costs and complexities involved generally increase with the number of thedecryption keys to be shared. The encryption key and decryption key are different in public keyencryption. Since we are proposing new era of Aggregate key cryptography. To produce constant lengthciphertext is also one of important task that we have materialized. In this paper, we propose a simple,efficient, and publicly verifiable approach to ensure cloud data security while sharing between differentusers. Since we introduce here, aggregate- key cryptosystem. Cryptographic methods are usually appliedto address this data sharing issue.

KEYWORDS: Cloud storage, public key encryption, cryptosystem, key aggregate encryption, and key aggregate cryptosystem.

I. INTRODUCTION

Cloud computing is considered as the next step in the evolution of on-demand information technology which combines a set of existing and new techniques from research areas such as service-oriented architectures (SOA) and virtualization. With the rapid development of versatile cloud computing technology and services, it is routine for users to leverage cloud storage services to share data with others in a friend circle, e.g., Dropbox, Google Drive and AliCloud. The shared data in cloud servers, however, usually contains users‟ sensitive information such as personal profile, financial data, health records, etc. and needs to be well protected. As the ownership of the data is separated from the administration of them, the cloud servers may migrate users‟ data to other cloud servers in outsourcing or share them in cloud searching. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authorization period and to provide fine-grained access control during this period. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. And main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. But it’s having serious issues while handling huge database and transaction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

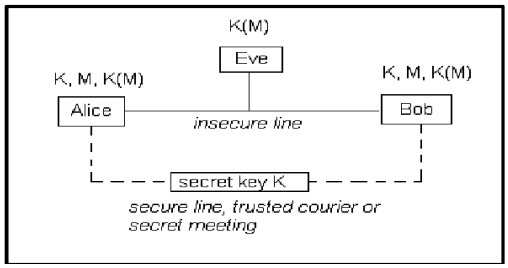

Figure 1: Public-key cryptography

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used, for example, to encrypt plaintext or to verify a digital signature; whereas the private key is used for the opposite operation, in these examples to decrypt ciphertext or to create a digital signature. 1. The costs and complexities involved generally increase with the number of the decryption keys to be shared. 2. The encryption key and decryption key are different in public key encryption. 3. 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 owner's anonymity.

Cryptography technique can be applied in a two major ways- one is symmetric key encryption and other is asymmetric key encryption. In symmetric key encryption, same keys are used for encryption and decryption. By contrast, in asymmetric key encryption different keys are used, public key for encryption and private key for decryption. Using asymmetric key encryption is more flexible for our approach. This can be illustrated by following example. Suppose Alice put all data on Box.com and she does not want to expose her data to everyone. Due to data leakage possibilities she does not trust on privacy mechanism provided by Box.com, so she encrypt all data before uploading to the server. If Bob ask her to share some data then Alice use share function of Box.com. But problem now is that how to share encrypted data. There are two severe ways: 1. Alice encrypt data with single secret key and share that secret key directly with the Bob. 2. Alice can encrypt data with distinct keys and send Bob corresponding keys to Bob via secure channel. In first approach, unwanted data also get expose to the Bob, which is inadequate. In second approach, no. of keys is as many as no. of shared

II. CLOUD DATA ENCRYPTION BASED QUANTUM (CDEQ)

Cloud data encryption based quantum technology platform dispels all security fears throughcloud data transmission [3], [4]. This technology offers: simple low-cost data protection, toolsand security services integration, and an efficient disasters recovery. Quantum technology solvesone of the key challenges in distributed computing. It can preserve data privacy when usersinteract with remote computing centers [6]. Its power came from the deployment of theQuantum Cryptography or Quantum Key Distribution (QKD) mechanisms, which are consideredas the art of the encryption/ encryption process [7], [8], see fig.1. Through quantum channels,data is encoded based on prepared states known as photons. These photons are then sent as"keys" for encryption/ decryption secured messages [9]. The advantage of using such photons indata transmission lays in the no-cloning theorem (the quantum state of a single photon cannot becopied).

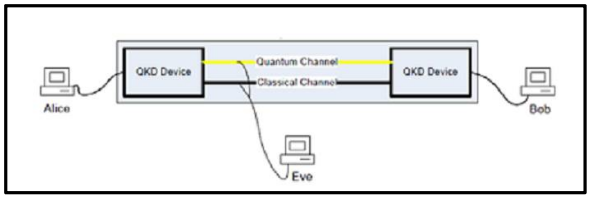

Figure 2: Schematic of QKD

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

III. THE CASE STUDY

The application developed using the cloud data encryption based quantum.

The application developed in ASP.net, is an application provided for sharing of data between the staff and the students. The login id for the staff and the students are created, and the staff can upload the notes of the subjects and the complete study material which they want to share with their students.
The Figure 3, shows the staff screen to upload the file.

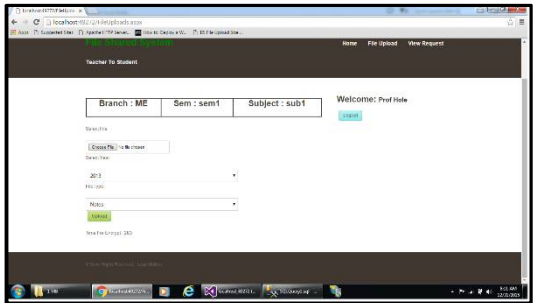

Figure 3: Staff Upload Screen

The students can download the various files uploaded by the staff on request. It is than shown as depicted in Figure 4.

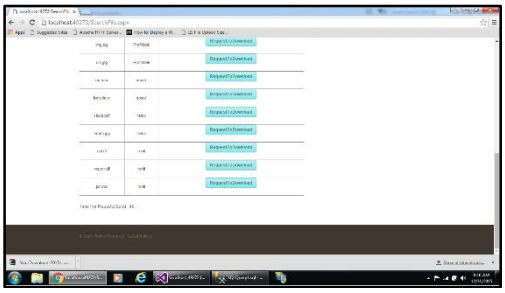

Figure 4: Student Request

If there's no request than the screen is shown as below in Figure 5.

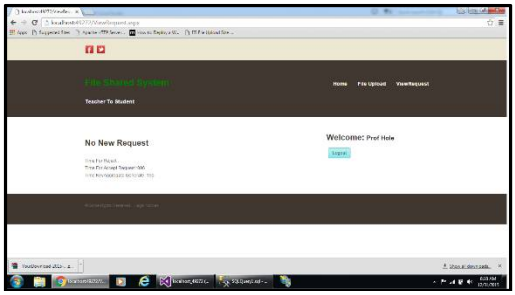

Figure 5: No Request screen

The time to upload the various files are as shown below in figure 6, and the encryption time for the same is predicted in Figure 7

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

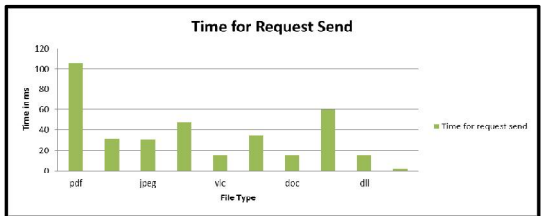

Figure 6: Time of various file upload

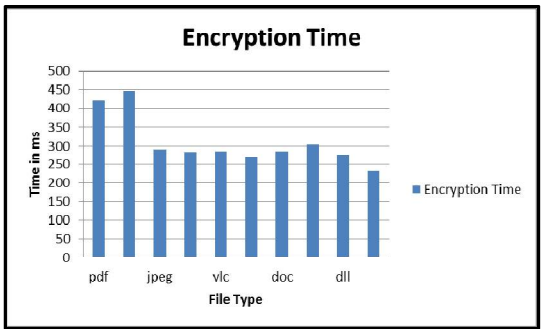

Figure 7: Encryption Time

The key is accepted which is sent as an aggregate key for downloading the file. The table below shows the detailing of the various keys generated to accept the key and time for key aggregation. The application created plots for the two values.

Time to accept Key	Time for Key Agg.
78	36
138	70
451	201
416	271
374	642

Figure 8: The key Aggregate Values

The graph plotted for the above data is

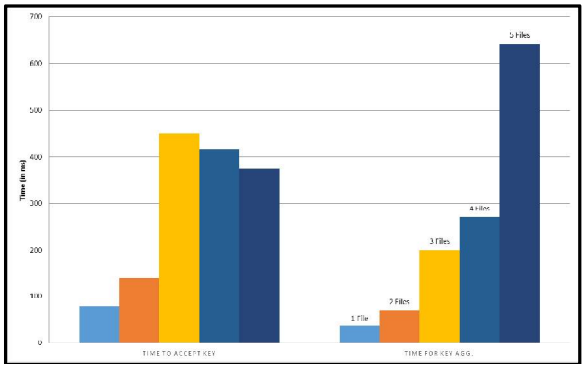

Figure 9: The plot of graph

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

File size is an important factor to compare the file size compare. The table below shows the various file size and its encryption time.

File size (in KB)	Encryption Time (in ms)
105	95
200	147
302	187
435	210
591	225
654	237
734	327
836	430
917	532

The plot of graph for the same, on the parameters of file size and its encryption time in ms.

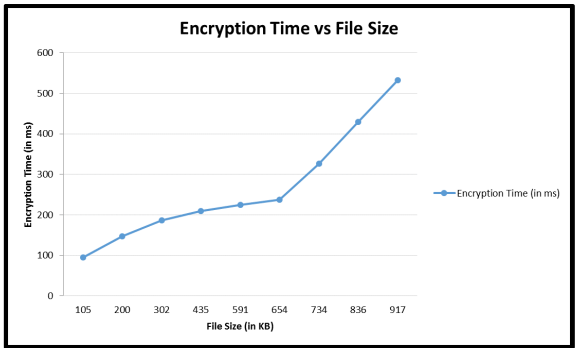

Figure 10: Encryption time vs File size

After checking for the file size, the next step is to check for the more complex procedure for the File type, with respect to its encryption time in ms.The various file types are the common types used in our daily accessibility.

File Type	Encryption Time (in ms)
Word (10MB)	42
PDF (10MB)	102
TXT (10MB)	132
ISO (1MB)	312
DLL (1MB)	322
JPEG (1MB)	327
VLC (1MB)	330

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

((A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

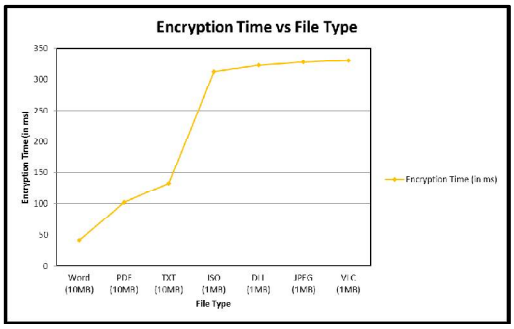

Figure 11: Encryption Time vs File Type

IV. CONCLUSION

This application on cloud can help the teaching feternity to share the data easily and connect easily with many students. In this paper, proposed system is found to be very efficient for sharing the data on cloud.
For this we have used Key aggregate encryption algorithm which support delegation of secret keys for different ciphertext classes in cloud storage. It also produces constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts which is here possible. Since in traditional methods unexpected privilege escalation will expose all data. And that we are able to avoid and provide more security by using key aggregate algorithm.

REFERENCES

1. G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009,http://www.theregister.co.uk/ 2009/03/16/ azure_cloud_crash/
2. P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation,January 2007, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf.
3. G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal,March 26, 2010.
4. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng,"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.
6. Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.
7. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
8. M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in CM Conference on Computer and Communications Security, 2009, pp. 121 –130.
9. S. Singh,"Different Cloud Computing Standards a Huge Challenge", The Economic times, 4 June 2009
10. J. Urquhart, "The Biggest Cloud computing Issue of 2009is Trust", C-NetNews, 7 Jan 2009.
11. Wangetai, "Scientific Cloud Computing: Early Definition and Experience",Proc. 10th International Conference High-Performance Computing andCommunications (HPCC 03)