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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Searchable Encrypted Data Sharing In Cloud Using Aggregate Trapdoor

Varsha Kadam[1], Prof. C. S. Kulkarni[2]

P.G. Student, Department of Computer Engineering, JSPM Narhe, Pune, Maharashtra, India[1]

Associate Professor, Department of Computer Engineering, JSPM Narhe, Pune, Maharashtra, India[2]

ABSTRACT: With the rapid development of information usage in society in the recent years, cloud systems are being more frequently used by Internet users. Among the many functions of cloud systems, the uploading and downloading files are more often used. But if the numbers of files are numerous, the keys which can decrypt the downloading files are also numerous. We address this practical problem by proposing key aggregate method with searchable encryption, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The encrypted data is search by trapdoor on cloud. Trapdoor is created by end user. To share the security key we have used secure electronic mailing system. The result of proposed system shows that our system is efficient and secure for cloud data sharing.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption, trapdoor.

I. INTRODUCTION

Most Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data [3], [5]. Cloud storage services may be accessed through a co-located cloud compute service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service or deployed on-premises. Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage. The dada sharing is important application of cloud computing [6]. One can upload or download the data inside cloud. We can store any type of data on cloud. That means data shared may be in the text format or may be in the multimedia format. This sharing of data should be in secure, efficient and flexible manner [8]. Otherwise the data attacker may stole our personal information and may misuse it.

To achieve such type of security inside the cloud we have used the key aggregation technique. In this we are encrypting the data which user want share on the cloud. For this encryption we are using the secrete key. It will create ciphers of fixed data size. These cyphers can be decrypt by using the aggregate key. This aggregate key will decrypt only bunch of cyphers other remaining ciphers will be confidential.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

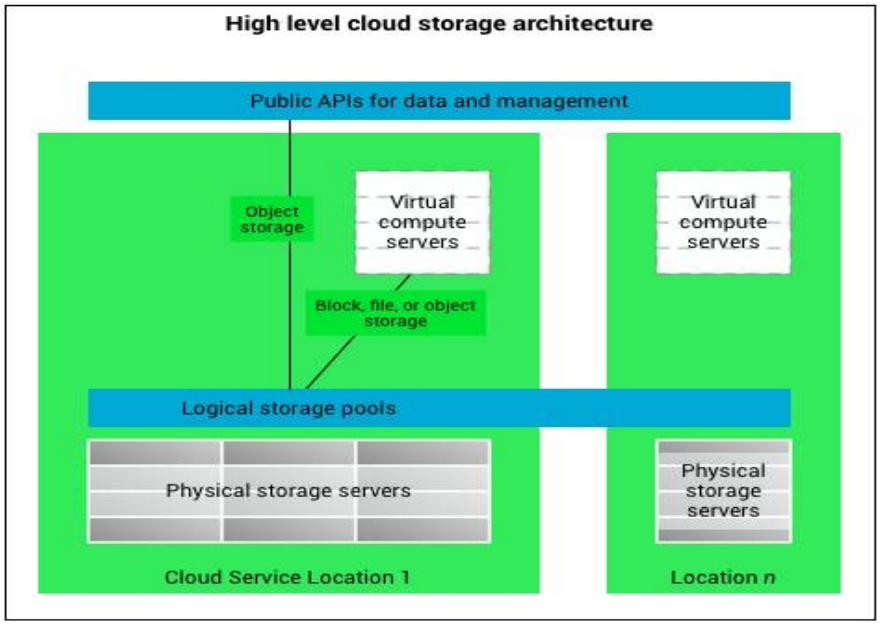

Figure 1.Architecture of data sharing in cloud storage

II. LITERATURE SURVEY

The importance of data sharing and the need to ensure privacy and security is discussed in [7], [9] a number of existing articles.

1. Security and privacy in the cloud:

This paper outlines the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. It provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud [12]. This explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud.

2. Dynamic Broadcast Encryption:

This paper uses Broadcast encryption which enables a broadcaster to transmit encrypted data or information to a set of users so that only a targeted subset of users can decrypt the data. Other than above characteristics, dynamic broadcast encryption it also allows the group monitor to include new members by preserving previously computed information, and user decryption secret keys need not be computed again and again [11], the Aggregation logic and size of cipher texts are remain unchanged and the group encryption key requires no modification.

3. Data Sharing in Cloud Using Hybrid Cryptosystem:

This system uses the slice of data cloud to encrypt or decrypt the data. The original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs [10], the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. The data owner retrieve the signature from secure mediator and then it allows user to upload or download the data over the cloud.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

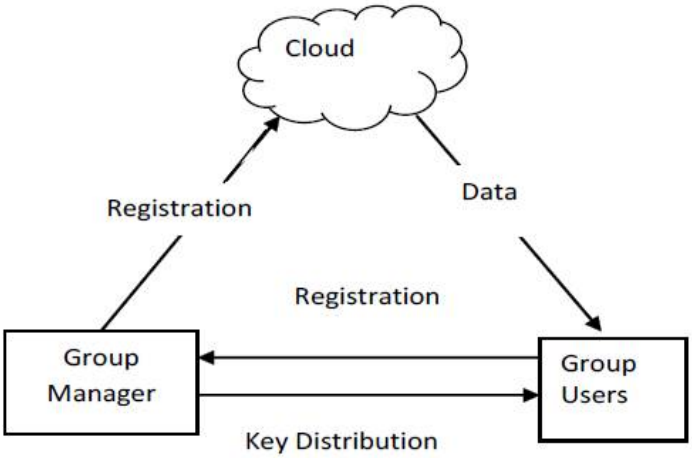

Figure: 2. Dynamic Broadcast Encryption.

4. Cryptographic storage system:

This system allows sharing of secure file on untrusted servers. It divides files into the group of file and encrypt each group of file with a unique file-key. The data owner can share the file groups with others by delivering the related lockbox key, where the lockbox key is used to encrypt the file-block keys [15]. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-key needs to be updated and distributed again for a user revocation.

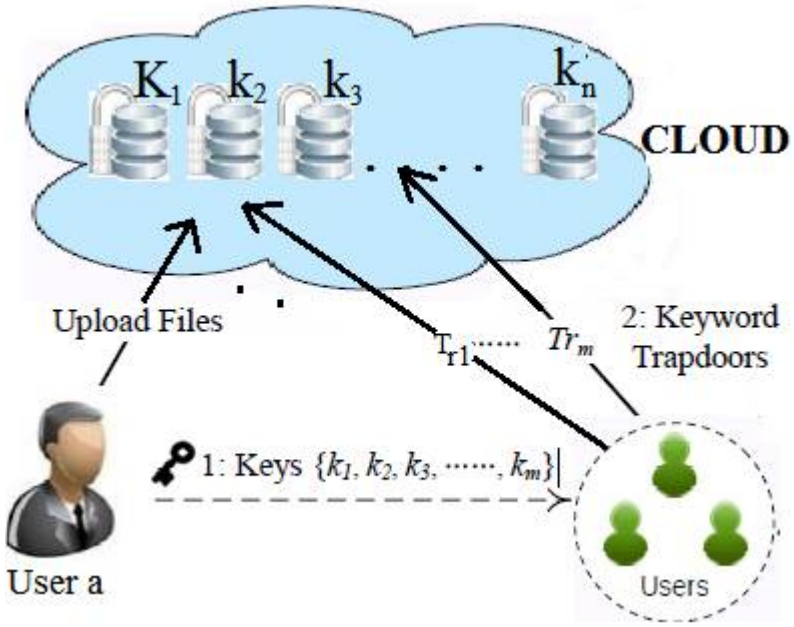

Figure. 3 Traditional Approach

The above figure shows the traditional approach of data sharing in which when user a wand to share the data over cloud then he needs to send bunch of aggregate keys to the end user and also end user will user keyword trapdoor. This system not supports the sharing of large number of files over cloud by using single aggregate key.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. PROPOSED SYSTEM

We proposed key aggregate method with searchable encryption, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents.The encrypted data is search by trapdoor on cloud. Trapdoor is created by end user. Proposed scheme supports searchable encrypted data sharing functionality. The following figure shows the key aggregate method with searchable encryption.

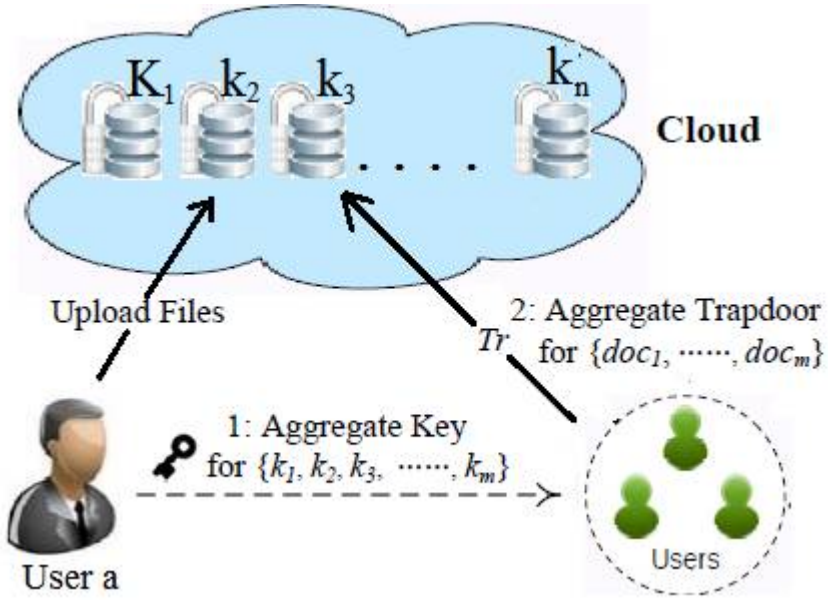

Figure 4. Proposed system

Proposed system generates two keys; one is secret key used for encryption and second is aggregate key used for decryption. The data owner creates the public system parameter and generates a secrete key which is public key pair. The data owner have rights to use the secret key from which he can generate an aggregate key which is use for decryption for a set of cipher text blocks. The both keys can be sent to end user in very secure manner. The authenticated user having an aggregate key can decrypt any block of cipher text. In proposed scheme data owner needs to submit or share only one aggregate key instead of number of aggregate keys and end user needs to submit only one aggregate trapdoor instead of number of trapdoors.

Our research work consist of main BE (Broadcast Encryption) algorithm which is comprises of three tuples setup, encrypt, and decrypt which are used to perform the above operations. These sub algorithms are as follow:

1. ***Setup:***
   This algorithm runs at data owner end. This takes input parameter as private keys to encrypt the data, number of receivers and documents to be share d, and produces security keys. The account is created on the untrusted server for sharing of data. This account is generated by data owner.

2. **KeyGen(K):**
   The keygen algorithm is get executed by the broadcaster who wants to share the data amongst n number of users. This algorithm is use for the generation of public key. The data owner generates a public secrete key to encrypt the data over cloud. He also creates an aggregate key to access the block of ciphers of limited size.

3. **Encrypt:**
   This algorithm encrypts the data provided by the data owner by using the secrete key. This encrypted data is then share among the cloud users.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

4. **Extract:**
The aggregate key is use for extracting the particular block of the ciphers from the cipher file. But other encrypted data remains secure.

5. **Trpdr(k;w):**
This algorithm is get executed by the end user to generate Trapdoor Trfor keyword W using security key K.

*Tr<---------- **Trpdr**(k;w);*

6. **Test(Tr, Cm):**
This algorithm is get executed at the user end to perform keyword search over encrypted data. It takes input Trapdoor Tr and keyword to be search, and output wether data contains particular keyword or not.

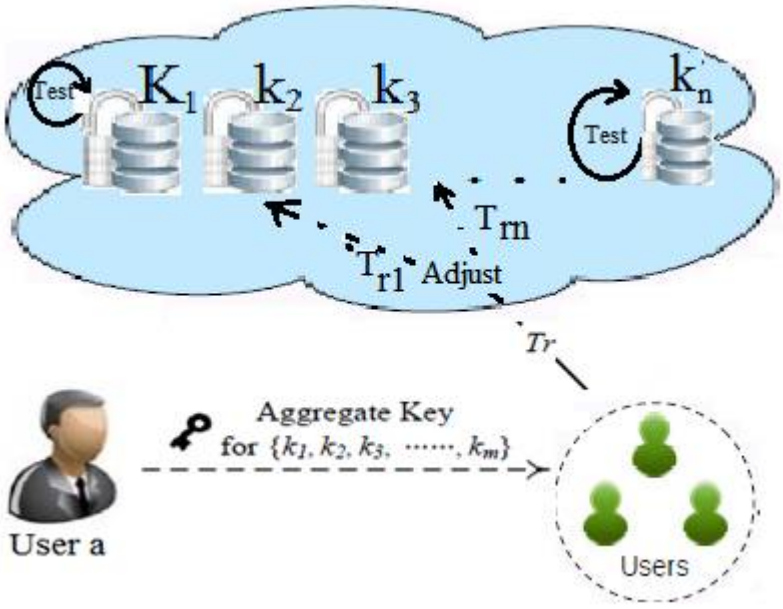

Figure 5. Key-aggregate searchable encryption

The adjust and test functions in the above figure are used to search the encrypted data. Adjust algorithm is to generate the right Trapdoor for the keyword search and Test function is to check weather document contains particular or not.

7. **Decrypt:**
The encrypted data is then decrypted by using the same secrete key which is use for encryption.

As the above figure shows, the key assignment is done in dynamic way. The aggregate key is use to decrypt only those ciphers which user wants. This key will not decrypt the other remaining ciphers. The main encryption and decryption is done by the secrete key. If any user enters the wrong secrete key or wrong aggregate key then the user will be blocked by the data owner. And the information which that user tries to retrieve is then added into non confidential storage. Only data owner can unblock that user and he may transfer the information from non-confidential storage to confidential storage. The user can only access the data on cloud if he has secret key and the aggregate key, otherwise he will be block forever.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. EXPERIMENTAL SETUP

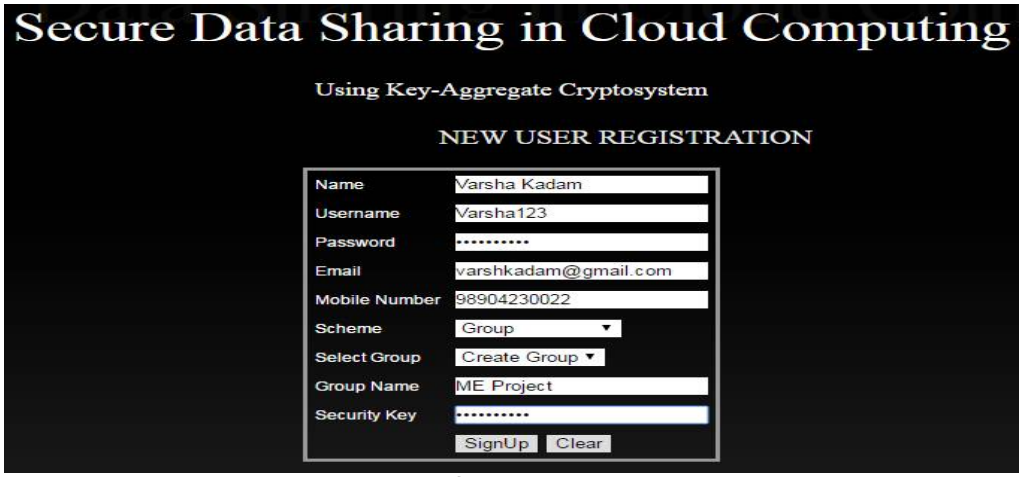

Figure6. User Registration

Figure 7. User Login

Figure 8. File Upload

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

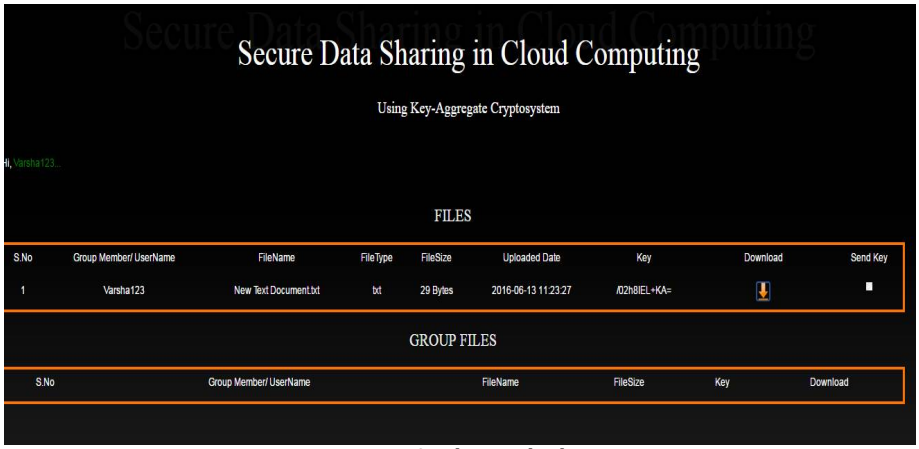

Figure 9. File Download

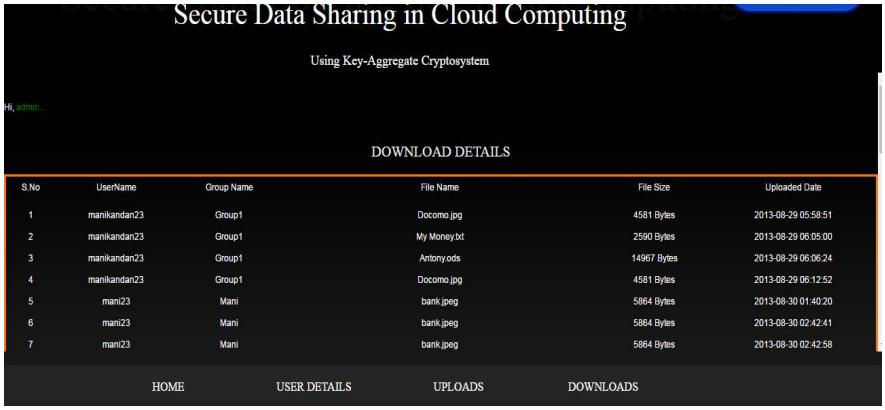

Figure 10. Download Count

Figure 11. File History

Figure 12. Upload Details

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

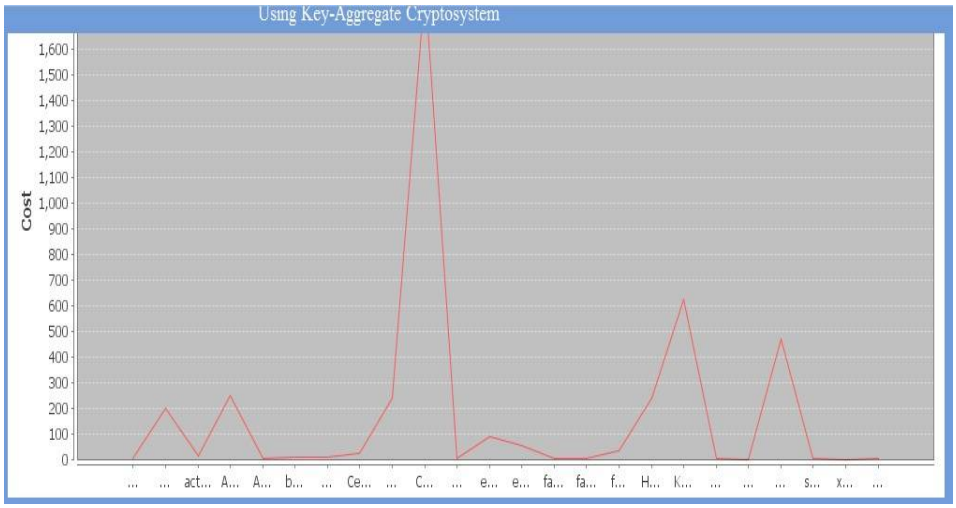

Figure 13.Cost Analysis

The above graphical analysis shows that the uploading and downloading cost of the files uploaded and downloaded on the cloud. The graph shows the file and cost of that downloaded file in KB

V. CONCLUSION

In We proposed Key aggregate method in which data owner only needs to share only one aggregate key to the user for large number of documents and end user needs to submit only one trapdoor to decrypt the files shared by the same owner. This sharing is done in a secure and confidential manner. Proposed scheme generates two keys. First is secret key which is used for encryption over the cloud. And the second key is aggregate key which is used to decrypt the data. The trapdoor is generated at user's side. This trapdoor submitted to the cloud by user. The cloud server can use this trapdoor to perform keyword search and return the result to user. The trapdoor algorithm takes as input the aggregate searchable encryption key and a keyword, then outputs only one trapdoor. The proposed system is found to be very efficient for sharing the data on cloud. However, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting is a future work.

ACKNOWLEDGEMENTS

Author would like to take this opportunity to express his profound gratitude and deep regard to my Prof. C. S. Kulkarni, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the research work. His valuable suggestions were of immense help throughout my research work. His perceptive criticism kept me working to make this research's in a much better way. Working under him was an extremely knowledgeable experience for me.

REFERENCES

1. R. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
2. L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.
3. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.
4. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
5. S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicatedto Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

6. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.
7. M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.
8. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
9. F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.
10. 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.
11. S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.
12. G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology – CRYPTO '89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.
13. W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002.
14. G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012.