Vishali. D *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 6, June- 2016, pg. 1-5 **ISSN: 2321-8363**
Impact Factor: 4.123

AN IMPLEMENTATION OF NOVEL SECURE DATA SELF-DESTRUCTING SCHEME IN CLOUD COMPUTING FOR SHARING SENSITIVE DATA

Vishali. D[1], Dr. R. Indra Gandhi[2]
[1]P. G Scholar, G.K.M. College of Engineering and Technology, Chennai, Tamilnadu, India
E-mail: vishadurai@gmail.com
[2]Professor, G.K.M. College of Engineering and Technology, Chennai, Tamilnadu, India
E-mail: shambhavi.rajesh@gmail.com

Abstract - In today's Scenario sharing resources plays a vital place in handling various application in a efficient manner. Most type of computing deals with sharing resources rather than having local servers or personal devices to handle applications. Any discussion involving data must address security and privacy, especially when it comes to managing sensitive data. After the recent leaks of countless millions of user login credentials, the privacy of your cloud-based data is another consideration. In order to tackle this problem, we propose a novel secure data self-destructing scheme in cloud computing. We create three way self-distraction scheme to secure the data using AES/DES Double Encryption Algorithm to secure the data. By using this, sensitive data will be securely self-destructed after a user-specified expiration time. Secondly, user can access the data only one time from the cloud. At last, if the user enters the incorrect key three times, the data will be self-distracted.

Key words: Delegate data, Guaranteed deletion, Confidentiality-protect, Fine-grained access control, Dynamic computing.

1. INTRODUCTION

The whole Internet takes the advantage of cloud computing for unlimited "virtualized" resources to users as services that hides the details of related platform information and implementation. Based on their commercial impact cloud service providers offer both highly available storage and massively parallel computing resources. In the recent past an increasing amount of data is being stored in the cloud by users with specified privileges. Cloud services big challenge is to manage the ever-increasing volume of data. Deduplication plays a vital role in bringing the scalability towards data management in cloud. Data deduplication is a specialized data compression technique used to eliminate duplicate copies and to improve storage utilization. Deduplication also reduces the number of bytes size while transferring data in network. The purpose of deduplication is to eliminate redundant data by keeping only one physical copy and giving link for reference. It takes place both in first and in block level. For file-level deduplication, it eliminates duplicate copies of the same file. Deduplication can also take place at the block level, which eliminates duplicate blocks of data that occur in non-identical files. Many authors shown related evident of Deduplication in their findings. Some of the author's point of view is discussed in forth coming section.

2. PROPOSED SYSTEM

A key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, every ciphertext is labeled with a time interval while private key is associated with a time instant. The ciphertext can only be

decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure.

2.1. ARCHITECTURE

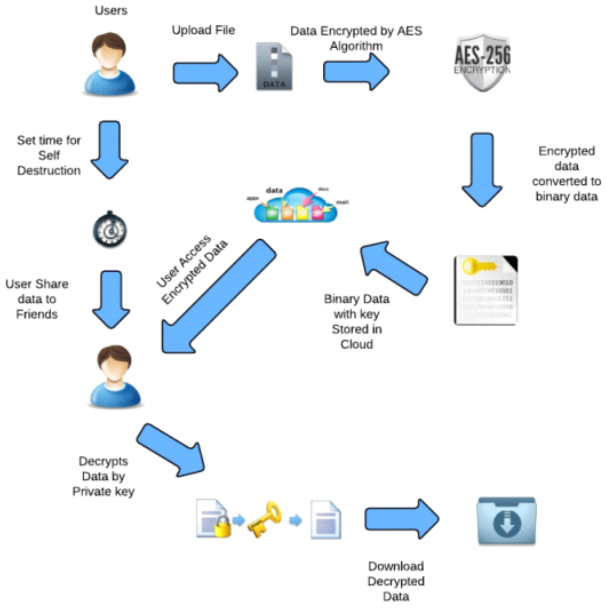

Fig 1. System Architecture

2.2Advantages of Proposed System

- Security issue will not be there.
- Privacy issues are minimized.
- Reducing the space required to store data in cloud.

3. MODULE DESCRIPTION

3.1 Modules

- Authentication and Authorization
- File Encryption and Data storing to Cloud.
- File Sharing
- File Decryption and Download
- Self-Destruction of Data

3.2 Authentication and Authorization

In this module the User have to register first, then only he/she has to access the data base. After registration the user can login to the site. The authorization and authentication process facilitates the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The Registration involves in getting the details of the users who wants to use this application.

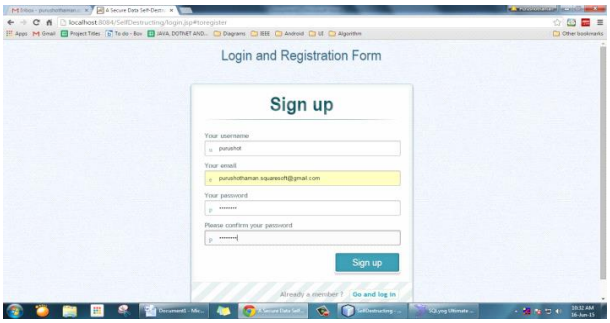

Fig.2 Registration

3.3 File Encryption and Data Storing to Cloud

In this module, User Upload the files which he wants to share. At first the uploaded files are stored in the Local System. Then the user upload the file to the real Cloud Storage (In this application, we use Dropbox). While uploading to the Cloud the file got encrypted by using AES (Advanced Encryption Standard) Algorithm and generates Private Key. Again the Encrypted Data is converted as Binary Data for Data security and Stored in Cloud.

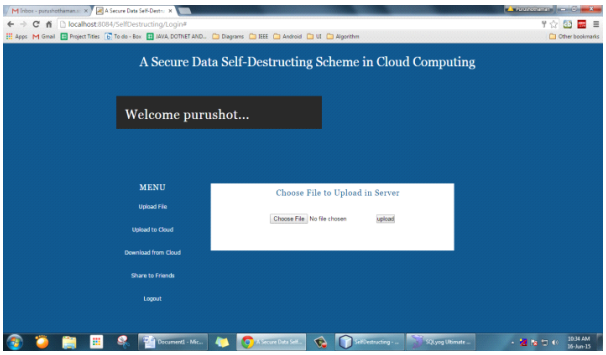

Fig.3 Data storing

3.4 File Sharing

In this module, the uploaded files are shared to the friends or users. In this, the Data Owner set the time to expire the data in Cloud. The Private Key of the Shared Data will be send through Email.

Fig.4 File Sharing

3.5 File Decryption and Download from Cloud

In this Module, the user can download the data by decrypting by using AES (Advanced Encryption Standard) Algorithm. The user should give corresponding Private Keys to decrypt the data. The data will be deleted if the user enter the Wrong Private Key for Three times. If the file got deleted then the intimation email will be sent to the Data owner. The Downloaded Data will be stored in Local Drive.

3.6 Self-Destruction of Data

The Data will be automatically deleted if the User does not downloaded the file successfully with in the time given by the data owner. If the user download the data, then the Self Destruction will be disabled. If the File got deleted by self-Destruction scheme, the intimation Email will be sent to Data Owner.

4. CONCLUSION AND FUTURE ENHANCEMENT

1. Conclusion

In this paper, the notion of authorized data deduplication was proposed to protect the data security by including differential privileges of users in the duplicate check. We also presented several new deduplication constructions supporting authorized duplicate check in hybrid cloud architecture, in which the duplicate-check tokens of files are generated by the private cloud server with private keys. Security analysis demonstrates that our schemes are secure in terms ofinsider and outsider attacks specified in the proposed security model. As a proof of concept, we implemented a prototype of our proposed authorized duplicate check scheme and conduct testbed experiments on our prototype. We showed that our authorized duplicate check scheme incurs minimal overhead compared to convergent encryption and network transfer.

2. Future Enhancement

Since this project is all about sharing files to friends perform computer actions the project has been designed keeping in mind the future scopes. What we have aimed and achieved creating is not a product but a tool to a better automotive environment, a tool can be used to shape many things in the future, thus this project will give rise to many future modifications forking in all directions. Some of the near future scopes of this project are as follows.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditingfor shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.
[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.
[3] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, "A full lifecycle privacy protection scheme for sensitive data in cloud computing," Peerto- Peer Networking and Applications. [Online]. Available: http://dx.doi.org/10.1007/s12083-014-0295-x
[4] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.
[5] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.
[6] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," International Journal of Network Security, vol. 16, no. 4, pp. 351–357, 2014.
[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, ser. LNCS, vol. 7371. Springer, 2005, pp. 457–473.

[8] 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. ACM, 2006, pp. 89–98.
[9] A. F. Chan and I. F. Blake, "Scalable, server-passive, useranonymous timed release cryptography," in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504–513.
[10] K. G. Paterson and E. A. Quaglia, "Time-specific encryption," in Security and Cryptography for Networks. Springer, 2010, pp. 1–16.
[11] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Large universe decentralized key-policy attribute-based encryption," Security and Communication Networks, 2014. [Online].
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy. IEEE, 2007, pp. 321– 334.

