Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

A Secure Data Self-Destructing Scheme in Cloud Computing

Lakshmi Kalvarayan
[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*

Abstract— With the quick growth of versatile cloud services, it becomes increasingly vulnerable to employ cloud services to split data in a friend circle in the cloud computing surroundings. Since it is not possible to perform full lifecycle solitude security, access control becomes a challenging task, particularly when we share receptive data on cloud servers. The KP-TSABE system is proving to be protected under the conclusion l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) supposition. Inclusive comparisons of the safety properties indicate that the KP-TSABE system proposed by us satisfies the protection requirements and is superior to other existing schemes.

Keywords— Security; Time-Specific Encryption

1. Introduction

As the ownership of the data is divided from the administration of them.To upload the file content in data possessor, when download file from client accessibility of files, there are a series of cryptographic systems which goes permiting a third-party auditor to ensure the accessibility of files on behalf of the data possessor without escaping anything about the data or without compromising the data owners obscurity. The crisis will happen when a file is shared to manifold users. One of the methods to the evils is to store data as an ordinary encrypted form. The drawback of encrypting data is that the client cannot share his/her encrypted data at a fine-grained level.When a data holder requirements to split someone his/her information, the owner must identify precisely the one he/she needs to split with the data owner needs to share data with several users according to the protection policy based on the users permits. The possessor has the right to state that convinced sensitive data is only suitable for a imperfect period of time. Timed-release encryption (TRE) provides an interesting encryption service where an encryption key is connected with a predefined discharge time and a recipient can only build the analogous decryption key in this time instance.

2. Existing System

Sharing data between users is possibly one of the most appealing features that inspires cloud storage. concerning accessibility of files there are a series of cryptographic systems which go as far as permitting a third-party auditor to ensure the accessibility of files on behalf of the data possessor without dripping anything about the data owner's obscurity. The dilemma will happen when a file is shared to manifold users.

3. Proposed System

In proposed a key-policy attribute-based encryption based time-specified attributes (KP-TSABE) a protected data self-destructing system in cloud computing. In the KP-TSABE system each ciphertext is labeled with a time while private key is linked with a time immediate.

Advantages of Proposed System

- Security problem will not be there.
- isolation problems are minimized.
- Reducing the space requisite to amass data in cloud.

4. Related Works

4.1 Attribute based encryption

Attribute-based encryption is one of the significant apps of identity-based encryption . ABE approaches in two aromas called KP-ABE and CP-ABE.

4.2 Secure Self-Destruction Scheme

A data self- destructing system, first planned by is a talented approach which designs a Vanish system allows clients to manage over the lifecycle of the responsive data to enhanced the Vanish structure and planned a protected self-destructing system for electronic data.

4.3 Time-Specific Encryption

The time-specific encryption system was initiated as an addition of TRE . In TRE a piece of secluded data can be encrypted in such a method that it cannot be decrypted until the instance called the release-time that was particular by the encryptor. They do not believe the responsive data privacy after finishing.

5. Concept

5.1 Authorization Period

It is the time distance predefined by a data possessor initial from the preferred discharge time and ending at the finishing time. The ciphertext is connected with this hiatus, the user can

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

build the decryption key only when the time moment is within this distance.

5.2 Expiration time

It is a threshold time instantaneous predefined by the proprietor. The shared data can only be accessed by the client before this time instant because the shared data will be self-destructed after expiration.

5.3 Full lifecycle

It is a time period from the formation of the shared data, approval period to ending time. It gives full lifecycle privacy defense for shared data in cloud computing.

6. Architecture

The client have to register first then only he/she has to admittance the database. After enroll the client can login to the site. The verification and approval procedure facilitates the scheme to defend itself and besides it defends the whole mechanism from illegal practice. The enrolment engages in getting the details of the clients who needs to employ this app. At first the uploaded files are piled up in the Local System. Then the client uploads the file to the actual Cloud Storage.

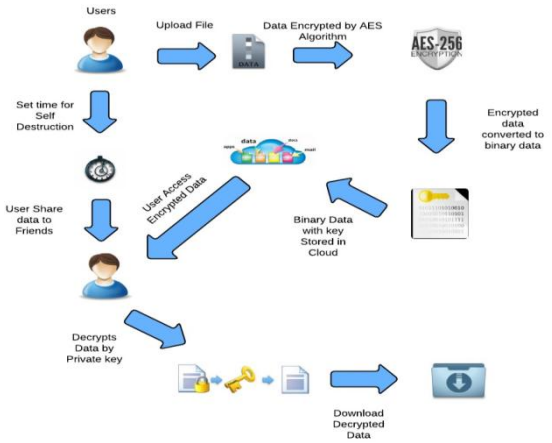

Fig.1: Data sharing architecture

File sharing the uploaded files are collective to the users. The Data possessor set the time to terminate the data in Cloud. The Private Key of the Shared Data will be propel through Email. File decryption and download from cloud the client can download the data decrypting by with AES Algorithm. The client should give corresponding Private Keys to decrypt the information. The information will be erased if the client enters the Wrong Private Key for Three times. If the file obtained erased then the allusion email will be propelled to the Data possessor. The Downloaded Data will be piled up in local Drive. Self devastation of information will be routinely erased if the client does not downloaded the file fruitfully within the time given by the data possessor. If the client downloads the information, then the Self devastations will be disabled. If the File got erased the allusion Email will be propelled to data possessor.

7. Conclusion

In this article, we proposed a novel KP-TSABE scheme which is talented to attain the time precise ciphertext in order to resolve these harms by realizes elastic fine-grained access control during the approval period and time-controllable, self-destruction after ending to the mutual and outsourced information in cloud computing.

References

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions, Vol. 2, no. 1, 2014, pp. 43–56.
[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, 2014, pp. 282–304.
[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 , Vol. 1, No. 2,2013, pp. 142–157.
[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, 2014, pp. 351–357.
[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption", 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", 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", 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 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]. Available: http://dx.doi.org/10.1002/sec.997
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption", Proceedings of the 28th IEEE Symposium on Security and Privacy. IEEE, 2007, pp. 321– 334.
[13] Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456– 465.
[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization", Public Key Cryptography–PKC 2011, pp. 53–70, 2011.
[15] A. Shamir, "How to share a secret", Communications of the ACM, Vol. 22, No. 11, 1979, pp. 612–613.