International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Review Paper On An Efficient Encryption Scheme In Cloud Computing Using ABE

Rutuja G. Kaple
Department of Computer Science and Engineering,
Sipna College of Engineering and Technology,
Amravati, India

Prof. S. B. Rathod
Department of Computer Science and Engineering,
Sipna College of Engineering and Technology,
Amravati, India

ABSTRACT

Security for the data which is stored on the cloud by user is very important issue. User may expect some security for their data from the cloud service provider, there can be serious issues concerning data security between user and service provider. To solve this kind of issues, we can use third party as an auditor. Here we have analyzed different ways to ensure secure data storage in cloud. We are going to provide the security to the user's data by using encryption technique. For this we are using the Advanced Encryption Standard algorithm for encryption and decryption. But when Cloud Service Provider has both encryption and decryption keys, there is threat to security and privacy of data. CSP may pass the user data without user's knowledge. For auditing we are introducing Third Party Auditor. Here the data will be encrypted at user side and will be in encrypted form over network and to TPA. TPA will verify the data before storing it on the cloud. There are large numbers of users of cloud computing who are accessing and modifying the data and they need the reliable service provider who can provide complete security for their data. So the TPA will audit the data and check the data integrity of client's data. Hence user will have more elaborated view over his data privacy.

Keywords: *Cloud Computing, Attribute based encryption, Key policy, ciphertext policy, hierarchical-ABE*

1. Introduction

In the network technology online data allotment has become a new pet, such as MySpace, Facebook .For now, the cloud computing is one of the most able applications platforms to solve the unstable expanding of data sharing along network. Computing technology increase by cloud computing that uses Internet. It consists of the use of computing assets. That are delivered as a service to give access to their data for storing and performing the preferred business operations, hence cloud service provider must provide the trust and security. There is valuable and most sensitive data in vast amount stored on the clouds. There are concerns about scalable, flexible and the fine grained access control in the cloud computing technology. For this intention there have been many of the related schemes that are proposed for purpose of encryption. Such as simple encryption technique that is typically studied. Hence we are going to discuss about Attribute Based Encryption schemes and how this scheme has been developed and also modified further into key policy. The cloud computing technique has rapidly become a very widely adopted standard for delivering services over the internet. Therefore, cloud services provider must provide the trust and security, as there is sensitive and important data in large amount stored on clouds. For protecting the privacy of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. In this paper we going to discuss about attribute based encryption scheme and its categories. Cipher text policy attribute based encryption is one of possible schemes which has much more appropriate and more flexible for general application authority accepts the user enrolment and creates some parameters. By the User

downloads and decrypts the interested cipher text from the cloud server provider. The shared files are usually have hierarchical structure. That's a group of files are divided into a many number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext time and cost of encryption could be saved. So, an access structure could be shared by the two files. Moreover, transport nodes are added in the given access structure, so users can decrypt all authorization files with computation of secret key once. The computation cost of decryption can also be reduced if users need to decrypt numerous files at the same time.

2. Literature Review

Atenieseet *al.*are the first to consider public auditability in their defined "provable data possession" model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA-based homomorphic authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocolis not provably privacy preserving, and thus may leak user data information to the auditor. Juelset *al.*describe a "proof of retrievability" (PoR) model, where spot-checking and error correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is a fixed priori, and public auditability is not supported in their main scheme. Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE.[3] Latterly, a variant of ABE named CP-ABE was proposed. Wan *et al.* proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A ciphertext policy hierarchical ABE scheme with short ciphertext is also studied in . In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority centeris lightened. At present, there are three types of access structures AND gate, access tree, and linear secret sharing scheme (LSSS) used in existing CP-ABE schemes. Cheung and Newport first used AND gate access structure to achieve CP-ABE scheme. Later, some improved schemes are proposed. Meanwhile, there are CP-ABE schemes based on access tree that support AND, OR, and threshold, and based on LSSS where and are the typical schemes of access tree and LSSS. Other CP-ABE schemes with specific features have been presented. For example, Hur proposed a data sharing scheme to solve the problem of key escrow by using an escrow free key issuing protocol between the key generation center and the data storing center. Green *et al.* and Lai *et al* .proposed CP-ABE schemes with outsourced decryption to reduce the workload of the decryption user. And Fan *et al* .proposed an arbitrary-state ABE scheme to solve the problem of the dynamic membership management. In addition, Guo*et al.* [15] proposed a novel constant-size decryption key CP-ABE scheme for storage-constrained devices. Shah *et al.* propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and the server's possession of apreviously committed decryption key. This scheme only works for encrypted files, and it suffers from the auditor state fulness and bounded usage, which may potentially bring in on-line burden to users when the keyed hashes are used up. In other related work, Ateniese *et al.* propose a partially dynamic version of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits.

3. Design Goal

For find out ranked search for effective operation of outsourced cloud data under the mentioned model, our system design should simultaneously realize security and performance guarantees as follows.

1. Efficiency : This also perform privacy should be achieved with low communication and computation overhead.

2. Multi – keyword Ranked Search : To implements search schemes which access multi – keyword query and provide result comparison ranking for effective data retrieval.

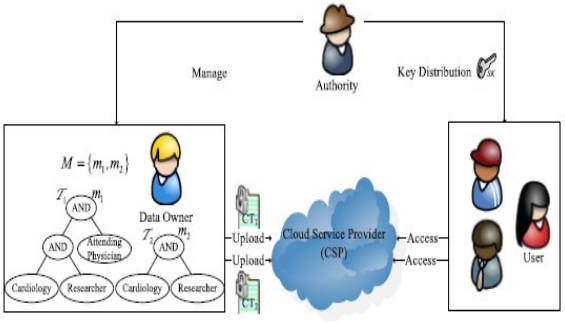

Fig.1: An example of secure data sharing in cloud computing.

4. Proposed Work

Now days there is increase in documents day by day and performing encryption and decryption will take time to execute so to eliminate the this we are proposing an third server based attribute based encryption scheme in cloud computing in which we are going to handle the secure sharing . In cloud storage due to highly encryption and decryption technique it is become very typical which will bear the responsibility of encryption and decryption so that the load on main server will gets down and helps to retrieve the data effectively. In proposed the auditing get applied with various file structures like integrity which will help the file encryption time more effective and security is get improved.

5. Conclusion

A system for efficient encryption scheme is implemented. In implemented system data storage security in Cloud Computing is an emerging computing paradigm, allows users to share information. Cloud storage is much more beneficial and advantageous than the earlier traditional storage systems especially in scalability, cost reduction, portability and functionality requirements. Cloud Computing is an area full of challenges and of paramount importance and many research problems are yet to be identified. System uses encryption/decryption keys. of uses data and stores it on cloud server. Each storage server has an encrypted file system which encrypts the clients data and store. The system ensures that the user data is stored only on trusted storage servers and it cannot be accessed by intruders. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud.

REFERENCES

1) Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou,Senior Member, IEEE, ”Privacy- Preserving Public Auditing for Secure Cloud Storage” IEEE Transactions on Computers, vol. 62,no. 2, February 2013.R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982.

2) CloudSecurityAlliance,“TopThreatstoCloudComputing,”http://www.cloudsecurityalliance.org, 2010

3) G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, ”Provable Data Possession at UntrustedStores,” Proc.14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

4) A. Juels and J. Burton, S. Kaliski, ”PORs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Comm.Security (CCS’07), pp. 584-597, Oct. 2007.008.

5) M.A. Shah, R. Swaminathan, and M. Baker, ”Privacy- Preserving Audit and Extraction of Digital Contents,” Cryptology ePrintArchive, Report 2008.

6) H. Shacham and B. Waters, ”Compact Proofs of Retrievability,” Proc. Int’l Conf. Theory and Application of Cryptology andInformation Security: Advances), in Cryptology (Asiacrypt vol. 5350, pp. 90-107, Dec. 2008.

7) A. Juels and B. S. KaliskiJr, “PORs: Proofs of Retrievability for Large Files,” in Proceedings of the 14th ACM Conference of Computer and Communications Security, pp. 584–597, 2007.

8) A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advancesin Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

9) V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryptionfor fine-grained access control of encrypted data,” in *Proc. 13th ACM Conf. Comput. Commun.Secur.*, Oct. 2006, pp. 89–98.

10) W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, “Efficient attribute-basedencryption from R-LWE,” *Chin. J. Electron.*, vol. 23, no. 4, pp. 778–782,Oct. 2014.

11) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp.Secur. Privacy*, May 2007,pp. 321–334.

12) L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in *Proc. 14th ACM Conf. Comput. Commun .Secur.*, Oct. 2007,pp. 456–465.

13) L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application," in *Proc.10th Int. Workshop Inf. Secur. Appl.*, Aug. 2009, pp. 309–323.

14) X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policyattribute-based access control towards revocation in cloud computing,"*J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

15) F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan,"CP-ABE with constant-size keys for lightweight devices," *IEEE Trans.Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.1276 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016