International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Implementation of an Efficient Encryption Scheme in Cloud Computing using ABE

Rutuja G. Kaple[1], Dr. S. S. Dhande[2], Prof. S. B. Rathod[3]

[1]Department of computer science and engineering, Sipna COET, Maharashtra, India
[2,3] Professor, Department of computer science and engineering, Sipna COET, Maharashtra, India

---

Abstract – *Cloud Computing is developing and considered next generation architecture for computing. Typically cloud computing is a arrangement of computing recourses available via internet. Historically the client or organisations store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. However in cloud computing, since the data is stored wherever across the globe, the client organizations have less control over the stored data. To build the trust for the development of cloud computing the cloud providers must protect the user data from unauthorised access . One technique could be encrypting the data on client side before storing it in cloud storage, however this technique has too much load from client point of view in terms of key management, continuance point of view etc. A trusted third party cloud supplier be used to provide security services, while other cloud provider would be data storage provider. The trusted third party security service provider would not store any data at its closing stages, and its only restricted to given that security service. While the user downloads the data from Storage Cloud, it is decrypted first which is then compared with original data stored in Security Cloud. lastly, this software/application provides the user with the ability to store the encrypted data in Storage cloud and encryption/decryption keys in security cloud service, Other advantage of delegating dependability to trusted third party is that it reliefs the client from any kind of key organization. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.*

Keywords*:* Cloud computing, data sharing, ciphertext-policy, attribute-based encryption.

1. INTRODUCTION

Cloud computing, as an promising computing paradigm, enables users to remotely store their data in a cloud, so as to enjoy services on demand. Cloud computing is one of the most trusted application platforms to solve the volatile expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Mostly for small and medium-sized enterprises with restricted budgets, they can achieve cost savings and the elasticity to scale savings on-demand, by using cloud-based services to manage projects, contacts and schedules, and the like. Access control is principal as it is the first line of defense that prevents unauthorized access to the shared data. Newly, attribute-based encryption (ABE) has been attracted much more attentions since it can keep data privacy and understand fine-grained, one-to-many, and non interactive access control. Ciphertext -policy attribute based encryption is one of possible technique which has much more flexibility and is more suitable for general applications. In cloud computing, as illustrated in authority accepts the user enrollment and creates some parameters. Cloud service provider is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. Cloud gives number of advantages like better reliability, flexibility and security user do not have to keep the data as it is maintained by the cloud service provider, pay only that they used, portability user can access his data from everywhere with the help of internet and they do not need to transmit the physical data storage devices, enabling suitable, on-demand network access. Though these benefits make cloud storage a very economical option for storing data it has some drawbacks like the data loss incidents may take place. There are lots of inner and outer threats, for the payback of their ownership, CSP to behave disloyally like data loss occurrence may be kept secret from client to maintain position, and there may be viruses in the network path or in the software [1]. Security and privacy issues of cloud storage are verification, correctness of data, availability, data leakage, data loss. So, it requires an auditing service to check the reliability of outsourced data. As clients have limited capacity and they are only able to upload and download data from cloud storage. User downloads all data in order to check integrity of stored data. It is very costly and tedious task, particularly when the user is set with a low calculation device (e.g. smart phone) or is not for all time related to the Internet. Therefore, it is necessary to offer an efficient audit service to check the availability and integrity of the stored data. In the proposed system a Third Party Auditor (TPA) is introduced who will verify the data integrity of the client's data stored on cloud storage. TPA audit data when user needed. TPA has more prospective than user and advantageous for cloud provider too because audit result from TPA gives more values for Cloud base service platform and also they fulfill the cloud computing concerns [2]. Finally, this software/application provides the user with the ability to store the encrypted data in storage cloud and encryption/decryption keys in security cloud service, and no single cloud service contributor has access to both. Other benefit of delegating responsibility to trusted third party is that it reliefs the client from any kind of key administration or over head is maintainance of any key information related to data on it device, because it allows the client to use any browser enabled devices to access such service.

2. LITERATURE SURVEY

Ateniese et al.[3] has first considered Public auditability in their model for demonstrable data control for ensuring the storage accuracy of the data files on the servers. They permit a client that has stored data at an untrusted server to check that the server possesses the original data without retrieving it. They had proposed the schemes is based on community audit ability. It generates proof for possession by randomly sample the blocks of data files, but this way the linear combination of the blocks may expose the data to the third party auditor. So their protocol was not fully privacy preserving. Juels et al. [4]. In this scheme, before archiving the data file F in the cloud storage, the verifier pre-computes the cryptographic stores this hash as well as the secret key

Shacham and Waters [6] system to improve a proof-of retrievability in compact proof of retriev ability should be possible to get the client's data from any checker that passes a verification check. The proof of retrievability schemes with full proofs of security has been presented by Juels and Kaliski [4]. Their scheme does not support public auditability and the user can perform fixed number of audit challenges. Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example,Wang *et al.* proposed a hierarchical ABE scheme by combining the hierarchical IBE [and CP-ABE. 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. 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 organization management. In addition, Guo *et al.* proposed a novel constant-size decryption key CP-ABE scheme for storage-constrained devices. A ciphertext policy hierarchical ABE scheme with short ciphertext is also studied. Other CP-ABE schemes with detailed features have been presented. For example, Hur proposed a data sharing scheme to explain the problem of key escrow by using an escrow free key issuing protocol between the key production center and the data storing center. Hohenberger and Waters proposed an online/offline ABE scheme to get better the speed of key generation and encryption, where each computation work in the two processes is divided into two phases: offline phase and online phase.

3. SYSTEM DESIGN

The system provide hash, access list, encryption/decryption by a trusted third party over the network in the form of software as a service .The data storage for each client is done in database . The trusted third party which provides these security services does not store any data at its ends, and stores only master key for each client for data encryption and decryption, and hash of the data which is intended on client side. To get better the security, the communication between client and security server is secured using key, which is used as a input for AES. This partition of dependability has big effect, as no single supplier has access to other data and security key, hash at the same time. Figure shows the system architecture.

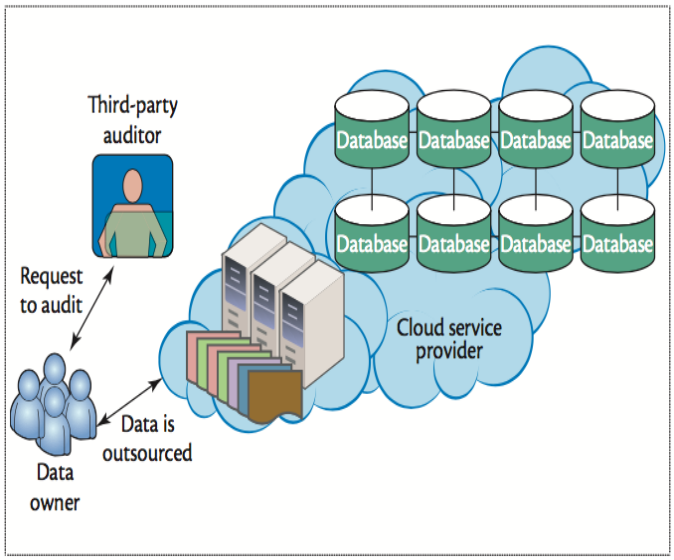

Fig 1 : System architecture.

Samples are taken from the data and it is established for integrity of data. In dynamic auditing, auditing is done on dynamic data. The dynamic data operations are alteration, insertion and deletion. Batch auditing is necessary when there is multiple owner and multiple cloud servers.

4. IMPLIMENTATION:

Implementation involves rotating the theoretical design

into a practical system. Hence it is careful as an important stage for success of project. Concepts in the design phase are interpreted to produce a functioning model. The implementation stage constitutes proper planning, thorough analysis of the existing system and it's constraints on implementation, designing of methods to get the necessary output. As shown in figure 2, TPA will be an intermediate between user and CSP.

A. Data Storage Service System

In this module, we considered four entities to store the data in secure manner:

- Data owner (DO)

Data owner has sample of data to be stored on the cloud and can access it when needed.

- Cloud service provider (CSP)

CSP has enough memory storage space that he provides to store data owner's data. CSP also have computation resources and applications that control data.

- Third party auditor (TPA)

TPA has capability to manage or outsourced data under the delegation of data owner.

B. Third Party Audit Service System

In this module, Third Party Auditor is occupied after the user uploads the file. The file uploaded to cloud comes to TPA , where it verifies the file and forward it to the cloud where it is uploaded on user storage space. TPA also generates the upload alerts and update alerts for user files.

For preserving the data integrity and security, we provide the reliability property and zero-knowledge property of confirmation systems. Due to these properties we can ensure that our system not only prevents falsification of cloud service providers but also reduce chances of data leakage during verification.

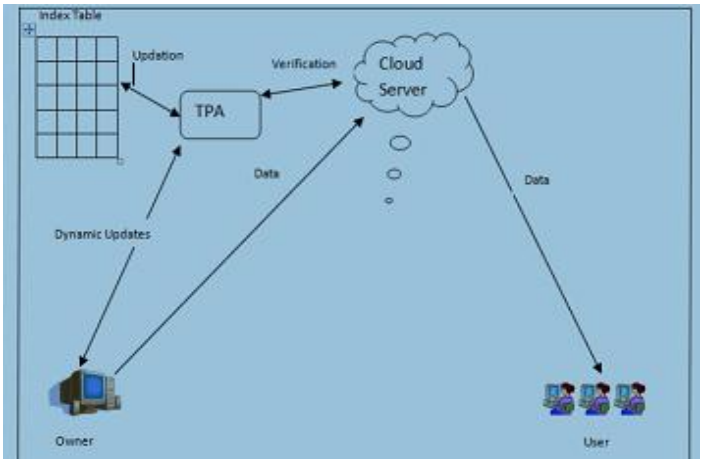

Fig 2 : Role of TPA.

ADVANTAGES:

- As we are using third party authority application our system is more efficient than existing system
- Attribute based encryption scheme in cloud computing is efficient system for storage of data.
- This encryption scheme will help to improve the security clauses in existing cloud system.
- System becomes more applicable.

5. CONCLUSION

We addressed the construction of an efficient audit service for data integrity in clouds. We proposed an interactive audit protocol to implement the audit service based on a third party auditor. In this module, the third party auditor acts as an agent of data owners. The Third party auditor performs periodic verification to monitor the data transfer by providing an optimized schedule. As the auditor doesn't demand local copy of data and it's in encrypted form hence it does not transport any new vulnerability towards data privacy and integrity. We only require to maintain the security over the third party auditor to make sure the privacy and security issues. Hence, our conception can be easily adopted in a cloud computing. This approach minimizes the workload of the cloud service providers, while it still tends to effectively identify misbehavior of cloud service providers with a high possibility.

6. FUTURE SCOPE

The proposed system will expanded and can be tested with the various platforms which will help them to perform data integrity modulation, the security level will improved with dual encryption mode.

References:

[1] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, 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]CloudSecurity Alliance, "Top Threats to Cloud Computing," 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 Untrusted Stores," 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 ePrint Archive, Report 2008.

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

[7] R.Ushadevi, V. Rajamani, "A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism", International Journal of Computer Applications (0975 – 8887) Volume 58– No.22, November 2012.

[8] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST Vol. 2, Iss ue 2, June 2011

[9] Tharam Dillon, Chen Wu and Elizabeth Chang. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[10] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[11] R. C.Merkle, "Protocols for public key cryptosystems," in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.

[12] Sahai and Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.