Reliability of Dynamic Data Storage in Cloud Computing

Kotha Mahesh[1], Avvaru Padmaja[2], Kumara Swamy[3], Mastan Vali[4]

[1]*Assistant Professor, CSE Department, Tirumala Engineering College, Hyderabad*
[2]*Assistant Professor, CSE Dept, Sree Dattha Institute of Engineering and Science*, *Hyderabad*
[3]*Assistant Professor, CSE Dept, Sree Dattha Institute of Engineering and Science*, *Hyderabad*
[4]*Assistant Professor, Dept of IT*, *J.B Institute of Engineering and Technology, Hyderabad*

Abstract: **Cloud Computing reducing the cost issues of organizations in terms of service providing. Reliable data storages is a big issue in cloud computing systems as organizations producing large volumes of data. Cloud Service Providers (CSP) is performing well in this regard by remote environment. Still reliability and security is an open problem by CSP in terms of false accusation. In this paper we attempted deal with the mentioned issues by using a good cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. This may gives reliable dynamic data storage in cloud computing.**

Keywords: **CSP, dynamic environment, mutual trust, Outsourcing data storage.**

1. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Over the last few years, cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its users and providers.

According to U.S National Institute of Standards and Technology (NIST), ―Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels.

2. RELATED WORK

The main objective of this project is constructing a secure data storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is providing the security on storage data on cloud and this data can access only owner of a cloud not another one person. Cloud storage could be a model of networked on-line storage wherever information is hold on in virtualized pools of storage that are usually hosted by third parties. Organizations cite information confidentiality as their serious concern for cloud computing, with encrypted information hold on third party as cloud system, the practicality of the storage system is restricted once general coding schemes are used for information confidentiality. In existing system normal encryption and decryption technique is used to encrypt and decrypt the data in cloud storage system. Data robustness is a major requirement for storage systems. Storing data in a third party's cloud system causes serious concern on data confidentiality. In order to provide security and to achieve the assurances of cloud data integrity and to enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed.

We worked on these issues with the help of a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. We used the concepts of the following

- This model allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append.
- This model ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data
- This model enables indirect mutual trust between the owner and the CSP
- This model allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

3. PROPOSED MODEL

We concentrate on the limitations of existed works as the user has to do most computation and the communication traffic between the user and storage devices is high. The user has to manage his cryptographic keys. If the user's device of storing the keys is lost or compromised, the security is broken. It is hard for storage servers to directly forward a user's messages to another one. The owner of the message has to retrieve, decode, decrypt and then forward them to another user.

In proposed system, the cloud storage systems, we propose a brand new threshold proxy re-encryption theme to create a secure distributed storage system. This distributed storage system conjointly lets a user forward his information within the storage servers to a different user while not retrieving the information back The distributed storage system not solely supports secure and strong data storage and retrieval, however conjointly lets a user forward his information within the storage servers to a different user while not retrieving the data back. The most technical contribution is that the proxy re-encryption theme supports cryptography operations over encrypted messages yet as forwarding operations over encoded and encrypted messages.

SCOPE

The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. More flexible adjustment between the number of storage servers and robustness. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure.

4. SYSTEM ARCHITECTURE

Data storage security on un-trusted remote servers:

Commonly, traditional access control techniques assume the existence of the data owner and the storage servers in the same trust domain. This assumption, however, no longer holds when the data is outsourced to a remote CSP, which takes the full charge of the outsourced data management, and resides outside the trust domain of the data owner. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. This general solution has been widely incorporated into existing schemes, which aim at providing data storage security on untrusted remote servers. Kallahalla et al.designed a cryptography-based file system called Plutus for secure sharing of data on untrusted servers. Some authorized users of the data have the privilege to read and write, while others can only read the data.

Goh et al. [9] have presented SiRiUS, which is designed to be layered over existing file systems such as NFS (network file system) to provide end-to-end security. To enforce access control in SiRiUS, each data file (d-file) is attached with a metadata file (md-file) that contains an encrypted key block for each authorized user with some access rights (read or write). More specifically, the md-file represents the d-file's access control list (ACL). The d-file is encrypted using a file encryption key (FEK), and each entry in the ACL contains an encrypted version of the FEK under the public key of one authorized user.

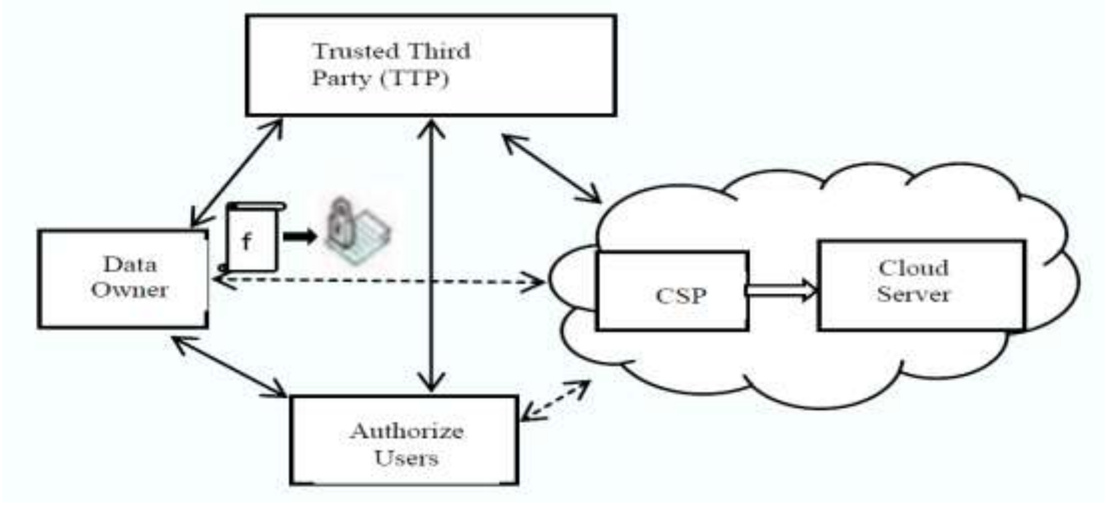

Fig.1. System Architecture

Based on proxy re-encryption [15], Ateniese et al. [10] have introduced a secure distributed storage protocol. In their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. The data owner keeps a master private key to decrypt the symmetric data keys. Using the master private key and the authorized user's public key, the owner generates proxy re-encryption keys. A semi-trusted server then uses the proxy re-encryption keys to translate a ciphertext into a form that can be decrypted by a specific granted user, and thus enforces access control of the data.

Vimercati et al. [11] have constructed a scheme for securing data on semi-trusted storage servers based on key derivation methods of [16]. In their scheme, a secret key is assigned to each authorized user, and data blocks are grouped based on users that can access these blocks. One key is used to encrypt all blocks in the same group. Moreover, the data owner generates public tokens to be used along with the user's secret key to derive decryption keys of specific blocks. The blocks and the tokens are sent to remote servers, which are not able to drive the decryption key of any block using just the public tokens. The approach allows the servers to conduct a second level of encryption (over-encryption) to enforce access control of the data. Repeated access grant and revocation may lead to a complicated hierarchy structure for key management [17].

Cloud computing data storage system model

The cloud computing storage model considered in this work consists of four main components as illustrated in Figure 1. The relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the CSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relationship between the data owner and the authorized users.

For confidentiality, the owner encrypts the data before sending to cloud servers. To access the data, the authorized user sends a data-access request to the CSP, and receives the data file in an encrypted form that can be decrypted using a secret key generated by the authorized user. It is assumed that the interaction between the owner and the authorized users to authenticate their identities has already been completed, and it is not considered in this work. The TTP is an independent entity, and thus has no incentive to collude with any party. However, any possible leakage of data towards the TTP must be prevented to keep the outsourced data private. The TTP and the CSP are always online, while the owner is intermittently online. The authorized users are able to access the data file from the CSP even when the owner is offline.

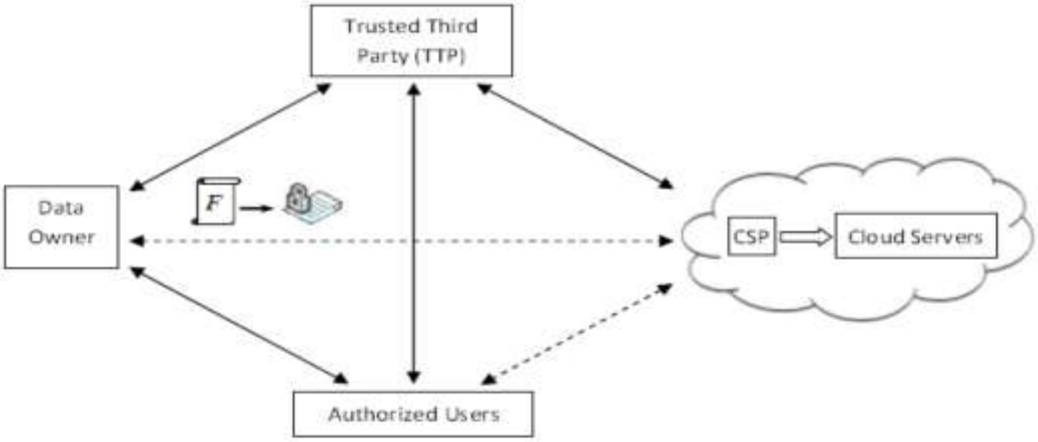

Fig.2. Cloud computing data storage system model

5. CONCLUSION

The cloud based storage scheme is proposed that allows owner to benefit from facilities offered by the CSP and enables indirect mutual trust between them. It enables data owners to release their concerns regarding confidentiality, integrity, access control of the outsourced data. To resolve disputes that may occur regarding data integrity, a trusted third party is invoked to determine the dishonest party (owner/users or CSP). In this paper, we have attempted a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data.

We have investigated the overheads added by our scheme when incorporated into a cloud storage model for static data with only confidentiality requirement. The storage overhead is ≈ 0.4% of the outsourced data size, the communication overhead due to block-level dynamic changes on the data is ≈ 1% of the block size, and the communication overhead due to retrieving the data is ≈ 0.2% of the outsourced data size. For a large organization with 105 users, performing dynamic operations and enforcing access control add about 63 milliseconds of overhead. Therefore, important features of outsourcing data storage can be supported without excessive overheads in storage, communication, and computation.

6. REFERENCES

[1]G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song," Provable data possession at untrusted stores" in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[2] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[3] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[5] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," Cryptology ePrint Archive, Report 2008/073, 2008, http:// eprint.iacr.org/.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International

Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[8] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[9] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing,"

BIBLIOGRAPHY

Mr. Kotha Mahesh, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. His research interest includes Data Mining, Big Data, Pure Mining & Cloud Computing. Now he is working as an Assistant Professor in CSE Dept, Tirumala Engineering College, Hyderabad.

Ms.Avvaru Padmaja, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining, Network Security & Cloud Computing. Now she is working as an Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.

Mr. Kumara Swamy, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. His research interest includes Cloud Computing, Data Mining & Network Security. Now he is working as an Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science**,** Hyderabad.

Mr. Mastan Vali, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. His research interest includes Computer Networks & Security, Cloud Computing and Data Mining. Now he is working as an Assistant Professor in Dept of IT, J.B Institute of Engineering and Technology, Hyderabad.