International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 30th December 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-13

Title: Privacy Preserving Ranked Multi Keyword Exploration For Multiple Data Owners In Cloud Data.

Volume 06, Issue 13, Page No: 270 - 274.

Paper Authors

*** PASUPULETI L S KOTESWARI, G RAVI TEJA.**

* Dept of CSE, St.Mary's Women's Engineering College.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PRIVACY PRESERVING RANKED MULTI KEYWORD EXPLORATION FOR MULTIPLE DATA OWNERS IN CLOUD DATA

***PASUPULETI L S KOTESWARI, **G RAVI TEJA**
*Scholar, Dept CSE, St.Mary's Women's Engineering College, Budampadu, Guntur
**Assistant Professor, Dept CSE, St.Mary's Women's Engineering College, Budampadu, Guntur

ABSTRACT—
The many organizations are adopting to use outsourcing data to remote cloud service providers (CSP).The CSPsstorage infrastructure can be rented by customers to store and get back unlimited amount of data by paying fees per gigabyte/month. To achieve higher level of scalability, availability the data must be replicate on multiple servers among multiple data centers. If the more copies the CSP is asked to store, the more fees the clients are charged. It is very important to the clients to have strong evidence that they actually get the service they pay for, and all these copies are reliable with the most recent modifications done by the clients. Efficient provable multicopy dynamic data possession (EPMDDP) method being proposed in this paper and includes following features; It provides an proofs to the clients that the CSP not cheat by storing fewer copies, It supports outsourcing of dynamic data, i.e., file level functions such as file alteration, addition, deletion, and append, and finally It allows only authorized users to access the file copies stored by the CSP.

Keywords—Cloud Computing, data duplication, cloud service provider (CSP), data replication, dynamic environment,outsourcing data storage.

I. INTRODUCTION

Cloud Computing is an important computing technology that can be viewed as virtualized pool of computing resources (e.g.: storage, processing power, memory, application, services and network bandwidth). The organizations allowed storing more data on the CSP than on private computer system by using outsourcing data to remote cloud service provider, and also organizations allowed to focus on innovations and relieve the load of constant server updates and other computing matter by using outsourcing of data storage. Data security and integrity protection in cloud computing is a challenging task. Data security can be handled by encrypting sensitive data before outsourcing to remote servers. It is vital demand of customers to have a strong proof that the cloud servers have their data that is not being corrupt with or partially deleted over time. As a result, many researchers have focus on the problem of provable data possession (PDP) and proposed different schemes to review the d ata stored on remote servers. PDP is a technique for ensuring data integrity over remote servers. In this model, do not need to store all file to local computer to check data owner creates some metadata information for each file, at the time of verification of data integrity it sends the metadata to the verifier side. The main design principle of outsourcing data is to provide dynamic behavior of data for any applications. It means stored data not only accessed by the authorized users, but it also scaled and efficient Examples of PDP construction that focus on dynamic data [3] – [7]. It is however for a single copy of the data file. The PDP model focuses for multiple

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

copies of static data [8] – [10]. The PDP system deals with multiple copies of dynamic data. The overall system integrity check fails when we are verifying multiple data copies if there is one or more corrupted copies. To handle this issue, a slight modification has been applied to the proposed scheme.

A. Paper Organization

The remainder of the paper is organized as follow. The related work is explained in session II. The proposed scheme is elaborated in section III. Section IV presents experiment result using DriverHQ cloud platform. Concluding remarks are given in section V.

II. RELATED WORK

Ateniese et al. [2] are the first to consider publicauditability by using "provable data possession" (PDP) model which ensure data files on untrusted storage. This scheme uses the RSA-Algorithm for the purpose of auditing outsourced data. The public auditability in this scheme mainly focus on linear combination of sampled blocks exposed to external auditor. When used directly, this protocol is not prove privacy preserving, and may l eak user data information to the auditor. Robert Di Pietro [3] propose a dynamic operation partially like block modification, deletion and append by using PDP scheme, it uses only symmetric key cryptography but with a bounded number of audits and also it is not suitable for public verifiability. Curtmola et al. [9] propose a multiple replica PDP (MRPDP) which prove that multiple replicas of client's data are stored at the cloud storage server, so that the data availability improved. When some of the existing replicas fail then it can be generate further replicas on demand but there will be little expense. It is not useful as it propose integrity issue. AyadF.Barsoum and M.AnwarHAsan [1] provides a multicopy dynamic data possession. It provides proofs to customer that CSP store all copies that are agreed upon the customers, it supports block level dynamic operation using map version table by data owner and also it allows authorized user to access data. Finally it discuss how to identify corrupted copies.

III. PROPOSED EPMDDP SCHEME

The generation of unique differentiable copies of the data file is the core design of efficient provable multicopy dynamic data possession (EPMDDP) method. Identical copies make the CSP to simply allow the owner by storing only one copy and pretending that it stores multiple copies. Using simple efficient method i.e. The EPMDDP method this ensures that CSP not cheat the customers by storing fewer copies and allowing data owner to update and scale the outsourced file copies to cloud servers which may be untrusted, so the data owner encrypts the file copies before outsourcing to cloud servers. The proposed system consists of main components shown in fig. 1:

1. The data owner may be an organization originally they store data in the cloud.
2. The CSP who maintains the cloud servers (CSs) and it can be paid storage space to store the owner's files.
3. The authorized users the set of data owner's client who have the right to access the remote data
4. verifier may be data owner or authorized user

The storage model used in this work can be used by many applications, like financial, scientific, and educational applications. For example, e-Health applications in that the patients database that may be large and

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

contain sensitive data it can be stored on the cloud servers. In this application e-Health organization can be considered as the data owner, and the physicians as the authorized users they have right to access patient's medical history.

Proposed System achieves the following main objectives:

We propose an Efficient Provable Multicopy Dynamic Data Possession method (EPMDDP). This method makes CSP to not cheat the customers by storing fewer copies, so it provides proofs to the customers. Additionally, the method supports outsourcing of dynamic data, i.e., it supports file level functions such as file alteration, insertion, removal and append. It allows only authorized users to access the data which is stored on the CSP. It allows reconstructing the corrupted copies using existing duplicate file copies. It finds economically motivated CSP based on cost and free space available on cloud by taking some assumption, and We discuss differences between analyses of the proposed method with a reference model.

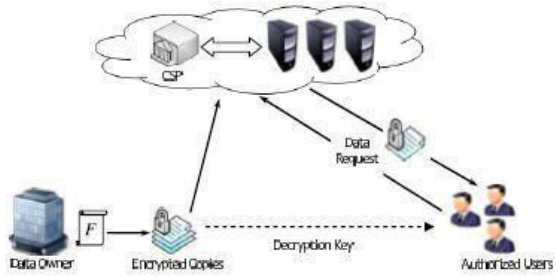

Fig. 1.Cloud computing data storage system model

System will be consisting of Admin Module, and User Module which is formed by using the basis of f unctionalities that are found in the system. Registration: The only registered user to the application can store the file into the cloud storage. Hashing Process: When user uploading the file to cloud, the file will be read in byte stream for generating MD5 key using hashing technique.

File Upload: File is uploaded on the cloud storage by using CSP, when we upload file ultimately the CSP store all copies of file which is agreed on service.

View files: File content can be seen in original format by data owner and authorized user.

File Modify: File can be modified only by data owner. Modification can be inserting, appending, editing.

File Deletion: The only data owner c can have right to delete the uploaded file.

File Download: The only verified files can be downloaded by the data owner or authorized users.

File Storage: The file can be stored in the cloud is an encrypted format using encryption algorithm.

Verifier: It is used to verify the copies of the file that are stored into cloud storage. It frequently checks the integrity of all file copies.

Integrity Verification: The user going to check the integrity process. The hash code is generated for each file uploading and downloading. The web server storage compares both hash code for integrity process. If both are identical then file is not modified.

III. EXPECTED RESULTS

We compare both two schemes i.e. reference model is TBPMDDP and with the proposed method i.e. EPMDDP from different perspectives: proofs computation times, verification times, and cost of dynamic operations. It has been reported that if the remote sever is missing a fraction of the data, then the number of blocks that needs to be checked to detect server misbehaviour with

high probability. As still work is progressing on to show expected results.

CONCLUSION

The management of huge amount of data at local remote servers is problematic and costly. Therefore, Cloud Service Providers offers storage-as-a-service as a paid facility to reduce cost and relieves the burden of constant server updates and other computing issues. The proposed new PDP scheme (called as EPMDDP) which supports outsourcing multicopy dynamic data, where the data owner is not only accessing data copies stored by the CSP, but also updating with recent modification to all copies of files that are on the remote servers. The scheme allows the verifier to verify the data integrity, and also it provides proofs to the customers they are storing all data copies that are agreed upon in the service contract. From performance analysis and experiment results, we have build that the EPMDDP scheme outperforms than the TB-PMDDP schemederived from a class of dynamic single copy PDP model.

REFERENCES

[1] Ayad F. Barsoum and M. Anwar Hasan, " ProvableMulticopy Dynamic Data Possession in Cloud Computing systems", in IEEE Transactions On Information Forensics And Security, Vol 10 No 3 March 2015.

[2] G.Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Commun. Secur. (CCS), New York, NY, USA, 2007. pp. 598-609

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc, 4th Int. Conf. secur. Privacy Commun. Netw. (SecureComm), New York. NY, USA. 2008. Art. ID9.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech. Rep.2009/081 [Online]. available: http://eprint.iacr.org/

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009,pp . 213-222.

[6] Q. Wang, C. Wang, J. Li, K.Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS), Berlin, Germany, 2009, pp. 355-370.

[7] Z.Hao, S. Zhong, and N. Yu. "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans.Knowl. Data Eng., vol 23, no. 9, pp. 1432-1437, Sep. 2011.

[8] A. F. Barsoum and M. A. Hasan. (2010). "Provable possession and replication of data over cloud servers," Centre Appl. Cryptograph. Res., Univ. Waterloo, Waterloo, ON, USA, Tech.Rep.2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2010/ cacr2010-32.pdf

[9] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Proc. 2nd Int. Symp. Data, Privacy, E-Commerce, Sep. 2010, pp. 84–89.

[10] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur., 2008, pp. 90–107.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Ms Pasupuleti L S Kotswari, Scholar, M.Tech, Department of Computer Science & Engineering, St.Mary's Women's Engineering College, Budampadu, Guntur.

Mr G. Ravi Teja, Assistant Professor, Department of Computer Science & Engineering, St.Mary's Women's Engineering College, Budampadu, Guntur.