ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

A Simulation Study of Outsourcing of Audit Service for Data Integrity in Cloud Computing

Anil Kushanpalli[1], V.Santosh Kumar[2], Ch.Ravindranath Yadav[3]

Student, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad, India [1]

Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad, India [2]

Associate Professor, Dept. of H&S, Sreyas Institute of Engineering and Technology, Hyderabad, India[3]

ABSTRACT: Cloud computing technology enables data owners to outsource data and relieve from the burden of maintaining computing resources. This is possible as cloud provides platform independent, location independent, scalable and low-cost storage services. With virtualization technology, the cloud computing is made affordable. However, when data owners do not have physical possession of data, they need rely on security of cloud service providers completely. Integrity of their data is an important concern. Audit services that can ensure data integrity are essential. Many techniques came into existence in the recent past. Recently Zhu et al. presented Provable Data Possession (PDP) based interactive protocol for ensuring integrity of outsourced data. Based on this technique, in this paper we built a prototype application that demonstrates the proof of concept. The proposed application simulates the cloud environment where the audit service is provided for data integrity. The empirical results reveal that the application provides secure access to cloud services and provide data integrity.

Keywords: Security, cloud storage, interactive audit service

I. INTRODUCTION

Cloud computing is an emerging technology that enables people of all walks of life to make use of shared computing resources in pay per use fashion. It does not need any capital investment. Instead users [1] of cloud can simply access the resources as if they are in the local machine. However, the services are not free. The cloud computing provides services such as Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Mining as a Service (MaaS). Out of all these services infrastructure service helps cloud users to outsource data to cloud server. Cloud service provider maintains data centers that can help in making the storage in a scalable fashion. Virtualization is also used in cloud computing in order to make the cloud services affordable. As can be seen in Figure 1, the cloud users can interact with cloud through Internet. They need a PC or any device which is Internet – aware in order to gain access to cloud computing paradigm.

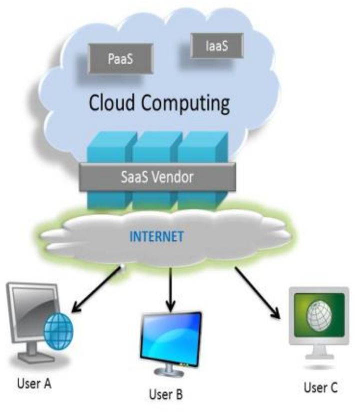


Figure 1 – Cloud computing environment

When data is out sourced to cloud, the data owners should relay on cloud service providers as they do not maintain local copy of data. Since the data is very huge and it is outsourced for the same reason, it is not feasible to maintain a local copy. As cloud server is untrusted, it is essential to have security mechanisms in place to protect the data. In other words, the data owner is worried about the integrity of outsourced data. Many techniques came into existence to protect outsourced data including Provable Data Possession (PDP). Recently in [2] this has been improved and interactive PDP with zero knowledge is built. This scheme is meant for helping data owner to take the help of third party auditor for audit services. It does mean that audit services can verify the integrity of outsourced data so that data owners can feel good as their data is secure.

In this paper, we implement some of the security mechanisms proposed in [2] in order to have secure outsourcing of data. Three parties are involved in the proposed scheme. They are data owner, cloud server and third party verifier. Data owner is responsible to store and retrieve data to/from cloud. He also involves in data dynamics in secure fashion. The cloud service provider is responsible to provide storage services and the security services available. The third party auditor, as the name implies, performs audit operations in order to ensure that the data integrity [3] is not lost. Data owner gives verification information to third party auditor so as to enable him to verify data integrity. The auditor performs audit on outsourced data and provides report to cloud data owner. The remainder of the paper is structured as follows. Section II reviews literature on secure outsourcing of data. Section III provides information about proposed system. Section IV presents the prototype application. Section V presents the experimental results while section VI concludes the paper besides providing directions for future work.

II. RELATED WORK

This section provides review of literature on security provided to outsourced data in cloud computing environment. For cloud computing scenario, the traditional cryptographic techniques do not work for ensuring data integrity. Without having local copy such schemes [4], [5] and [6] do not work and thus cannot provide a practical solution. As the communications become expensive, the traditional approaches can't be applied to outsourced data to cloud.

With traditional cryptographic techniques the public auditability becomes expensive and infeasible. The cloud service providers and cloud users might take the help of a TPA as they can avail expert services of TPA. Many schemes came into existence. They include PDP [7], Proof of Irretrievability [1], and some of the improved forms of these two techniques. These techniques are based on the probabilistic proof techniques. They also work in publicly verifiable way. Thus public auditability came into existence.

In [8] and [9] the researchers focused on the public audit services. These schemes are privacy preserving in nature. Generally they split the outsourced file into n blocks and generate verificationo code for each block. All blocks are kept in equal size with 20 bytes or 160 bits. This kind of concept was explored well in [10]. There are some issues with tags generated for security. They include insufficient auditing. In order to overcome this problem fragment technique was introduced. Dynamic scalability is one of the core design principles of cloud computing. It does mean that users can access data and also perform data dynamics.

III. PROPOSED SYSTEM

The proposed system involves three parties. They are data owner, cloud service provider and third party auditor. Data owner is responsible to store and retrieve data to/from cloud. He also involves in data dynamics in secure fashion. The cloud service provider is responsible to provide storage services and the security services available. The third party auditor, as the name implies, performs audit operations in order to ensure that the data integrity is not lost.

Data owner gives verification information to third party auditor so as to enable him to verify data integrity. The auditor performs audit on outsourced data and provides report to cloud data owner.

For actual scheme for interactive auditing the mechanisms are taken from [1]. Figure 1 illustrates the schematic diagram showing three parties involved in outsourcing data to cloud, retrieving it and providing interactive audit services.

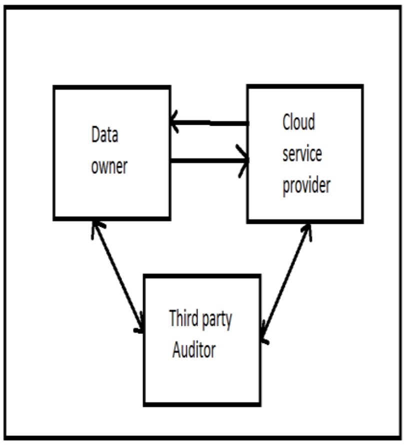


Figure 2 – Schematic overview of the parties involved

As shown in Figure 2, the cloud service providers such as Google, Microsoft, and IBM etc. help in outsourcing data in the real world. However, in this paper we built a custom simulator application that demonstrates the parties' involvement. In the proposed prototype implementation the three parties are named as client, service provider and third party verifier. The flow of activities of each party is presented in Figure 2.

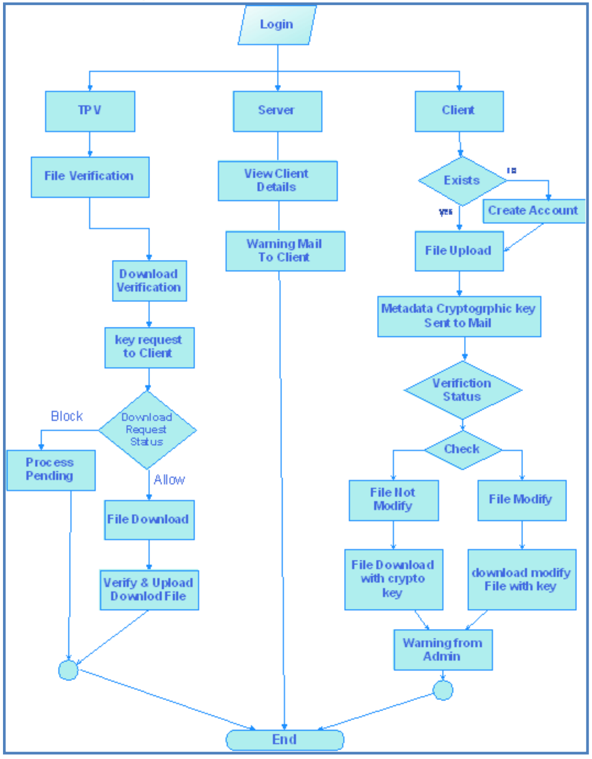
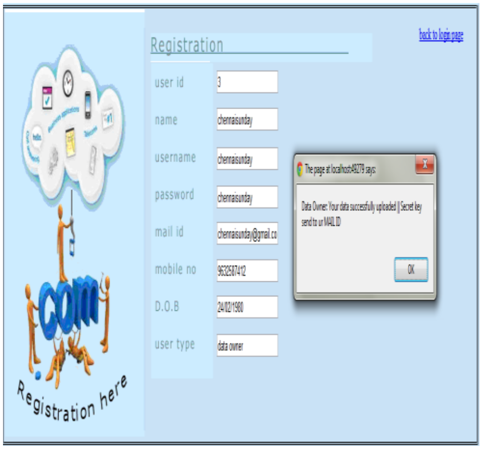


Figure 3 – Flow of activities of all parties

As can be seen in Figure 3, a client can register himself and perform operations like file upload, download file, communication with auditor, getting messages related to verification from auditor. The server part will perform operations like storing given data and providing desired messages from time to time. The third party verifier is responsible to perform the activities like file verification, download verification, key request to client and so on.

IV. PROTOTYPE APPLICATION

We built a prototype application using Visual Studio 2012 in a PC with Windows 7 operating system, 4GB RAM, core 2 dual processor. Microsoft .NET 4.0 is the framework used for application development. The application is built using ASP.NET and C#. The application demonstrates the operations of all the parties involved.



Registration

back to login page

user id: 3
name: chennaisunday
username: chennaisunday
password: chennaisunday
mail id: chennaisunday@gmail.co
mobile no: 9632587412
D.O.B: 24/02/1980
user type: data owner

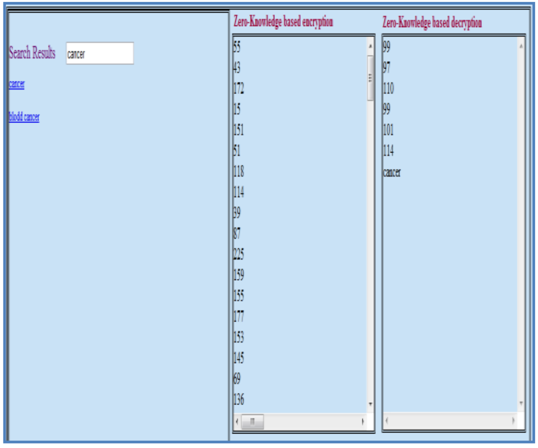
The page at localhost:49279 says:

Data Owner: Your data successfully uploaded || Secret key send to ur MAIL ID

OK

Figure 4 – Registration form

Data owner registers himself in order to have an account with cloud service provider. This account is used by him from time to time to outsource data beside other data dynamics. After registration process, the data owner can perform various operations.



Search Results: cancer

cancer

blodd cancer

Zero-Knowledge based encryption

```
55
43
172
15
151
51
118
114
39
87
225
159
155
177
153
145
69
136
```

Zero-Knowledge based decryption

```
99
97
110
99
101
114
cancer
```

Figure 5– Zero knowledge based encryption and decryption operations

As can be seen in Figure 5, it is evident that there is result for zero knowledge based encryption and decryption for select data. There are other operations involved such as third party verifier taking verification details from client and making efficient audit services so as to ensure data integrity.

V. EXPERIMENTAL RESULTS

Experiments are made with files having different size. Computation and communications costs against given file size with ratios such as 10%, 20%, 30%, 40% and 50% are used. As the ratio and file size decreases computational time and communication cost are reduced.

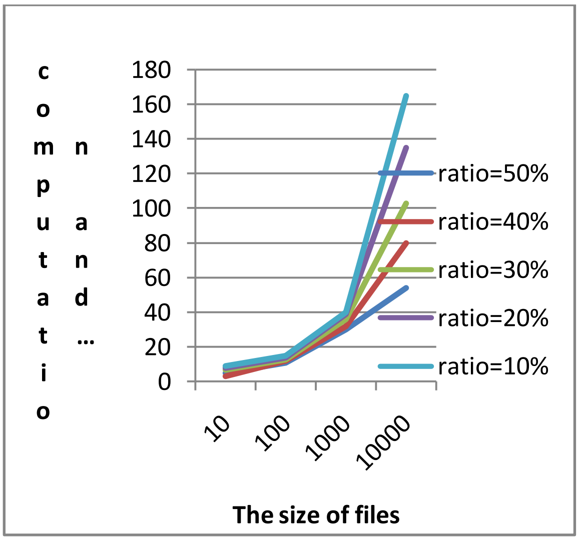


Figure 6 - Experiment results under different file size

As shown in the figure 6 the horizontal axis represents size of files while vertical axis represents computation and communication costs. The results reveal that the file size has its influence on computation and communication costs.

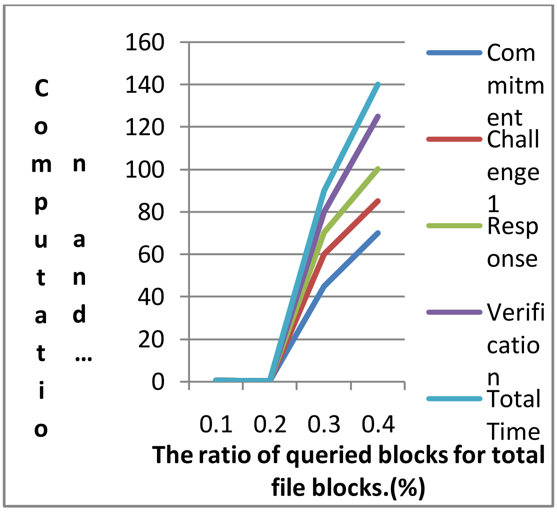


Figure 7 - Experiment results under different file blocks

As shown in the figure 7 the horizontal axis represents size of file blocks while vertical axis represents computation and communication costs. The results reveal that the file block size has its influence on computation and communication costs.

VI. CONCLUSIONS AND RECOMMENDAITONS

In this paper, we study the data integrity of outsourced data. Data owners outsource their data to cloud. Based on the security concepts presented in [2], in this paper we built a prototype application that demonstrates the concept of secure outsourcing of data. The proposed application facilitates three parties to have respective operations. They are data owner, cloud service provider and third party verifier. Data owner is responsible to store and retrieve data to/from cloud. He also involves in data dynamics in secure fashion. The cloud service provider is responsible to provide storage services and the security services available. The third party auditor, as the name implies, performs audit operations in order to ensure that the data integrity is not lost. Data owner gives verification information to third party auditor so as to enable him to verify data integrity. The auditor performs audit on outsourced data and provides report to cloud data owner. The empirical results reveal that the proposed application simulates the proof of concept. Our future work includes working security mechanisms with real cloud.

REFERENCES

[1] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.

[2] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, , Stephen S. Yau, , Ho G. An, and Chang-Jun Hu, Dynamic Audit Services for Outsourced Storages in Clouds, IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 6, NO. 2, APRIL /JUNE 2013, p227-238.

[3] Amazon Web Services, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[4] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758, 2010.

[5] A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.

[6] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of User-Friendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009.

[7] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm.Security, pp. 598-609, 2007.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.

[9] M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp. 782-793, 2007.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology Advances in Cryptology (ASIACRYPT '08), J. Pieprzyk, ed., pp. 90-107, 2008.

BIOGRAPHIES

Anil Kushnapalli is currently working towards his M.Tech degree in Sreyas Institute of Engineering and Technology, Hyderabad, India. His research interests include networking and cloud computing

Vennu Santosh Kumar received the Masters degree in Computer Science and Engineering in the year 2010. He is Microsoft Certified System Engineer & CISCO Certified Network Administrator, he worked as a System Engineer in WIPRO Technologies(INDIA). In 2011 he joined as an Associate Professor at Sreyas Institute of Engineering and Technology in Computer Science Department. He has been involved in several tutorials, workshops, technical paper presentations .His research interests are focused on Computer Networks, Network Security & Mobile Computing.

Chintala Ravindranath Yadav is a perceptive academician, with an M.B.A to his credit, and pursued his Post-masters in Business Administration from University of North Carolina at Greensboro, U.S.A. He worked in leading edge organizations for several years in U.S.