International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

Data Storage Transparent Security in Cloud Computing

K.Divya
M.Tech Scholar -CSE
Sri Indu College of Engg and Tech
Ibrahimpatan, Hyderabad, TS, India

P.Navya Sri
M.Tech Scholar-CSE Dept
Sri Indu College of Engg and Tech
Ibrahimpatan, Hyderabad, TS, India

Tejavath Charan Singh
Assistant Professor, Dept of CSE
Sri Indu College of Engg and Tech
Ibrahimpatan, Hyderabad, TS, India

Abstract: **Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.**

Keywords: **Data integrity, dependable distributed storage, error localization, data dynamics, Cloud Computing**

1. INTRODUCTION

Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge 2 scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don‘t have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon‘s S3 is such an example. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system. Cloud computing infrastructure accelerates and fosters the adoption of innovations Enterprises are increasingly making innovation their highest priority. They realize they need to seek new ideas and unlock new sources of value. Driven by the pressure to cut costs and grow simultaneously they realize that it‘s not possible to succeed simply by doing the same things better. They know they have to do new things that produce better results. Cloud computing enables innovation. It alleviates the need of innovators to find resources to develop, test, and make their innovations available to the user community. Innovators are free to focus on the innovation rather than the logistics of finding and managing resources that enable the innovation.

This paper describes cloud computing, a computing platform for the next generation of the Internet. The paper defines clouds, explains the business benefits of cloud computing, and outlines cloud architecture and its major components. Readers will discover how a business can use cloud computing to foster innovation and reduce IT 5 costs. Introduction Enterprises strive to reduce computing costs. Many start by consolidating their IT operations and later introducing virtualization technologies. Cloud computing takes these steps to a new leveland allows an organization to further reduce costs through improved utilization, reduced administration and infrastructure costs, and faster deployment cycles. The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability.

Existing Project Traditional Cryptographic: From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users‘loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

Existing Project Third Party Data Warehouse: Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

3. ARCHITECTURE

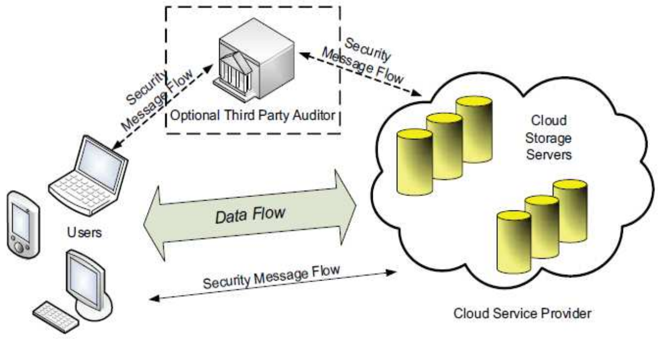


Fig.1.Architecture

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. No user data privacy, Security risks towards the correctness of the data in cloud

We focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.

- In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.

- Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions.

4. MODULES

4.1. System Model

User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

4.2. File Retrieval and Error Recovery

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one. We can guarantee the successful file retrieval with high probability. On the other hand, whenever the data corruption is detected, the comparison of pre-computed tokens and received response values can guarantee the identification of misbehaving server(s).

4.3. Third Party Auditing

As discussed in our architecture, in case the user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing.

4.4. Cloud Operations

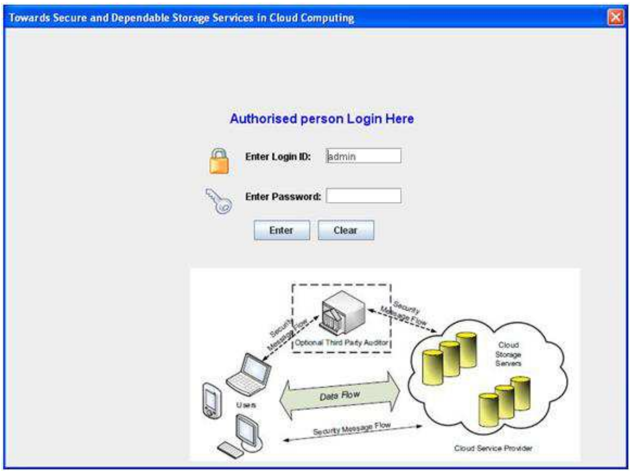
Update Operation: In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, we refer this operation as data update. In other words, for all the unused tokens, the user needs to exclude every occurrence of the old data block and replace it with the new one.

Delete Operation: Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

Append Operation: In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which we refer as data append. We anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

5. OUTPUT SCREENS

5.1. Cloud Server Login



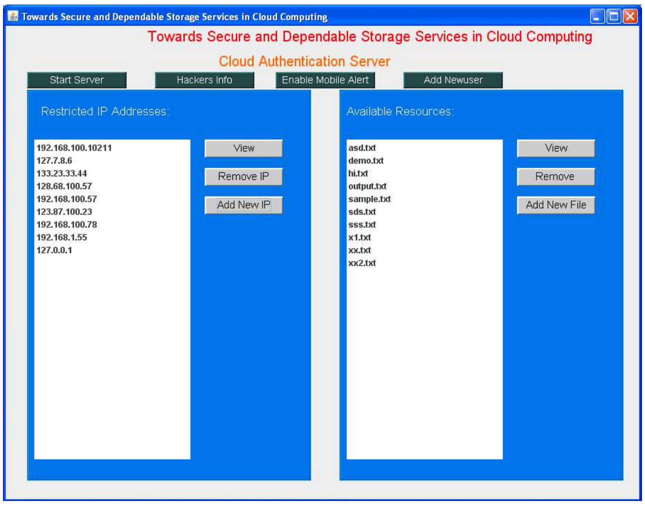
Towards Secure and Dependable Storage Services in Cloud Computing

Authorised person Login Here

Enter Login ID: admin

Enter Password:

Fig.2. SS1:Cloud server login page



Towards Secure and Dependable Storage Services in Cloud Computing

Towards Secure and Dependable Storage Services in Cloud Computing

Cloud Authentication Server

Restricted IP Addresses:

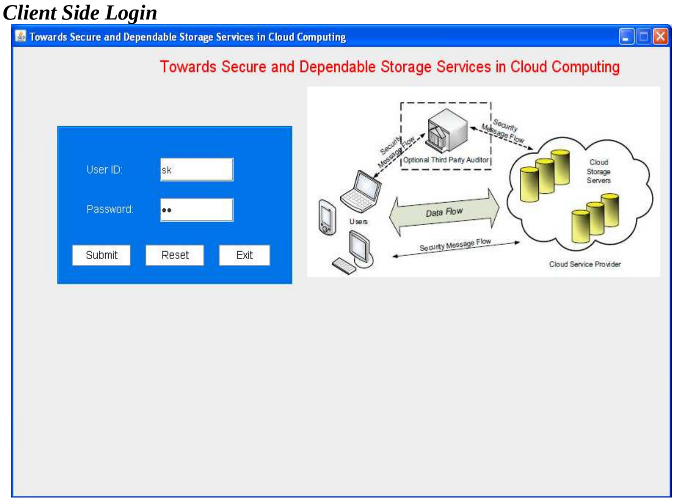
192.168.100.10211
127.7.8.6
133.23.33.44
128.68.100.57
192.168.100.57
123.87.100.23
192.168.100.78
192.168.1.55
127.0.0.1

Available Resources:

asd.txt
demo.txt
hi.txt
output.txt
sample.txt
sds.txt
sss.txt
x1.txt
xx.txt
xx2.txt

Fig.3. SS3 -Available Resources

Client Side Login



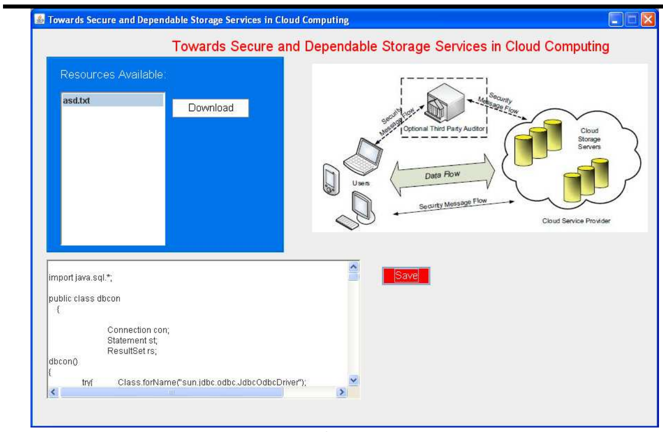
Towards Secure and Dependable Storage Services in Cloud Computing

Towards Secure and Dependable Storage Services in Cloud Computing

User ID: sk

Password: ••

Fig.4. Client side Login



```
import java.sql.*;

public class dbcon
   {

                  Connection con;
                  Statement st;
                  ResultSet rs;
dbcon()
{
          try{        Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
```

Fig.5. SS9 –Downloading Information Available On Resource

6. CONCLUSION

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users‘ data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasurecoded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

REFERENCES

[1]. Amazon.com, ―Amazon Web Services (AWS),‖ Online at http://aws. amazon.com, 2008.

[2]. N. Gohring, ―Amazon‘s S3 down for several hours,‖ Online Athttp://www.pcworld.com/businesscenter/article/142549/amazo s s3 down for several hours.html, 2008.

[3]. A. Juels and J. Burton S. Kaliski, ―PORs: Proofs of Retrievability for Large Files,‖ Proc. of CCS '07, pp. 584–597, 2007.

[4]. H. Shacham and B. Waters, ―Compact Proofs of Retrievability,‖ Proc. of Asiacrypt '08, Dec. 2008.

[5]. K. D. Bowers, A. Juels, and A. Oprea, ―Proofs of Retrievability: Theory and Implementation,‖ Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.

[6]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable Data Possession at Untrusted Stores,‖ Proc. OfCCS '07, pp. 598–609, 2007.

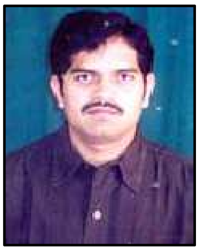
[7]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, ―Scalable and Efficient Provable Data Possession,‖ Proc. of SecureComm '08, pp. 1– 10, 2008.

[8]. T. S. J. Schwarz and E. L. Miller, ―Store, Forget, and Check: UsingAlgebraic Signatures to Check Remotely Administered Storage,‖ Proc.

About the authors:

K.Divya, completed B.Tech from Guru Nanak Institute Of Technology, Hyderabad, JNTUH with Distinction. Currently pursuing M.Tech 2nd Year in Sri Indu College Of Engineering and Technology. Areas of Interest are Cloud Computing, Advance Problem Solving, OOAD, Web Technologies.

P.Navya Sri, completed B.Tech from Guru Nanak Institute Of Technology,Hyderabad,JNTUH with Distinction. Currently pursuing M.Tech 2nd Year in Sri Indu College Of Engineering and Technology. Areas of Interest are Cloud Computing, Data Base Management Systems, Computer Networks, Web Technologies.



Tejavath Charan Singh received his B.Tech degree in Computer Science Engineering from JNT University, Hyderabad, India, in 2006, the M.Tech degree in Software Engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in 2010. Worked as an Assistant Professor in the dept. of Computer Science Engineering at Holy Mary Institute of Technology & Science (HITS COE). Presently, working as assistant professor in dept. of Computer Science Engineering at Sri Indu College of Engineering and Technology. His research interests include Data Mining, Network Security, Information Security, Web Services and Mobile computing.