TPA Based Public Auditing for Data Storage Security in Cloud Computing

[1]Karuna G, [2]K. Ravindra, [3]Sekhar Ch.
[1,2]Dept. of CSE, Avanthi Institute of Engg. and Tech. Cherukupalli (P), Bhogapuram (M), Vizianagaram, AP, India
[3]Dept. of CSE, Vignan's IIT, Visakhapatnam, AP, India

Abstract
In this paper we discuss the evolvement if cloud computing paradigm and present a framework of Third Party Auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. Cloud computing as the on-demand and remote provision of computational resources has been eagerly waited for a long time as a computing utility. It helps users to store their data in the cloud and enjoy the high quality service. However, users do not have physical possession on their own data, hence using a shared pool of configurable computing resources. When users put their data (of large size) on the cloud, the data integrity protection is challenging. Enabling public audit for cloud data storage security is important. Users can ask an external audit party to check the integrity of their outsourced data. Security and performance analysis show that the proposed schemes are highly efficient and provably secure.

Keywords
Cloud Computing, Public Audit Ability, Third Party Auditor (TPA)

I. Introduction

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualized resources are provided aa service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them.

The underlying concept dates back to 1960 when John McCarthy opined that "computation may someday be organized as a public utility"; indeed it shares characteristics with service bureaus which date back to the 1960s. The term cloud had already come into commercial use in the early 1990s to refer to large ATM networks. By the turn of the 21st century, the term "cloud computing" had started to appear, although most of the focus at this time was on Software as a service (SaaS).

A. Types Of Cloud Computing

1. Public Cloud

An IT capability as a service that providers offer to consumers via the public Internet.

2. Private Cloud

An IT capability as a service that providers offer to a select group of customers.

3. Internal Cloud

An IT capability as a service that an IT organization to its own business (subset of private cloud).

4. External Cloud

An IT capability as a service offered to a business that is not hosted by its own IT organization.

5. Hybrid Cloud

IT capabilities that are spread between internal and external clouds While there are many roads to cloud computing from existing client-server infrastructures, there are at least three major

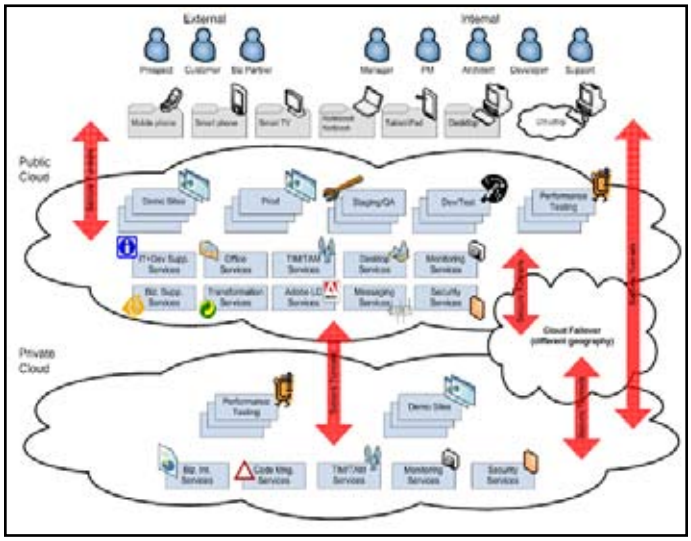

Fig. 1: Cloud Computing Architecture

In this paper, we address the security issue from information assurance and security point of view. That is, we take holistic view of securing cloud computing by using the third party auditor (TPA), vehicle.

Earlier works performs auditing only for static data. We enhance the system with dynamic operations on data locks i.e.) data update, append and delete.

II. Related Work and Proposed System

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. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability.

This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the

new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.

3. 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.

III. System Design

Software as a Service (SaaS) is a popular cloud service model. Applications are accessible various web browsers.

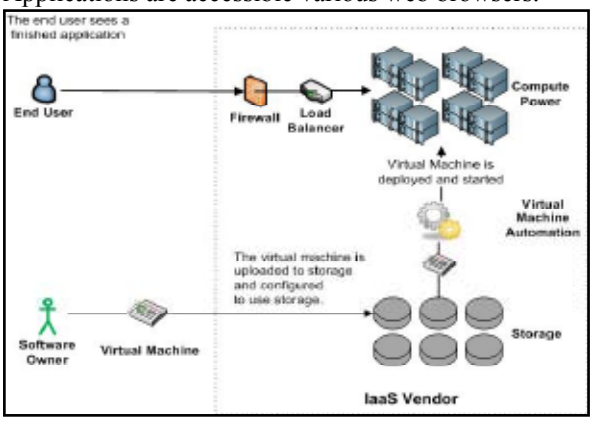

Fig. 2: Architectural Diagram of Software as a Service

Cloud computing components are classified as

- Cloud Client
- Cloud Storage Server (CSS)
- Third Party Auditor (TPA) and Mobile Alert.

Client

An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.

Cloud Storage Server (CSS)

An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data.

Third Party Auditor

An entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

Mobile Alert

An entity, which produces an alert to the cloud storage service provide or administrator who manages the cloud storage server.

A. Input Design

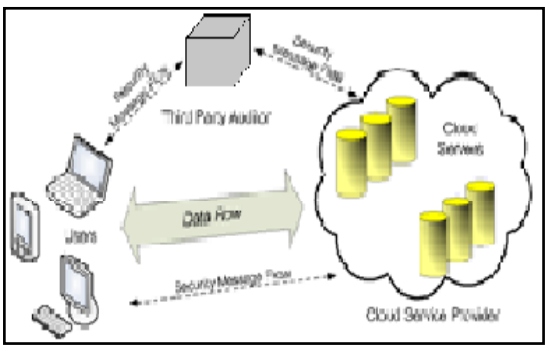

Fig. 2: The Architecture of Cloud as a Storage Service

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

B. Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

C. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.

- Trigger an action.
- Confirm an action.

IV. Design of TPA

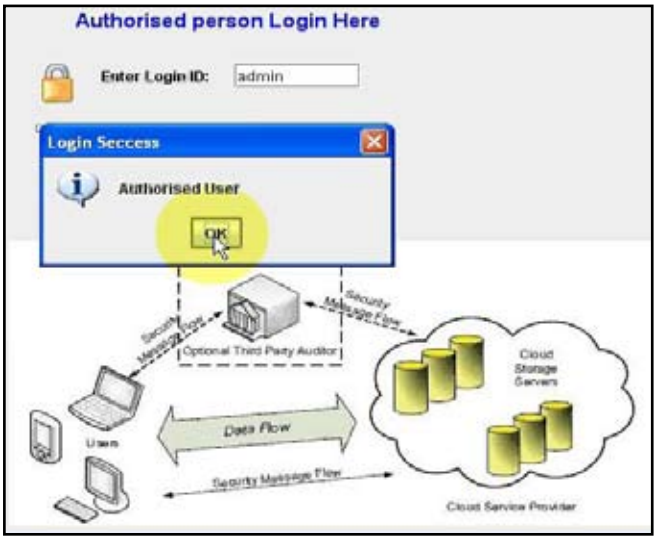

Fig. 3: Login Screen

Fig. 4: Cloud Authenticate Server

Fig. 5: Key Entry Screen

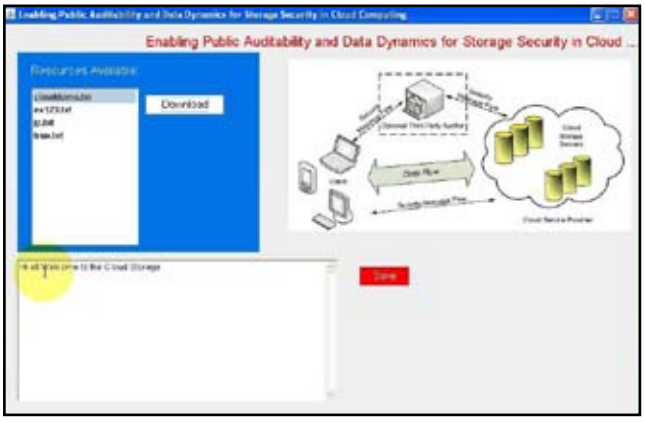

Fig. 6: Resource Available Checking Screen

Fig. 7: Mobile Alert Screen

V. 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 erasure coded 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.

We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. We envision several possible directions for future research on this area. The most promising one we believe is a model in which public verifiability is enforced. Public verifiability, supported in allows TPA to audit the cloud data storage without demanding users' time, feasibility or resources. An interesting question in this model is if we can construct a scheme to achieve both public verifiability and storage correctness assurance of dynamic data. Besides, along with our research on dynamic cloud data storage, we also plan to investigate the problem of fine-grained data error Localization.

References

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

[2] N. Gohring (2008),"Amazon's S3 down for several hours", [Online] Available: http://www.pcworld.com/businesscenter/article/142549/amazo s s3 down for several hours.html

[3] Sekhar Ch, U Nanaji,"Secure Cloud by IT Auditing", International Journal of Modern Engineering Research (IJMER), Vol. 1, Issue 2, pp. 332-337, [Online] Available: http://www.ijmer.com

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

[5] H. Shacham, B. Waters,"Compact Proofs of Retrievability", Proc. of Asiacrypt '08, Dec. 2008.

[6] K. D. Bowers, A. Juels, A. Oprea,"Proofs of Retrievability: Theory and Implementation", Cryptology ePrint Archive, Report 2008/175, 2008, [Online] Available: http://www.eprint.iacr.org/.
[7] G. Ateniese, R. D. Pietro, L. V. Mancini, G. Tsudik,"Scalable and Efficient Provable Data Possession", Proc. of SecureComm '08, pp. 1– 10, 2008.
[8] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", Proc. 14th European Symp. Research

Mrs G Karuna received the B.Tech Degree from JNTU, Kakinada in 2009 and She is currently pursuing M.Tech in the Department Of Computer Science and Engineering in Avanthi Institute of Engineering Technology Of JNTUK Affiliation, Her research interests include Data Mining, Cloud Computing.

Mr. Ravindhra received the the M.Sc from Andhar university, Vizag, and M.Tech in Computer Science Technology(CST) GITAM University. He is working as Assistant Professor In CSE Dept, at Avanthi Institute of Engineering andTechnology, Vizianagaram. And also Worked as Programmer in TEQIP (Technical Education Quality Improvement Program) at Andhra University College of Engineering from December 2005 to August 2009. His research interests include Data Mining, and Computer Networks.

Mr. CH. Sekhar received the the B.Tech Degree from JNTU, Hyderabad in 2005 and M. Tech degree in Computer Science Engineering JNTU, Kakinada in 2011, He is working as a Sr.Asst.Prof In CSE Dept, Vignan's IIT, Vizag, and also Worked as Sr. Assistant Professor in Avanthi Groups of College from Sep 2005 to May 2012. Research interests include Data Mining, Cloud Computing and Computer Networks.