INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 5, MAY 2013
ISSN 2229-5518

A NOVEL APPROACH FOR VERIFYING INTEGRITY OF DYNAMIC DATA STORAGE IN CLOUD ENVIRONMENT

S.NIKETHINA B.TECH IT

Abstract - Cloud computing refers to the use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.). Cloud users may access the server resources using a computer or other device. In cloud computing, applications are provided and managed by the cloud server and data is also stored remotely in the cloud configuration. Users do not download and install applications on their own device or computer; all processing and storage is maintained by the cloud server. Security is the major problem in Cloud as its open to many users. This work studies the problem of ensuring the integrity of dynamic data storage in Cloud Computing. In order to maintain the integrity of data in cloud public audit ability is provided to the network. This can be done by third party auditor (TPA) on behalf of the cloud client to verify the integrity of the dynamic data stored in the cloud. This eliminates the interference of Client to check their intactness which is important in achieving economies of scale for Cloud Computing. The forms of data operation such as block modification, insertion, and deletion is also a significant in the cloud function which is done here. The security problems of direct extensions with dynamic data updates is detected. In particular, to achieve efficient data dynamics, the existing proof of storage models is improved by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks and to further explore the technique of bilinear aggregate signature the result is extended, where TPA can perform multiple auditing tasks simultaneously.

Index Terms—Data storage, public auditability, data dynamics, cloud computing.

S.NIKETHINA.B.TECH(IT), is currently pursuing masters degree program in computer science and engineering in Coimbatore institute of technology, India, PH-9500610270.
E-mail : snikethina@gmail.com..

1.INTRODUCTION

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typicallythe Internet).Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

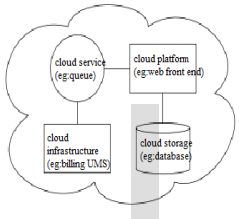
A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic; a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet.In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market.

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 5, MAY 2013
ISSN 2229-5518

1.1 THE INTERCLOUD

The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based. The term was first used in the context of cloud computing in 2007. It became popular in 2009 and has also been used to describe the datacenter of the future.The Intercloud scenario is based on the key concept that each single cloud does not have infinite physical resources. If a cloud saturates, the computational and storage resources of its infrastructure, it would not be able to satisfy further requests for service allocations sent from its clients.

1.1 ARCHITECTURE



Architecture of cloud

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.

1.3 CLIENT

A cloud client consists of computer hardware and computer software that relies on cloud computing for application delivery and that is in essence useless without it. Examples include some computers (example: Chromebooks), phones (example: Google Nexus series) and other devices, operating systems(example: Google Chrome OS), and browsers.

1.4 SERVER

The servers layer consists of computer hardware and computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

1.5 THE PRINCIPLES OF PUBLIC AUDIT

The Public Audit Forum believe that there are three fundamental principles which underpin public audit:

- the independence of public sector auditors from the organisations being audited;
- the wide scope of public audit, that is covering the audit of financial statements, regularity (or legality), propriety (or probity) and value for money; and
- the ability of public auditors to make the results of their audits available to the public, and to democratically elected representatives.

1.5 CLOUD STORAGE:

Cloud storage is a model of networked online storage where data is stored on virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers; and people who require their data to be hosted buy or lease storage capacity from them and use it for their storage needs.

2. PROBLEM DEFINITION

2.1SYSTEM MODEL

Three different network entities can be identified as follows:

1. 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

2. 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

3. Third Party Auditor (TPA): 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. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 5, MAY 2013
ISSN 2229-5518

certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies. In case that clients do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA.

2.2 SECURITY MODEL

In security model the checking scheme can be secure if

1. There exists no polynomial-time algorithm that can cheat the verifier with non-negligible probability

2. There exists a polynomial-time extractor that can recover the original data files by carrying out multiple challenges-responses. The client or TPA can periodically challenge the storage server to ensure the correctness of the cloud data, and the original files can be recovered by interacting with the server. The security model has subtle but crucial difference from that of the existing PDP or PoR models in the verification process. These schemes do not consider dynamic data operations, and the block insertion cannot be supported at all. This is because the construction of the signatures is involved with the file index information . To deal with this limitation, remove the index information is removed and so individual data operation on any file block will not affect the others. In order to achieve this blockless verification, the server should take over the job of computing and then return it to the provider.http://www.ijser.org.

The consequence of this variance will lead to a serious problem: it will give the adversary more opportunities to cheat the provider. Due to this construction, the security model differs from that of the PDP or PoR models in both the verification and the data updating process. Specifically, the tags in our scheme should be authenticated in each protocol execution other than calculated or pre-stored by the verifier. Here server and provider (or client, TPA and verifier) is used interchangeably.

2.3 PROPOSED SYSTEM

The objective of the proposed system is to present the security protocols for cloud data storage service. The basic solutions is to provide integrity assurance of the cloud data .A Merkle Hash Tree (MHT) is used in the proposed scheme which is a wellstudied authentication structure and is intended to efficiently and securely prove that a set of elements are undamaged and unaltered. It is constructed as a binary tree where the leaves in the MHT are the hashes of authentic data values. Here exists a polynomial-time extractor that can recover the original data files by carrying out multiple challenges-responses. The client or TPA can periodically challenge the storage server to ensure the correctness of the cloud data, and the original files can be recovered by interacting with the server. The security model has subtle but crucial difference from that of the existing PDP or PoR models in the verification process. The proposed scheme do not consider dynamic data operations, and the block insertion cannot be supported. This is because the construction of the signatures is involved with the file index information. Here the security model differs from PDP or PoR models in both the verification and the data updating process. Specifically, the tags in this scheme should be authenticated in each protocol execution other than calculated or pre-stored by the verifier. In this scheme, the server and provider (or client, TPA and verifier) are used interchangeably.

3. OVERVIEW OF THE PROJECT

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 scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high quality services from data and software that reside solely on remote data centers. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers.In this project a separate space is allocated for storing data in cloud environment. It provides more security for data from unauthorized users. Here security is achieved by public auditability. In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 5, MAY 2013
ISSN 2229-5518

cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks .http://www.ijser.org.

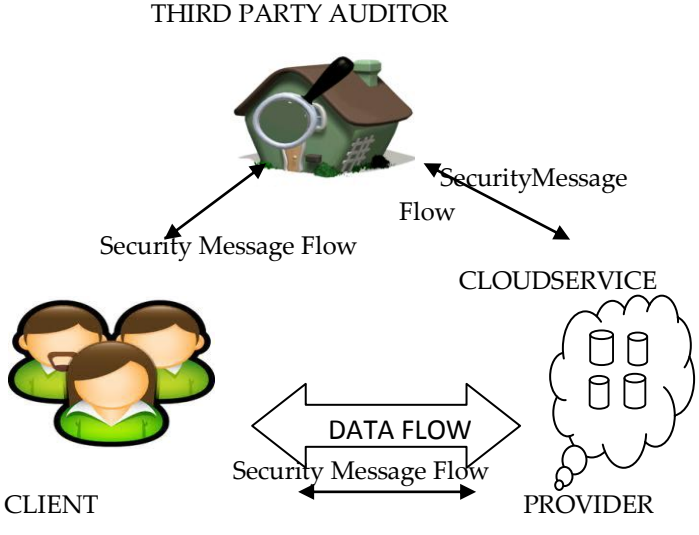
3.1 Design Goals

Our design goals can be summarized as the following:

1. Public auditability for storage correctness assurance: to allow anyone, not just the clients who originally stored the file on cloud servers, to have the capability to verify the correctness of the stored data on demand.
2. Dynamic data operation support: to allow the clients to perform block-level operations on the data files while maintaining the same level of data correctness assurance. The design should be as efficient as possible so as to ensure the seamless integration of public auditability and dynamic data operation support. 3. Blockless verification: no challenged file blocks should be retrieved by the verifier (e.g., TPA) during verification process for efficiency concern.

3.2 FIGURES

For further information about typesetting cloud computing providers, please visit the IJSER styel guide: http://www.ijser.org.



3.3 ACKNOWLEDGEMENT

I thank the almighty for His blessings on us to complete this project work successfully.With profound sense of gratitude I sincerely thank the **Managing Trustee of SNR and SONS, Thiru C.Soundararaj D.Text(Bolton)., L.T.I(Manchester).,** and **Joint Managing Trustee, Thiru R.Vijayakumhar B.E., M.S., MBA.,** for having provided me the necessary infrastructure required for the completion of my project. With profound sense of gratitude I sincerely thank the **Head of the Institution Dr.R.Radhakrishnan** for his kind patronage, which helped in pursuing the project successfully. With immense pleasure I express our hearty thanks to **Head of the Department Dr.R.Nedunchezhian** Department of Information Technology for his encouragement towards the completion of this project. With immense pleasure we express our hearty thanks to my project guide **Prof.N.Saranya M.TECH.,** for her encouragement, pertinent suggestions and valuable guidance towards the completion of this project and I also thank my project coordinator **Prof.V.Karpagam M.E., (Ph.D)** Department of Information Technology,SRI RAMAKRISNHA ENGINEERING COLLEGE.

I convey my thanks to all teaching and non-teaching staff members of the IT Department of my college who rendered their co-operation by all means for completing this project. Also I thank my parents and friends who were very supportive for completion of my project.

4.CONCLUSION

To ensure cloud data storage security, it is critical to enable a Third Party Auditor(TPA)to evaluate the service quality from an objective and independent perspective. Public auditability also allows clients to delegate the integrity verification tasks to TPA while TPA themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is how to construct verification protocols that can accommodate dynamic data files. In this paper, the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing is explored. Here construction is deliberately designed to meet these two important goals while efficiency being kept closely. To achieve efficient data dynamics,the proof of storage models is improved by manipulating the classic

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 5, MAY 2013
ISSN 2229-5518

Merkle Hash Tree construction for block tag authentication.. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

REFERENCES

[1]. K.D. Bowers, A. Juels, and A. Oprea, "Hail: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), pp. 187-198, 2009

[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-609, 2007

[3]. P.Devanbu, M.Gertz,C. Martel, and S. Stubblebine. Authentic third-party data publication. In IFIP DBSec'03, also in Journal of Computer Security, Vol.11, No. 3, pages 291-314, 2003, 2003

[4]. A.Juels and B.S. Kaliski Jr., "Pors: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007