Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

RIGOROUS PUBLIC AUDITING SUPPORT ON SHARED DATA STORED IN THE CLOUD BY PRIVACY-PRESERVING MECHANISM

Dhanashri Bamane
Vinayak Pottigar
Subhash Pingale
Department of Computer Science and Engineering
SKN Sinhgad College of Engineering Korti, Pandharpur, Maharashtra,India

ABSTRACT

Cloud storage systems allow data owners to host their data on cloud servers and users (data consumers) can access their data from cloud servers. The paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud server. Generally security in cloud is achieved by signing the data block before sending to the cloud server. Moreover, users should use cloud storage like the local storage and they didn't worry about the integrity of the data. In large-scale cloud storage systems, the data may be updated dynamically, so existing remote integrity checking methods served for static archive data are no longer applicable to check the data integrity. Thus, efficient and secure dynamic auditing protocols desired to convince data owners that the data is correctly stored in the cloud. The public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of stored data when needed. To securely introduce an effective third party auditor (TPA), these are : 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we propose a secure cloud storage system supporting privacy-preserving and public auditing.

KEYWORDS: Data storage, privacy-preserving, public auditability, cryptographic protocols, cloud computing

INTRODUCTION

Cloud computing eliminate the need for maintaining expensive computing hardware. The service provided by the cloud is very economical. The user pay only for what he/she used i.e. based on storage space, processors, ram size and database. The cloud provides the facility like storage of data, accessing service and using infrastructure. In Cloud, application software and services are move to the centralized large data center which is not trustworthy. Through the use of virtualization and resource time-sharing, clouds address with a single set of physical resources for large user base with different needs. Thus, clouds promise to enable for their owners the benefits of an economy of scale and, at the same time, reduce the operating costs for many applications.

The Cloud service providers (CSPs) manage the PCS and offer the services as the following three categories: software as a service, platform as a service, and infrastructure as a service. If you look category wise the cloud computing divided into public cloud, private cloud, hybrid cloud. In public cloud, the service provider avail the services like software applications, storage, Infrastructure. Whereas private clouds can accessed by particular organizations. Hybrid cloud comprises with public and private cloud. The main challenge in the cloud is data integrity and preserving. Recently many works focusing on providing three advanced features for remote data integrity checking protocols these are data dynamic, public verifiability and privacy against verifiers. The proposed system support data dynamics at the block level, including block insertion, blocks modification and block deletion, it support public verifiability, by which anyone can perform the integrity checking operation. The system supports privacy against third party verifiers.

LITERATURE REVIEW

A. Boyang Wang

A novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, they exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. [1]

B. G Ateniese, R Burns, R Curtmola,

A model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. [2]

C. H. Shacham and B. Waters

The proposed first system built from BLS signatures and secure in the random oracle model, featuresa proof-of-retrievability protocol in which the client's query and server's response are both extremely short. This scheme allows public verifiability: anyone can act as a verifier, not just the file owner.[3]

D. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia

The proposed a framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. They use a new version of authenticated dictionaries based on rank information.[4]

E. Boyang Wang, Baochun Li and Hui Li

The Proposed the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. They also identify the difficulties and potential security problems of direct extensions with fully dynamic data updates.[5]

F. Boyang Wang

The proposed a work that achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). IT also supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. [6]

G. B. Chen

The proposed Remote Data Checking-Network coding (RDC-NC), a novel secure and efficient RDC scheme for network coding-based distributed storage systems. RDC-NC mitigates new attacks that stem from the underlying principle of network coding**. [7]**

H. Y .Zhu

The proposed a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. The audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection**.** [8][9]

I. Boyang Wang

The propose a design a certificate less public auditing mechanism to eliminate the security risks introduced by PublicKey Infrastructure (PKI). Specifically, with this mechanism public verifier does not need to manage certificates to choose the right public key for the auditing. [10]

PROBLEM FORMULATION

The aim of this work is to study and implement Data preserving and auditing in cloud server. The owner of data will audit the shared data and checking the integrity without downloading the complete data. Our system

achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the third party auditor. Due to multiple delegated auditing performance of auditing will increase and network overhead will reduce.

SYSTEM ARCHITECTURE

The system model in this paper involves three parties: the cloud server, a group of users and a public verifier. There are two types of users in a group: the admin and user groups. The admin initially stored data in the cloud and shares it with groups. Both the admin and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services. User outside the group intending to utilize shared data is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge-and-response protocol between a public verifier and the cloud server.

Data Dynamics

The meaning of Data Dynamics is to update data dynamically on cloud server. The main operations are block insertion, block modification and block deletion.

Public Verifiability

During the process of data uploading and downloading secret key sent to the client's email and can perform the integrity checking operation. The public verifiability has two entities: a challenger that stands for either the client or any third party verifier, and an adversary that stands for the untrusted server.

Metadata Key Generation

The metadata is data about data. Let the verifier V wishes to the store the file F. Let this file F consist of n file blocks. Initially preprocess the file and create metadata to be appended to the file. Let each of the n data blocks have m bits in them. A typical data file F which the client wishes to store in the cloud.

Each of the Meta data from the data blocks m_i is encrypted by using a RSA algorithm to give a new modified Meta data M_i. Without loss of generality Show this process. The encryption method can be improvised to provide still stronger protection for Client's data. All the Meta data bit blocks that are generated using the procedure are to be concatenated together. This concatenated Meta data should be appended to the file F before storing it at the cloud server. The file F along with the appended Meta data with the cloud.

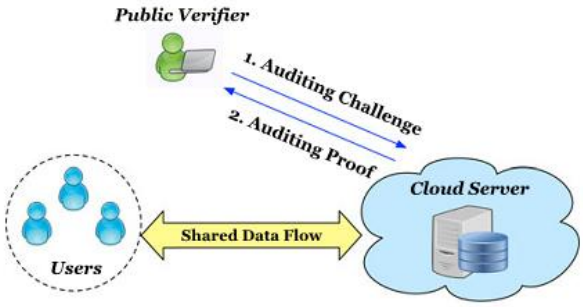

Figure 1

RESEARCH METHODOLOGY

Security is the most important issue in cloud computing. Cloud computing entrusts services with users data, software and share among the users. Cloud provides a platform as a service (PaaS), software as a service (SaaS) and Infrastructure as a service (IaaS). The cloud provides the support to desktop application to mobile application which includes web application etc. The basic purpose of the cloud is to eliminate the cost of hardware through the service.

In Cloud maintaining data integrity is one of the most important and difficult task. When we talk about cloud users, they are using cloud services provided by the cloud provider. So we cannot trust the service provider to handle the data, it is high chances of modification of the original data and the data integrity may be lost. If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider. So, in this case, we take the help of a trusted third party auditor to check for the integrity of our data.

The system is developed under Visual Studio 2013 Express edition with ASP.net (C#, .net Framework 4.0), Microsoft SQL Server 2012 Express edition, and The Microsoft Azure Cloud emulator is used for testing purpose. The system provides highly secure way for data integrity and security. It also helps traceability due to which the auditing will become easier. Whenever the user want to download the data the admin will get the complete information about the user through the email and at the same time it store the user detail on the web site which can be further use for auditing. The system generate metadata key though the file attribute.

CONCLUSION

Implementation of cloud on local Microsoft Azure gives awesome results. There are many challenges in local implementation some of them are Microsoft Azure emulator supports 2GB file size but uploading the 2GB File size require lot of modification in File Uploading control in ASP.net.

The system provides batch auditing and data verification without the complete downloading of data. Generally the integrity of data is check at local level so the mentioned system provides the optimal solution for data integrity checking and auditing system but system allows the same purpose through online hence lot of network overhead will avoided. The cryptography is used to calculate the hash and key generation purpose based on the uploading file. The system provides highly secure data storage with facility of auditing with traceability feature.

ACKNOWLEDGMENT

I would like to thank my guide Prof. Vinayak Pottigar and co-guide Prof. Subhash Pingale for their valuable contribution in completing my work. I would also express thank to my family for moral support.

REFERENCES

[1] Boyang Wang, Baochun Li and Hui Li, "Privacy Preserving Public Auditing for Shared Data in the Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, Hanuary-March 2014.

[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. 598-610, 2007.

[3] 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 (ASIACRYPT '08), pp. 90-107, 2008.

[4] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[9] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, 2012.

[10] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.

AUTHORS PROFILE

Dhanashri Bamane is working toward the ME degree in the SKN Sinhgad College of Engineering, Korti-Pandharpur, Solapur University. Her research interests include cloud computing.