Integrity Check of Shared Data on Cloud with Various Mechanisms

Sarika Katkade
ME Scholar,
Department of Information Technology,
PCCOE, Pune, India

J. V. Katti
Associate Professor,
Department of Information Technology,
PCCOE, Pune, India

ABSTRACT
Cloud computing is the process and adoption of existing technologies and paradigms. The aim of cloud processing is to allow users to take benefit from all of these solutions, without the need for deep information about or competence with each of them. This new era of information storage service also introduces new security issues, because data is organized on third party which might not exactly be trust deserving always. Data integrity is main security concern. Information integrity is the preservation of, and the guarantee of the accuracy and consistency of, data over its entire life-cycle. This kind of survey paper elaborates different protocols that verify remote control data accuracy. These protocols have been proposed a model for ensuring the long-term security and availability of data stored at remote untrusted hosts.

General Terms
Cloud data, Data verifiability and User revocation

Keywords
Cloud security, Data Integrity, Third party auditor, Data security, Encryption

1. INTRODUCTION

1.1 Cloud computing
Cloud computing is a type of large-scale distributed processing paradigm. The phrase "cloud" is commonly used in technology to describe a sizable collection of objects that creatively appear from afar as a cloud and identifies any set of things whose details are not further inspected in a given context [3]. It is a model for enabling, on-demand usage of a shared pool of configurable computing resources likewise computer networks, web servers, storage, applications and services. It provides the chances of enhancing IT systems management and is changing the way in which hardware and software are designed, purchased, and employed. There are a variety of applications that can be delivered to users through cloud computing models, from content management to specialist applications for activities [7]. Among all the assistance provided by cloud computing, cloud storage is one of the main services that enables cloud users to move their data from local storage systems to the cloud.

Cloud storage service brings drastic benefits to data owners, by reducing cloud users' load of storage management and equipment maintenance, staying away from investing a tremendous amount in software and hardware, by enabling the data access independent of physical position, accessing cloud data anytime and from everywhere.

Cloud storage offers worldwide payable and location third party storage services for cloud users, it is now a quick profit growth justification in cloud computing. According to a survey in [4], cloud storage does induce some new security hazards to data owners. Several cloud users would do not like to use cloud storage space due to some serious security worries. A very first concern of cloud users is the sincerity of their outsourced data files. There are several factors that might lead to data file corruption error [11]. First, cloud companies are not fully relied on. As a result, for a reason, the cloud service agency might be eliminating the information that are almost never or even not utilized in order that it can save the space for storing other documents for charging extra expenditures. Second, the stored data could be corrupted scheduled to cloud servers' inability, hardware failure, management problems or adversary attacks. Nevertheless, in order to keep a good reputation, cloud service agency may purposefully hide data loss events. In cloud storage, data integrity and leakage are getting to be a major concern of cloud users [12].

Possibly though the cloud storage space providers commit a reliable and secure storage service to users, the sincerity of outsourced can still be corrupted due to carelessness of humans or failures of hardware/software[2][3]. Besides interior threats, external adversaries may also destroy the ethics of the outsourced data in the cloud. Consequently, public integrity auditing is needed to convince you that the outsourced data is appropriately stored in the cloud. To ensure the integrity of outsourced data in an untrustable cloud, a number of protocols have been recommended depending on various techniques. Undoubtedly, the encryption technology is still a powerful strategy to ensure data security of cloud computing [6]. How to apply the highly efficient security, how to quickly search the encrypted data, how to carry on fast recovery, the way to turn the access control of data and so on, all of above are a series of key and difficult issues that data security of cloud computing must resolve.

1.2 Data Integrity
Cloud platform is suitable for operating data intensive and computational intensive applications, whether it is business applications or scientific applications. There is a serious requirement to deal with the data security issues for preserving the data integrity, privacy and trust in the cloud environment [10]. While security concerns are protecting some organizations from adopting cloud computing at all.

Various other folks are protecting against resources by using a blend of a secure internal private cloud, along with public atmosphere. Security is crucial for work flow that deal with hypersensitive data. Unique authentication gain access to control, privacy or sincerity. From the existing literatures, as the applications and services model of cloud computing is different from the tradition end-to-end execution of the encrypted communication to ensure data security, an untrusted third get together will participate the process of virtualization storage and processing of massive data, this brings new data security issues [2]. Certainly, the encryption technology is still a powerful measure to ensure data security of cloud computer.

How to implement the highly efficient encryption, how to quickly browse the data encrypted, how to continue disaster recovery and fast recovery, how to proceed the access control of data and so on, most of above are a series of key and difficult problems that data security of cloud computing must resolve.

2. RELATED WORK

2.1 An identity-based auditing mechanism from RSA

Information auditing is extremely important for securing cloud storage space since it allows cloud users to verify the integrity with their outsourced data efficiently. To cope with this, ID-CDIC, an identity-based cloud data integrity checking process which can minimize need of the complex license management in traditional cloud data integrity checking protocols[7]. The proposed tangible construction from RSA personal can support variable-sized document blocks and public auditing. In addition, a formal security model for ID-CDIC and prove the security of our construction under the RSA assumption with large public exponents in the random oracle model.

2.2 Public Integrity Auditing using Code Based Cloud Storage

The system includes 3 different entities: data owners, cloud servers and third party auditor. Data owners have a sizable volume of data to be stored in the cloud. Cloud servers provide data storage space service and have significant storage resources[2]. The auditor is able to check the integrity of information stored in the cloud. Actually in the public auditing, the auditor can be any enterprise in the cloud, i. e., data owners, cloud servers providers, or other third parties. Anyone who is with the auditing parameters can execute the auditing procedure.

In this system, data owners first encode the data document by using regenerating code, and then store the coded file across multiple cloud servers.[9] The multiple cloud web servers may locate in the same provider or different service providers. Data owners may perform block-level active functions on the outsourced data, i.e., stop, modification, insertion, and removal. The auditor could proficiently verify the integrity of the information stored across multiple cloud servers, even the data file is frequently updated by the information owners.

2.3 Public Verifiability Using Multiple TPAs

For data integrity confirmation use a third get together auditor, specifically a sole third party auditor. TPA to help an end user verify the data with the cloud server supplier (CSP)[3]. However, just one third party auditor may become a bottleneck in the overall system procedure and may degrade system performance because thousands of users may delegate their tasks to a sole third party auditor[11]. For securing data sincerity via a multiple alternative party auditors based mutual authentication to overcome the above mentioned limitations and ensure high-level security. MTPAs prevent TPAs from to become bottleneck in the system, thereby leading to improved performance. Gain access to control should be applied to determine traditional users and minimize the possibility of unauthorized users. The communication and computation expense should be reduced. Information integrity with high security may be ensured when blocks of information are distributed between multiple auditors for verification.

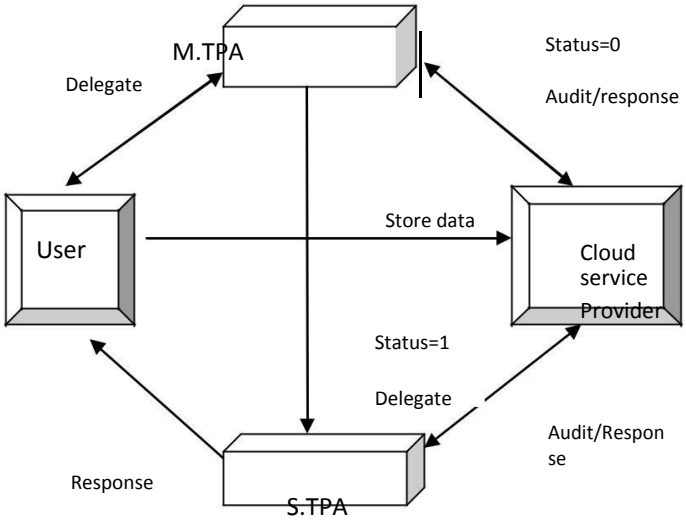

Figure 1: System Architecture of multiple TPA

2.4 RSA Partial Homomorphic and MD5 Cryptography

For keeping the data secure firstly the data is encrypted with the RSA homomorphic algorithm after that public and private key related with file is generated. As encryptions are performed file is ready to be uploaded on cloud servers[4]. After uploading, data owner gets its general detail like uploading time, date, hash generation of file and verification. In this approach for maintaining data security access permission to the specified file is defined. In case if any, malicious get the data they are not able to decrypt it. To check data integrity, data owner can verify their cloud data by requesting for verification option. The data owner requests to perform a hash value of the data present at cloud are calculated. This calculated hash value matches with the old hash value which is present at owner end[10]. If this value match's then data present at the cloud is safe and no modification has been done if it does not match then there are some changes on cloud data.

2.5 Integrity auditing of shared datawith Secure User Revocation

For user revocation and efficient integrity checking, a public integrity checking scheme utilizing polynomial-basedauthentication tags, which is collusion-resistant and of a constant computational cost on the user side[5]. The Shamir Secret Sharing, splits the re-signing process into a number of parts and deploy them to different proxies. In particular, the decentralized re-signing process make the collusion attacks practically infeasible. Shamir secret sharing scheme proposed a public integrity auditing for shared data in the cloud with efficient auditing and collusion-resistant user revocation[9]. The TPA is able to publicly audit the integrity of the shared data in the cloud for the group. The group is an entity consisting of users, who create data and share with each other[12]. Users in the group trust each other and are able to manage the group cooperatively. Cloud users of the group can easily modify the shared data and share data within the group. The shared data is further divided into a series of blocks and each block is attached a signature computed by its modifier.

3. COMPARISON ANALYSIS

3.1 Encryption Technique

For Data integrity various encryption algorithms are used like an RSA algorithms[1] , message digest 5 algorithms [4] , Shamir secret sharing [5] which helps for dynamic user revocation for protecting integrity of file.

3.2 Public Verifiability

All above mentioned techniques in section 2, provides Public verification in case of users share information in group and need to be secret for that group only.

3.3 Advantages

Using RSA algorithm, complexity of maintaining traditional Public key certificate [1]. System performance get improved[2] using dynamic code based storage. Collusion Problem tackled using sharing scheme[5].

4. CONCLUSION

This article mainly discussed about cloud data integrity, different integrity techniques and user authenticator scheme that helps assurance of data. Using multiple third party auditor, bottleneck of TPA can be reduced. Communication and computation overhead should be reduced. The public key infrastructure is used to build cloud data confidential that unauthorized user not allowed to access any data other than their respective access control. Encryption and decryption is done by RSA partial algorithm, whereas MD5 hashing algorithm is used for secure data backup.

5. DIRECTIONS FOR FUTURE RESEARCH

The performance reviews help us to find the drawbacks and future needs of data security over remote end. As a result, the survey work will be supportive for researcher to focus on the suggested various cryptographic techniques for ensuring data accuracy.

6. REFERENCES

[1] Yong Yu, Liang Xu, Man Ho Au, Willy Susilo , Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, Jian Shen ,“Cloud data integrity checking with an identity-basedauditing mechanism from RSA”, Future Generation Computer Systems 62 (2016) 85–91, 2016.

[2] Kai He, Chuanhe Huang, Jiaoli Shi, Jinhai Wang,“Feature Public Integrity Auditing for Dynamic RegeneratingCode Based Cloud Storage”, IEEE Symposium on Computers and Communication (ISCC), 2016.

[3] Salah H. Abbdal , Hai Jin, Ali A. Yassin, Zaid Ameen Abduljabbar Mohammed Abdulridha Hussain, Zaid AlaaHussien, Deqing Zou , “An Efficient Public Verifiability andData Integrity Using Multiple TPAs in Cloud Data Storage”, IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security, 2016.

[4] Priyanka Ora, Dr.P.R.Pal, “Data Security and Integrity inCloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography”, IEEE International Conference on Computer, Communication and Control (IC4-2015), 2015.

[5] Yuchuan Luo, Ming Xu, Shaojing Fu, Dongsheng Wang,Junquan Deng, “Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation”, IEEE Trustcom/BigDataSE/ISPA, 2015.

[6] A. Abidi, B. Bouallegue, and F. Kahri, “Implementation of elliptic curve digital signature algorithm (ECDSA)”, Proceedings of the Global Summit on Computer InformationTechnology (GSCIT’14), Sousse, Tunisia, IEEE, pp. 1–6, 2014.

[7] K. Selvamani and S. Jayanthi, “A review on cloud data security and its mitigation techniques”, Procedia Computer Science, Elseveir, vol. 48, pp. 347 – 352, 2015.

[8] Y. Deswarte, J.-J. Quisquater, and A. Sadane, “Remote integrity checking”, Proceedings of the Sixth Working Conference on Integrity and Internal Control in Information Systems, Springer, USA, pp. 1–11, 2004.

[9] C. Yao, L. Xu, X. Huang, and J. K. Liu, “A secure remote data integrity checking cloud storage system from threshold encryption”, Journal of Ambient Intelligence and Humanized Computing, Springer, vol. 5, no. 6, pp. 857–865, 2014.

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns,“Remote data checking for network coding-based distributed storage systems”, Proceedings of ACM Workshop Cloud Computing Security (CCSW’10), 2010.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores”, in Proceedings of ACM CCS 2007, pp. 598–610.

[12] Y. Yu, J. Ni, M.H. Au, C.X. Xu, et al., “Improved security of a dynamic remote data possession checking protocol for cloud storage”, 2014, Expert Syst. Appl. 41 (17) (2014).

[13] B. Wang, B. Li, H. Li, “Public auditing for shared data with efficient user revocation in the cloud”, in: Proceeding of IEEE INFOCOM’13, Turin, Italy, April 14–19, 2013, pp. 2904–2912.

[14] H. Wang, “Identity-based distributed provable data possession in multicloud storage”, IEEE Trans. 8 (2) (2014) 328–340, 2014.