ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Groupo Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Privacy Preserving Public Auditing for Data in Cloud Storage

M.Priya[1], E. Anitha[2], V.Murugalakshmi[3]

M.E, Department of CSE, Karpagam University, Coimbatore, Tamilnadu, India[1, 3]

M.E, Department of AE, Sri Subramanya College of Engg & Tech, Palani, Tamilnadu, India[2]

ABSTRACT-Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. Cloud Computing reduces cost by allocate computing and storage resources, complex with an on demand provisioning mechanism relying on a pay per use business model. The User doesn't have to worry about storage and maintenance of cloud data. As the data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on cloud. Users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data. Specifically, our contribution in this work can be summarized as the following aspects: Stimulate the public auditing system of data storage security in Cloud Computing and provide a privacy preserving auditing protocol, i.e., our proposal supports an external auditor to audit user's outsourced data in the cloud without learning information on the data content. In Our scheme is the first to support scalable and capable public auditing in the Cloud Computing. In exacting, our scheme achieves batch auditing where several delegated auditing tasks from different users can be performed concurrently by the TPA.

KEYWORDS— Cloud Computing, Cloud Storage, Privacy Preserving, Public Auditing, TPA, Batch Auditing

I. INTRODUCTION

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything from computing power to computing infrastructure, applications, business processes to personal collaboration — can be delivered as a service wherever and whenever need. Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A .Cloud Services

Cloud computing is anything that involves services over the internet. These services are broadly classified into three categories: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Cloud software as a service (SaaS) is the on-demand service developed for end users; provider will license the software for their own use. As the software is managed over the central location over the web, the user need not required to handle the upgrades. E.g.- gmail. And the next service is cloud platform as a service (PaaS) is designed for the application developers, which provide all the facilities for developing the web applications easily with more features without the complexity of buying and maintaining the software and the infrastructure. E.g.-Google App Engine. Finally the cloud infrastructure as a service (IaaS) is way of delivering the cloud computing infrastructure which provisions the storage, service and network.

As it is fully outsources service it is not necessary to purchase the server, software and other equipments for the business and the service providers benefit from cost saving.

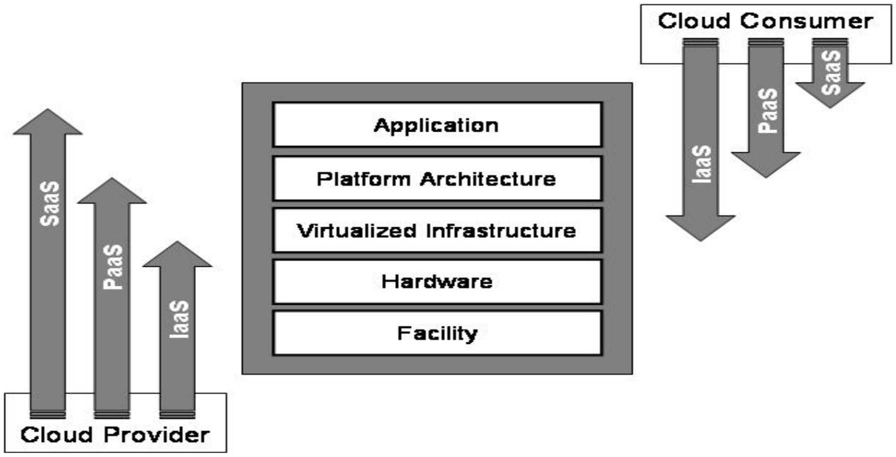

Figure 1: Differences in Scope and Control among Cloud Service Models

B. Cloud Storage

Cloud storage is an important service of cloud computing, which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud. However, this new paradigm of data hosting service also introduces new security challenges. Owners would worry that the data could be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take. Sometimes, cloud service providers might be dishonest. They could discard the data which has not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud.

In existing system, the clients store the data in server that server is trustworthy and after the third party auditor can audit the client files. So, the third party auditor can stolen the files. The main Disadvantage of the Existing system can support both features with the help of a third party auditor. Consider a cloud storage system in which there are a client and an untrusted server. The user stores their data in the server without keeping a local copy. Hence, it is of critical importance that the client should be able to verify the integrity of the data stored in the remote untrusted server. If the servers modify any part of the client's data, the user should be able to detect it; furthermore, any third party auditor should also be able to detect it. In case a third party auditor verifies the integrity of the client's data, the data should be kept private against the third party auditor. Advantages of the proposed scheme have the following main contributions: Remote data integrity checking protocol for cloud storage. The proposed system inherits the support of data dynamics, and supports public verifiability and privacy against third-party verifiers, while at the same time it doesn't need to use a third-party auditor. Data correctness and security analysis of the proposed system which shows that data is secure against the untrusted cloud service provider and private against Third Party Auditor.

II. THE SYSTEM AND HAZARD MODEL

We consider a cloud data storage service connecting three different network entities, the cloud user (U), who has bulky amount of data files to be stored in the cloud; the cloud server (CS), which is managed by the cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources, the third party auditor (TPA), who has knowledge and capabilities that cloud users do not have and is trusted to assess the cloud storage service dependability on behalf of the user upon call. Users rely on the CS for cloud data storage and Protection. They may also dynamically interact with the CS to access and update their stored data for various application purposes. To save the computation resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA. Namely, in most of time it behaves correctly and does not move away from the prescribed protocol execution. However, for their own benefits the CS might ignore to keep or purposely delete rarely accessed data files which belong to normal cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to continue reputation. We assume the TPA, who is in the production of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. However, it harms the user if the TPA could learn the outsourced data after the audit. To authorize the CS to respond to the audit delegated to TPA's, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are authenticated against such a certificate. These authentication handshakes are omitted in the following presentation.

SYSTEM ARCHITECTURE

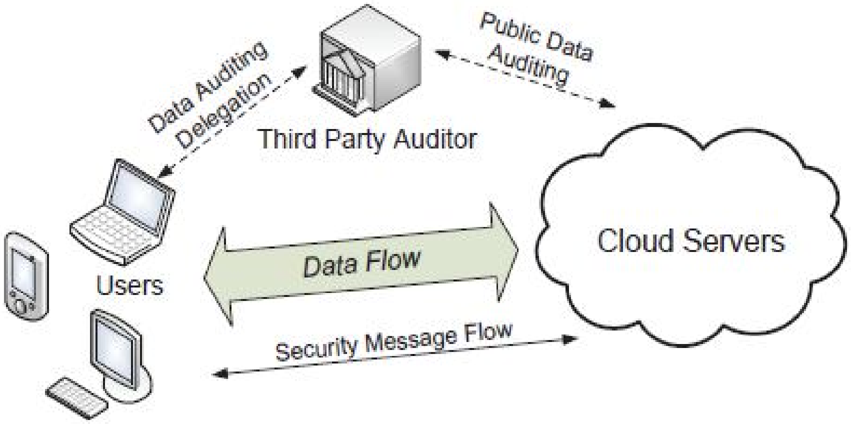

Fig. 1: The architecture of cloud data storage service

III. DESIGN GOALS

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees.

A. Public Audit ability: to permit TPA to validate the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

B. Storage accuracy: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.

C. Privacy-preserving: to guarantee that the TPA cannot derive users' data content from the information collected during the auditing process.

D. Group auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

E. Lightweight: to permit TPA to do auditing with minimum communication and computation overhead.

IV. PRIVACY PRESERVING DATA INTEGRITY CHECKING

A privacy preserving remote data integrity checking protocol with data dynamics and public verifiability make use of a Remote Data Integrity Checking Protocol. The protocol provides public verifiability without the help of a third party auditor. It doesn't leak any privacy information to third party, which provides good performance without the support of the trusted third party and provides a method for independent arbitration of data retention contracts. But it gives unnecessary computation and communication cost.

A. The public auditing protocol: To achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic linear authenticator with random masking technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server. Our design makes use of a public key-based HLA, to equip the auditing protocol with public auditability.

V. HOMOMORPHIC ENCRYPTION

Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. Definition: An encryption is homomorphic, if: from Enc(a) and Enc(b) it is possible to compute Enc(f (a, b)), where f can be: +, × and without using the private key. Among the Homomorphic encryption we distinguish, according to the operations that allows to assess on raw data, the additive Homomorphic encryption (only additions of the raw data) is the Pailler and Goldwasser-Micalli cryptosystems, and the multiplicative Homomorphic encryption (only products on raw data) is the RSA and El Gamal cryptosystems.

VI. CONCLUSION

We propose a privacy-preserving public auditing system for data storage security in Cloud Computing. Cloud computing security is a major issue that needs to be considered. Using TPA, We can verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security. So client can trust on cloud storage service which is provided by cloud because TPA works as a representative of data owner. We achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It also supports data dynamics.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou," Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009,pp.1–9.

[2] C Wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[3] P. Mell and T. Grance, "Draft NIST working definition of Cloud Computing".

[4] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, 3-42.

[5] Q. Wang, C. Wang, Kui Ren, W.Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", in IEEE transaction on parallel and distributed system May 2011.

[6] C. Wang, Q. Wang and K. Ren, "Ensuring Data Storage security in Cloud Computing", IEEE Conference Publication, 17th International Workshop on Quality of Service (IWQoS), 2009

[7] Balkrishnan. S, Saranya. G, Shobana . S and Karthikeyan .S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012

[8] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security" Proceedings of the World Congress on Engineering 2012 Vol I WCE 2012, July 4 - 6, 2012, London, U.K.

[9] AbhishekMohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.

[10] K Govinda, V. Gurunathprasad and H. sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, vol 4,no. 2, ISSN: 2249-9954,4 August 2012