Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 69 – 76

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Third Party Public Auditing scheme for Cloud Storage

Swapnali More[a], Sangita Chaudhari[b]

[a,b]*Department of Computer Engineering, A.C.Patil College of Engineering, Kharghar, Navi Mumbai 410210, India*

Abstract

Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of this work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data. This proposed auditing scheme make use of AES algorithm for encryption, SHA-2 for integrity check and RSA signature for digital signature calculation.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Cloud Storage; TPA; Privacy Preserving ; Public Auditing; Integrity;

1. Introduction

According to the NIST definition, "Cloud computing is a model for enabling ubiquitous, 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" [12].

* Corresponding author.
E-mail address: more.swapnali2312@gmail.com, sangita.sc@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.010

Making use of the cloud saves both users time and money. In Cloud computing, the term cloud is a metaphor for the Internet, so the phrase Cloud computing is defined as a type of Internet-based computing, where different services are delivered to an organization's computers and devices through the Internet [4]. Cloud computing is very promising for the Information Technology (IT) applications; however, there are still some issues to be solved for personal users and enterprises to store data and deploy applications in the Cloud computing environment. Data security is one of the most significant barriers to its adoption and it is followed by issues including compliance, privacy, trust, and legal matters. Therefore, one of the important goals is to maintain security and integrity of data stored in the cloud because of the critical nature of Cloud computing and large amounts of complex data it carries. The users concerns for security should be rectified first to make cloud environment trustworthy, so that it helps the users and enterprise to adopt it on large scale [4].

The foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. Threats, data loss, service disruption, outside malicious attacks, and multi tenancy issues are the security challenges included in the cloud. Data integrity in the cloud system means preserving the integrity of stored information. The data should not be lost or modified by unauthorized users. Cloud computing providers are trusted to maintain data integrity and accuracy of data. Data confidentiality is also important aspect from user's point of view because they store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality could be addressed by increasing the cloud reliability and trustworthiness in Cloud computing. Therefore security, integrity, privacy and confidentiality of the stored data on the cloud should be considered and are important requirements from user's point of view [4]. To achieve all of these requirements, new methods or techniques should be developed and implemented.

Data auditing is introduced in Cloud computing to deal with secure data storage. Auditing is a process of verification of user data which can be carried out either by the user himself (data owner) or by a TPA. It helps to maintain the integrity of data stored on the cloud. The verifier's role are categorized into two: first one is private auditability, in which only user or data owner is allowed to check the integrity of the stored data. No other person has the authority to question the server regarding the data. But it tends to increases verification overhead of the user. Second is public auditability, which allows anyone, not just the client, to challenge the server and performs data verification check with the help of TPA. The TPA is an entity which is used so that it can act on behalf of the client. It has all the necessary expertise, capabilities, knowledge and professional skills which are required to handle the work of integrity verification and it also reduces the overhead of the client. It is necessary that TPA should efficiently audit the cloud data storage without requesting for the local copy of data. It should have zero knowledge about the data stored in the cloud server. It should not introduce any additional on-line burden to the cloud user [6].

The three network entities viz. the client, cloud server and TPA are present in the cloud environment. The client stores data on the storage server provided by the cloud service provider (CSP). TPA keeps a check on client's data by periodically verifying integrity of data on-demand and notifies client if any variation or fault is found in client's data. Figure 1 shows the cloud data storage architecture.

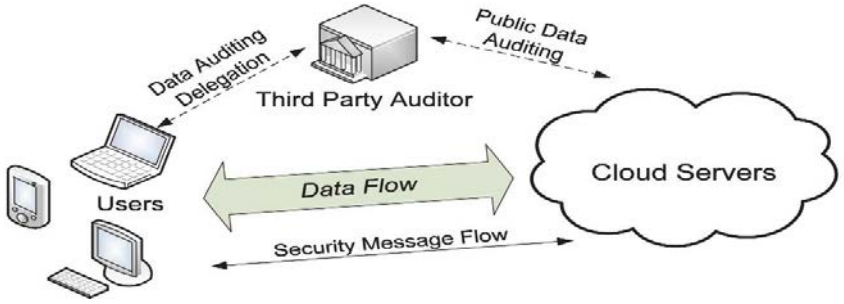

Fig. 1. Cloud Data Storage Architecture