Chapter 15
Cloud-Based TPA Auditing With Risk Prevention

V. Abinaya
Hindusthan College of Arts and Sciences, India

Veera Talukdar
RNB Global University, India

A. V. Senthil Kumar
Hindusthan College of Arts and Sciences, India

Ankita Chaturvedi
IIS University (Deemed), India

Rohaya Latip
Universiti Putra Malaysia, Malaysia

G. Vanishree
IBS Hyderabad, India

Gaganpreet Kaur
Chitkara University, India

ABSTRACT

The chapter focuses on cloud security audit mechanisms and models. Here the third-party auditor (TPA) will be provided with the authority access scheme where the security of the auditing system will be enabled. The TPA will check out the auditing verification and shows a message about the data audited. The purpose of this work is to develop an auditing scheme that is secure, efficient to use, and possesses the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. It consists 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. 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. Thus, the system frequently checks the security of the server-side resources.

DOI: 10.4018/978-1-6684-8098-4.ch015

INTRODUCTION

Cloud computing, where computation and data storage are done in data centers rather than on individual portable PCs, has become highly popular in recent years. Users may store their data remotely and take use of cloud apps thanks to cloud storage, which eases the load of managing local hardware and software. Taking use of cloud storage is a crucial component of file sharing nowadays as more people access their data online. Databases and application software are moved to big data centers via cloud computing, where the administration of the data and services is not justifiable. Data sharing is possible because to cloud platform applications, ideas, and services such processing power, networking, virtualization, and storage. Be sure that the problems most important to you are user privacy and data security. Secure and flexible data storage services are offered by cloud storage service providers, which are ideal for a range of storage needs. Data owner control over the data is lost once it is transferred to the cloud, creating additional security threats to the data's confidentiality and integrity. Cloud storage has gained popularity in recent years thanks to its many applications, including data archiving, file backup, and information sharing. File sharing is implemented in many ways by cloud storage services based on how they are used and what order the permission categories are given. Data confidentiality and user authenticity are required in order to safeguard users and data from one another as well as from hackers. Huge volumes of data are created by these e-applications as they continue to evolve at an accelerated rate in e-business, e-science, and social networking. For instance, popular social networking services like Twitter and Facebook keep serving billions of page visits, managing billions of information, and many images.

Cloud computing is very talented for IT schemes but some obstacles remain for discrete users and organizations to overcome in order to save and device cloud computing systems. Data security is one of the most important contests to its implementation and enforcement, privacy, trust and legal concerns are being undertaken. Therefore, one primary priority is to ensure the confidentiality and integrity of the data stored in the cloud, because cloud storage is essential and thus carries vast quantities of large amounts of data. Users' security concerns should first be addressed to ensure that the cloud environment is reliable, so that users and companies take it on a large scale. Cloud security concerns are imperative: anonymity, safety of in formation, data availability, location of data and safe broadcast. Threats, data loss, service failures, external malicious attacks and multi-lease issues are among the security threats in the cloud. The confidentiality of data in the cloud network ensures the confidentiality of stored information is protected. No unlicensed users should lose or modify the data. Cloud computing providers rely on information security and information constancy. Data confidentiality is also important to the customer, because they store sensitive or private data in the cloud. Authentication and access control mechanisms are used to ensure data privacy. Information security can be addressed by collective cloud presentation and cloud storage reliability. The health, integrity, privacy and confidentiality of stored cloud data and critical user requirements should also be considered. Modern approaches and strategies to satisfy all the secriteria should be developed and implemented.

Cloud Computing

A collection of interconnected, virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLAs) negotiated between the service provider and customers make up the cloud, a parallel and distributed computing system. Clouds are vast collections of readily available and reachable virtualized resources, including hardware,