Abstract

Cloud computing has emerged as one of the latest computing paradigm and is a growing technology for upcoming years. According to NIST Cloud computing is a model for convenient, on-demand network access to a large pool of computing resources. Resource can be hardware or software resource and this pool of resources can be rapidly provisioned and released with minimum management effort or cloud service provider interaction [1].

In Cloud computing, different types of data and program can be stored at different locations, the cloud data centers and can be accessed whenever required, from anywhere, via different type of devices having internet connection. Due to this method of storing user’s data at cloud provider’s end, users gets numerous benefits such as, access flexibility, large storage capability, and resilience. In Cloud computing vendor supplies the hardware infrastructure, and the software interacts with the user through a front-end portal [2][3].

One of the service provided by the Cloud computing is Cloud storage, in which user information
and data is stored, managed, backed up on multiple locations as a replica and made available to users via interconnection network. Apart from all benefits and advantages there are some concerns as well related to cloud computing, as in cloud computing data is put outside the control of the end user on a location that is unknown to the user. Due to this, Cloud computing also raises to various security issues. [4] End user is concerned about the integrity of data that is stored in cloud, as user’s data can be modified by attackers or even in some cases due to employee espionage.

The cloud server is just used to save the encrypted blocks of data for the user. By using the auditing approach processing overhead of cloud server and verifying authority can be largely reduced. Cryptography is an effective technique that helps to assure user’s data accuracy. The Cryptographic techniques can be used in cloud to protect the data from attackers. In this paper, the significance of cryptography is discussed by which possibility of attacks on cloud data can be reduced. This paper covers some of the existing cryptographic methods that ensure the security of cloud data. In this paper auditing scheme is presented using cryptographic techniques and by using the auditing scheme based on the cryptography user data becomes more secure, that leads to enhancement of trust between the end user and cloud provider. Cloud data auditing is necessary for securing data in cloud storage since it facilitates cloud users to verify the integrity of their outsourced data effectively and efficiently.

References


Index Terms

Computer Science Security
Keywords

Cloud Server, IaaS, PaaS, SaaS, TPA.