Abstract

Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, accessibility, low cost and many other luxuries. It provides gigantic storage for data and faster computing to customers over the internet. It essentially shifts the database and application software to the large data centers, i.e., Cloud, where management of data and services may not be completely trustworthy. That is why companies are reluctant to deploy their business in the cloud even cloud computing offers a wide range of luxuries. Security of data in the cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. In the current era of digital world, the amount of sensitive data produced by many organizations is outpacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization’s end. A data owner pays for a desired level of security and must get some compensation in case of any misbehaviour committed by the CSP. On the other hand, the CSP needs a protection from any false accusations that may be claimed by the owner to get illegal compensations. In this paper, a cloud-based storage scheme is proposed that allows the data
Enabling Indirect Mutual Trust for Cloud Storage Systems

owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has two important features: (i) It allows the owner to outsource sensitive data to a CSP, and it ensures that only authorized users (i.e., those who have the right to access the owner’s file) receive the outsourced data. It enforces the access control of the outsourced data. (ii) It enables indirect mutual trust between the owner and the CSP.

References


- V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM
- M. Blaze, G. Bleumer, and M. Strauss, &quot;Divertible protocols and atomic proxy cryptography,&quot; in EUROCRYPT, 1998, pp. 127–144.

**Index Terms**

Computer Science  
Cloud Computing

**Keywords**

Access control  
Cloud computing  
Cloud service provider  
Data security  
Data outsourcing  
Mutual trust  
Storage-as-a-Service