Abstract

Storage-as-a-Service offered by cloud service suppliers (CSPs) could be a paid facility that permits organizations to source their sensitive information to be held on remote servers. During this paper, we tend to propose a cloud-based storage theme permits) the info owner to learn from the facilities offered by the CSP and enables indirect mutual trust between them. The planned theme has four vital features: (i) it permits the owner to source sensitive information to a CSP, and perform full block-level dynamic operations on the outsourced information, i.e., block modification, insertion, deletion, and append, (ii) it ensures that licensed users (i.e., those that have the proper to access the owner's file) receive the most recent version of the outsourced information, (iii) it allows indirect mutual trust between the owner and also the CSP, and (iv) it permits the owner to grant or revoke access to the outsourced information. We tend to discuss the protection problems with the planned theme. Besides, we tend to justify its performance through theoretical analysis and a model implementation on Amazon cloud platform to judge storage, communication, and computation overheads.

References


- G. Ateniese, K. Fu, M. Green, and S. Hohenberger, &quot;Improved proxy re-encryption schemes with applications to secure distributed storage,&quot; in NDSSS, 2005.
- V. Goyal, O. Pandey, A. Sahai, and B. Waters, &quot;Attribute-based encryption for fine-grained access control of encrypted data,&quot; in CCS &apos;06, 2006, pp. 89–98.


Index Terms

Computer Science  Distributed Systems

Keywords
Outsourcing information storage  dynamic atmosphere  mutual trust  access management