Enhancing Data Dynamics and Storage Security for Cloud Computing using Merkle Hash Tree and AES Algorithms

Abstract

With increase in the number of cloud users and the amount of sensitive data on cloud, security of cloud has become more important. Massively scalable data centers are provided by the cloud which can be accessed from anywhere and at anytime. Cloud computing allows users to store data and access it on demand thereby utilizing fewer resources in client system. However many malicious activities in cloud have accompanied the growth of cloud users. One of the greatest security challenges is storage security in cloud. It must make possible for users to store data without worrying about the need to verify its integrity. Thus, enabling public auditing for cloud storage is of critical importance so that users can restore to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. In this paper we make use of Public-Auditing. We propose a way in which the Merkle Hash Tree (MHT) used in a method called RSASS, is made dynamic by using the concept of relative index to compute the index of leaf node quickly and a dynamic operation scheme based on this tree structure for cloud storage. Also, instead of using RSA algorithm, we have made use of AES algorithm because AES requires less encryption-decryption time as well as less buffer space as compared to RSA algorithm. We thus propose a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data-confidentiality and security.
- Simar Preet Singh, and Raman Maini, "COMPARISON OF DATA ENCRYPTION ALGORITHMS", International Journal of Computer Science and Communication (IJCSC),
Enhancing Data Dynamics and Storage Security for Cloud Computing using Merkle Hash Tree and AES Algorithms


Index Terms

Computer Science  Security

Keywords

Advanced Encryption Standard  Cloud Computing  Data Integrity  Dynamics Data Operations
Merkle Hash Tree
Public Auditability
Storage Security.