World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:10, No:11, 2016

A Security Cloud Storage Scheme Based Accountable Key-Policy Attribute-Based Encryption without Key Escrow

Authors : Ming Lun Wang, Yan Wang, Ning Ruo Sun

Abstract : With the development of cloud computing, more and more users start to utilize the cloud storage service. However, there exist some issues: 1) cloud server steals the shared data, 2) sharers collude with the cloud server to steal the shared data, 3) cloud server tampers the shared data, 4) sharers and key generation center (KGC) conspire to steal the shared data. In this paper, we use advanced encryption standard (AES), hash algorithms, and accountable key-policy attribute-based encryption without key escrow (WOKE-AKP-ABE) to build a security cloud storage scheme. Moreover, the data are encrypted to protect the privacy. We use hash algorithms to prevent the cloud server from tampering the data uploaded to the cloud. Analysis results show that this scheme can resist conspired attacks.

Keywords : cloud storage security, sharing storage, attributes, Hash algorithm
Conference Title : ICSMCM 2016 : International Conference on Sustainable Manufacturing and Cloud Manufacturing
Conference Location : Paris, France
Conference Dates : November 21-22, 2016