Enhancing Confidentiality and Integrity in Cloud Computing using RSA Encryption Standard and MD5 Hashing Algorithm

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 181
Number 14
Year of Publication: 2018

Authors:
Katende Nicholas, Cheruiyot Wilson, Ann Muthoni Kibe

10.5120/ijca2018917788

Abstract

Cloud computing has revolutionized how services are rendered and used by some many people in the world like providing hardware, software and infrastructural storage to many users at any time. This is in terms of software as a service, platform as a service and infrastructure as a service, hence providing room for convinience to the cloud consumers to choose what they want presently and catering for their future needs since its elastic. With the company’s or individual’s data held by a third party that is the cloud provider, it brings out the security issues in respose to confidentiality, availability and integrity of the data at the cloud provider’s side. In this reseach paper solution is provided to maintain confidentiality of data and integrity of data at the cloud provider’s side. This framework contains RSA encryption standard and MD5 hashing alogorithm. In this solution data is encrypted using RSA which generates both public and private keys used in the encryption and the decryption then using MD5 to generate the hash value which is stored before the data is sent to the cloud provider. The hash value is checked upon retring of data from the cloud and if its still the same then the data was not modified or tempered with if else then the cloud provider has bleeched the contract. All these approaches
undergo through the following steps Encryption, Hashing, Data uploading on a cloud, Verification and Decryption.

References


Index Terms

Computer Science
Algorithms

Keywords

Cloud Computing, RSA, MD5