Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.401 – 407

RESEARCH ARTICLE

AES and DES Using Secure and Dynamic Data Storage in Cloud

[1]Prasanth SP, [2]Gowtham B

[1]Information Technology & V.S.B.Engineering College, Tamilnadu, India

[2]Information Technology & V.S.B.Engineering College, Tamilnadu, India

[1] gowthambruse@gmail.com; [2] prasanthitboss@gmail.com

Abstract---Cloud computing is the usage of both hardware and software as a service through the internet. When it comes to software as a service, it itself depends on the hardware to execute the instructions and hence can carry out the user's request. When the data is accessed through the internet in the cloud, security on the data being transferred will be the major concern. Since cloud computing is scalable and the servers are located in a distributed manner, security is still increasing higher. Users of the cloud can access the cloud from anywhere, from any device, so the device is also to be secured from security attacks. Data that are stored in the cloud is also in the risk of security attacks. To ensure security for the data that are stored in the cloud the Digital Signature Algorithm (DSA) is used to ensure the integrity of the file and Advanced Encryption Standard (AES) algorithm to encrypt and decrypt the files in the cloud storage. Public auditability can also be implemented by using the public key that is created during the file creation or editing process. Secure Hash Algorithm-1 hash function is used to create the message digest in the Digital Signature Algorithm, any other hash functions can be used in the place of SHA-1 like SHA-2, MD5 etc. Advance Encryption Standard Algorithm (AES) is used in the application to encrypt the data stored in the cloud, so that the files stored in the cloud will be free from all the users of the cloud including the administrator of the cloud and the files can be verified to check the integrity of the file.

Keywords— Security; data storage; dynamic data; public auditability

Full Text: http://www.ijcsmc.com/docs/papers/January2014/V3I1201479.pdf