International Conference on Latest Innovation in Engineering Science and Management
Buddha Institute of Technology, GIDA, Gorakhpur (UP)
30th - 31st March 2019 www.conferenceworld.in ISBN : 978-93-87793-80-4

Three-Stage Security in Data Storage at Cloud Server

Akash Dubey[1], Utkarsh Srivasatav[2], Risabh Pandey[3],Shailesh Patel[4]

[1,2,3]Student,[4]Assistant Professor, CSE, Institute of Technology & Management,

GIDA, Gorakhpur, U.P.

Abstract

Cloud Computing is offering the data storage at cloud server and user can access these data even on move. Anytime anywhere computing is now a norm for user. Security of stored data at remote server has been always an issue which has drawn the attentions of many researchers from both places: industry and academics. Symmetric and asymmetric cryptographic algorithms can be used to encrypt the data. In symmetric encryption, we use a key for both purposes: encryption and decryption. In asymmetric encryption public key is used for encryption and private key is used for decryption. However cryptanalyst can decrypt the data by spending considerable amount of time. There exists always a doubt about the security of data which is kept on remote server under different policies. Steganography is a process of hiding data in some other files. The source file may be an image file, an audio file or even a video file. In the proposed scheme, authors are suggesting to use two servers and a local machine for data storage. The plaintext is first split into three parts. For two parts (the parts of data to be stored on remote server), we can use any encryption techniques either symmetric or asymmetric keys encryption. Even we can use symmetric approach for one part and asymmetric approach for other part also. The resident part, that part of data which is kept on local machine, along with the metadata (include IP addresses of remote servers and keys) are stored at the local machine. Authors further suggest using Steganography where plaintext is hidden in a source file by encrypting the plaintext with a symmetric key. In this we observe that entire data is fragmented into various parts and after encryption these parts are being distributed over many servers. Now in decrypting the data the three machines have to participate and as metadata is at local machine it increases the security of data.

Keywords: Cloud Computing, Symmetric Encryption Techniques, Asymmetric Encryption Technique, Cryptanalyst, Steganography, Plaintext.