A HYBRID SECURITY FRAMEWORK FOR CLOUD COMPUTING

Basnayaka B.M.B.D.B.[1*] and Jayasena K.P.N.[1]
[1]Department of Computing & Information Systems, Sabaragamuwa University of Sri Lanka, Sri Lanka
[*]barathabasnayaka@gmail.com

Cloud computing describes the pool of shared resources that can be accessed remotely. Cloud security plays an important role in cloud computing. Data encryption is the technique of cloud security that converts data into a distinct form or code so that it can only be read by people with access to a secret key or password, In this research we proposed hybrid security framework . In this framework we used both cloud encryption algorithms and sorting algorithms. In the first phase we used sorting algorithms such as insertion sort, quick sort and merge sort algorithms based on the volume of elements input to secure cloud data. According to the performance graph the merge sort showed the least time consuming. Generally, standard 3DES, AES2 and RSA algorithms are used for text message transmission in encryption or decryption techniques In the second phase, we analyzed the effectiveness of 3DES, RSA and AES2 encryption algorithms for the input of different data sizes. AES2 showed the lowest time at each moment. Based on the AES2 algorithm and the Merge sort algorithm the new hybrid algorithm frame work is proposed. This frame work can be applied to enhance the cloud information safety.

Keywords: *AES2, Cloud security, Encryption , Hybrid algorithm, Merge sort*