Abstract

Introducing Cloud computing to the globe has changed many conceptual and infrastructural bases for today’s and tomorrow’s computing. It has made the global thinking migrates rapidly towards cloud based architecture. Clouds bring out a variety of benefits including computing resources configurability, cost controllability, sustainability, mobility and service flexibility. However, the new concepts that clouds introduce such as outsourcing, multi-tenancy, and resource sharing create new challenges and raise a broad range of security and privacy issues. Cryptography is the art-of-science of protecting data privacy by converting it to unreadable format using standard mathematical techniques. This paper provides a comprehensive study for eight of the most common symmetric cryptographic algorithms, namely, DES, 3DES, Blowfish, Twofish, RC2, RC5, RC6 and AES. A comparative analysis based on the structure of the algorithm, encryption and decryption times, throughput and memory utilization has been performed to examine the performance of each algorithm.

Index Terms
Keywords

Cloud Computing, DES, 3DES, Blowfish, Twofish, RC2, RC5, RC6, AES