Abstract

Advanced Encryption Standard (AES) is one of the most popular encryption algorithms. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a Mix Column. In this paper the parallel implementation of AES cryptography algorithm is evaluated and compared in terms of running time, speed up and parallel efficiency. The parallel implementation of AES is implemented using message passing interface (MPI) library, and the results have been conducted using IMAN1 Supercomputer. The experimental results show that the run time of AES algorithm is decreased as the number of processors is increased. Moreover, the speedup for the data size of 16, 32, 64, 128, 256, and 1024-KB is increased when the number of processors is equal to 2, 4, 8, and 16.

References

Performance Evaluation of AES algorithm on Supercomputer IMAN1


Index Terms

Computer Science
Algorithms
Keywords

AES Encryption, MPI, Supercomputer, Parallel Computing.