Performance Improvement of Double Data Encryption Standard Algorithm using Parallel Computation

International Journal of Computer Applications Foundation of Computer Science (FCS), NY, USA

Volume 179 - Number 25

Year of Publication: 2018

Authors:

Amaal Shorman, Mohammad Qatawneh

10.5120/ijca2018916527

Abstract

Most of the applications require information security on network. Cryptography is a method to provide information confidentiality, authenticity, and integrity. Double Data Encryption Standard algorithm (2DES) is used by several applications to protect their information security. However, current implementations of 2DES algorithm suffer from large execution time. Parallel computation is a promising technique to improve the performance of an algorithm. Divide and conquer method is mainly used in parallel computation to solve the algorithm in parallel by partitioning a task into sub-task and allocating them to available processors. In this paper, sequential and parallel 2DES are evaluated and compared in terms of the running time and the speedup. The parallel 2DES algorithm is implemented using Message Passing Interface (MPI) library, and the results have been conducted using IMAN1 supercomputer. Results showed that the run time of parallel 2DES algorithm outperforms the sequential one. Moreover, on a large number of processors, parallel 2DES achieves better parallel efficiency. Therefore, the parallel 2DES provides much better performance in term of execution time than the serial ones and would be useful to apply it to encrypt and decrypt multimedia.
References

Index Terms

Computer Science  Algorithms

Keywords

Cryptography, Double Data Encryption Standard, MPI, Parallel Computation, Supercomputer