Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.615 – 622

RESEARCH ARTICLE

A Novel Security Technique in Message Passing Interface Systems

UDHAYASHANKAR.S[1], Dr. K.P. KALIYAMURTHIE[2], MATHIVILASINI.S[3]

[1]Department of information Technology, Bharath University, India
[2]Department of information Technology, Bharath University, India
[3]Assistant Professor, Ethiraj College for Women, India

Abstract— *In the concept of Message Passing Interface (MPI) chatting and file transmission the decryption part will be done automatically. Here three types of keys are used; they are public, private and secret key. Keys are displayed to the destination only if they accept the request or else displaying of key is not possible in the destination side and also it won't give or establish the Connection. In largely spread clusters, computing nodes are naturally deployed in a variety of computing sites. The Information processed in a spread cluster is communal among a group of distributed processes or client by high-quality of messages passing protocols (e.g. message passing interface - MPI) running on the Internet. Because of the open available nature of the Internet, data encryption for these large-scale distributed clusters becomes a non-trivial and challenging problem. We improved the security of the MPI protocol by encrypting and decrypting messages sent and received among computing nodes. We are listening carefully on MPI rather than more protocols because MPI is one of the most accepted communication protocols for cluster computing environments. From among a multiple of MPI implementations, we selected MPICH2 developed by the Argonne National Laboratory. Design goal of MPICH2 - a commonly use MPI implementation - is to join portability with high presentation. we gives a security enhanced MPI-library with the standard MPI interface, data communications of a conservative MPI program can be secured without converting the program into the corresponding secure report. We included encryption algorithms into the MPICH2 library so that data in secret of MPI applications could be readily preserved without require modifying the source codes of the MPI applications. This system use Sandia Micro Benchmark and Intel MPI Benchmarks to evaluate and compared the performance of original MPICH2 and Enhanced Security MPICH2. According to the performance estimation, ES-MPICH2 provides protected Message Passing Interface by give up sensible system performance.*

Key Terms: - Secret key; Encryption; MPI; Parallel Computing; Cryptosystem

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I42013129.pdf