"A Survey On Message Passing Interface With Enhancement Security For Untrusted Network"

Sharanabasava Potaraj
M.Tech Student
Department of CSE
VTU, BNM Institute of Technology
Bangalore, India

Girish G. S
Associate Professor
Department of ISE
VTU, BNM Institute of Technology
Bangalore, India

Abstract— **An increasing number of clusters are connected to each other by internet, which creates a potential threat for security over unsecured network. This paper addresses this kind of security issue. In this paper, to solve this security issue we are concentrating on message passing interface(MPI). Which is the most popular protocol for parallel computation. We have integrated symmetric and asymmetric algorithms with encryption/decryption in to the MPICH2 library with MPI standard. The library performs key generation, key exchange and data transfer without using any additional codes. The overhead incurred by the confidentiality services in ES-MPICH2 is marginal for small messages. The security overhead in ES-MPICH2 becomes more pronounced with larger messages.**

Keywords-Symmetric algorithm, Asymmetric algorithm, Encryption, Decryption, TCP/IP protocol, MPICH2(Message Passing Interface Channel-2), OS(Output stream), IS(Input stream).

1.INTRODUCTION

Since there is a fast improvement of the internet, an increasing number of organizations and companies are connecting their computing systems over public network for the better accessibility. Those computing nodes connecting to the public network can be accessed by anyone from anywhere. Data processed in a public network is accessed among a group of users by the virtue of message passing protocols (e.g., message passing interface-MPI) or secured data transmitted among computing nodes[1].

Maintaining data security in a message passing over an unsecured network is critical for a wide spectrum of security-aware MPI applications, because unauthorized access to the security-sensitive messages by unsecured network can lead to serious security treats. Therefore, it is necessary to protect confidentiality of messages exchanged among a group of trusted processes.

It is a difficult and challenging problem to offer security services for wide scale shared computing nodes, since there is an open accessible nature of the networks. To handle this issue, we enhanced the security of the MPI protocol by encrypting and decrypting messages sent and received among nodes connecting to the public network.

In this paper, we concentrated on MPI protocol, since MPI is one of the well known communication protocols for cluster computing environments. More Number of scientific and other applications are running on public network were developed using the MPI protocol.

Over most of MPI design, we have chosen MPICH2 developed by the Argonne National Laboratory[2]. The design goal of MPICH2 is to combine portability with high performance. We incorporated encryption algorithms into the MPICH2 library.

Therefore, the data confidentiality of MPI can be readily preserved without the change of the source codes of the MPI applications. The communications of a conventional MPI program can be secured without altering the corresponding version, since we provide a security enhanced MPI-library with the standard MPI interface.

2.RELATED WORK

There are few possible ways to improving security of MPI applications.

In first approach, the programmers can add source code to address the issue of message confidentiality. For example, the programmers may rely on external libraries (e.g., SEAL[3] and Nexus[4]) to implement secure applications. Such an application-level security approach not only makes the MPI applications error prone, but also reduces the portability and flexibility of the MPI applications.

In the second approach, the MPI interface can be extended in the way that new security-aware APIs are designed and implemented (see, for example, MPISecI/O[5]). This MPI interface level solution enables programmers to write secure MPI applications with minimal changes to the interface. Although the second approach is better than the first one, this MPI interface level solution typically requires an extra code to deal with data confidentiality.

The third approach a channel level solution is proposed in this study to address the drawbacks of the above two approaches. Our channel level solution aims at providing message confidentiality in a communication channel that implements the channel Interface 3 (CH3) in MPICH2. The standard MPI mechanism called MPICH2 to offer data confidentiality for secure network communications in message passing environments[6].

In the present system the socket is connected from input stream of server to the out put stream of the client and input stream of client to the output stream of server. The data which is to be sent at the input stream of server is reached to the out put stream of client and vice versa. There is no security for the data. The data transmission is happened through the port numbers. The present system does not provide any security to TCP/IP layer. Since it does not incorporated symmetric and asymmetric encryption/decryption algorithm. The TCP/IP channel simply forward the data from server to client. Hence it is prone to threats.

The existing system of a data exchange between server and destination is shown in the figure 1.

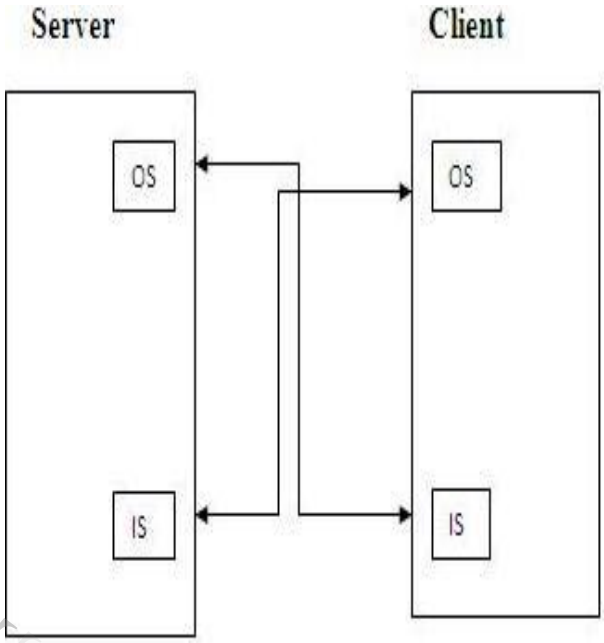

Fig 1. Block diagram of Existing System

3.PROPOSED SYSTEM

In this work we are implementing MPI (Message Passing Interface) to offer data confidentiality for secure network communications in message passing environments. Our proposed security technique incorporated in the MPICH library can be very useful for protecting data transmitted in open networks like the Internet.

The MPICH mechanism allows application programmers to easily write secure MPI applications without additional code for data confidentiality protection. We seek a channel level solution in which encryption and decryption functions are included into the MPICH library. Our MPICH maintains a standard MPI interface to exchange messages while preserving data confidentiality.

The existing system does not provide security for the TCP/IP protocol in socket level. In the proposed system we are binding TCP/IP link by using symmetric and asymmetric encryption/decryption algoritmhs. The MPI API's are used as interface to transfer the data between source and destinstion as shown in the figure 2.

The symmetric algorithm uses three types of algorithms such as AES, DES and 3DES. The user can select any of the algorithm for encryption. The data is encrypted in the source side and transferred the data in to cipher text and again in the receiver side it is decrypted into the plain text by using the same algorithm.

The symmetric algorithm uses three types of algorithms such as AES, DES and 3DES. The user can select any of the algorithm for encryption. The data is encrypted in the sorce side and transferred the data in to cipher text and again in the receiver side it is decrypted into the plain text by using the same algorithm. The symmetric algorithm provides both private and public key.

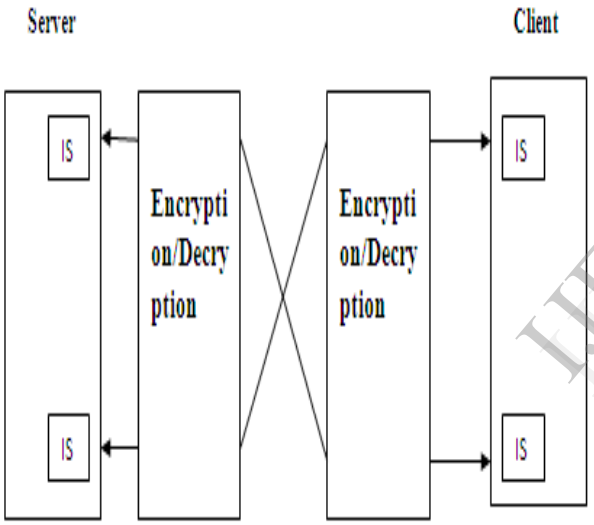

Fig 2. Block diagram of Proposed System

If the user wish to send the data by using the asymmetric algorithm, the system provides asymmetric algorithms too. The user can use asymmetric algorithms such as RSA algorithm and RSA with padding for encryption and decryption. The asymmetric algorithm provides only secrete key rather than private and public key.

The symmetric and asymmetric algorithms such as AES, DES, 3DES, RSA and RSA with padding are so fexible so these algorithms can be used as general purpose. This is shown in the figure 3.

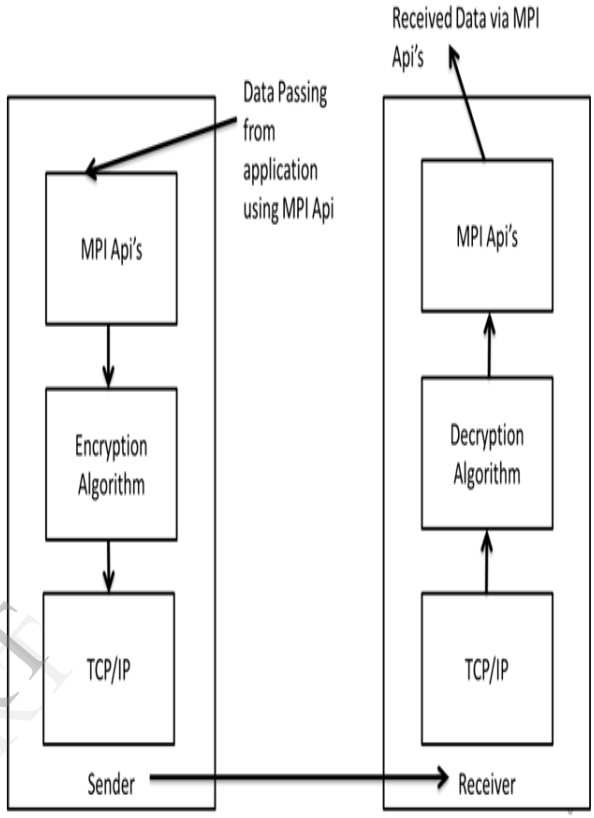

Fig 3. System Overview.

3.1 System Overview:

In this paper, we are trying to build a message passing interface that encapsulates the unsecured TPC/IP Layer with a secure layer that involves both symmetric and asymmetric crypto security to TCP/IP Protocol.

The implemented MPICH2 frame work provides an API's that enables application programmers to selectively choose any crypto graphical algorithm and symmetric key in MPICH2. This feature makes it possible for programmers to easily and fully control the security services incorporated in the MPICH library. To demonstrate this feature, we have incorporated AES, DES Symmetric Key Encryption/Decryption and RSA Asymmetric Encryption/Decryption in MPICH2.

We Build API's that is free from key generation, key exchange and provides both symmetric/asymmetric encryption/decryption. This allows users to readily include these API's for secure message passing system.

To demonstrate the working of these API's, we can show the library that adds a security layer over TCP/IP API's and to show the working of the library we build a secure file transfer application that include hashing for integrity. The application demonstrates the file transfer that includes both symmetric cryptography and asymmetric cryptography. We also enhance of work to include hashing algorithm for data corruption check while transfer. The System provides all these feature via MPI.

4. CONCLUSION

The existing methode does not provide security in the socket level. It requires many modules to provide the security. That is, it requires different modules for each operation such as key generation, key exchange and data ransfer. The present present system doesnot provide encryption and decryption. In the proposed system, we have built the library functions. Which performs enccryption, decryption, key generation, key exchange and data transfer only by using library functions through API's. API's are the single line of code which performs the all the above operations using library functions. In this way we are securing the data in socket level. In the present paper we have concentrated only on TCP/IP link. It can be extended to the UDP also. And any one can build further libraries for other features by using our library functions. Those are the aspects of future enhancement.

REFERENCES

[1] Xiaojun Ruan, Qing Yang, Mohammed I. Alghamdi, Shu Yin, and Xiao Qin, "ES-MPICH2: A Message Passing Interface," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 3, May/June 2012

[2] W. Gropp, E. Lusk, N. Doss, and A. Skjellum, "A High-Performance, Portable Implementation of the Mpi Message Passing Interface Standard,"Parallel Computing, vol. 22, no. 6, pp. 789-828, 1996.

[3] D.S. Wong, H.H. Fuentes, and A.H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices,"Proc. 17th Ann. Computer Security Applications Conf. (ACSAC), pp. 92-101, 2001.

[4] I. Foster, N.T. Karonis, C. Kesselman, G. Koenig, and S.Tuecke, "A Secure Communications Infrastructure for High-Performance Distributed Computing,"Proc. IEEE Sixth Symp. High Performance Distributed Computing,pp. 125-136, 1996.

[5] R. Grabner, F. Mietke, and W. Rehm, "Implementing an mpich-2 Channel Device over Vapi on Infiniband,"Proc. 18th Int'l Parallel and Distributed Processing Symp.,p. 184, Apr. 2004.

[6] M. Lee and E.J. Kim, "A Comprehensive Framework for Enhancing Security in Infiniband Architecture," IEEE Trans. Parallel Distributed Systems,vol. 18, no. 10, pp. 1393-1406, Oct. 2007.