International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

An Enhanced Security Technique with Authentication for Mobile and Pervasive Computing

Stud. S. Gobhika [#1] Prof. A.T. Ravi [#2]

[#1 2] *Department of Computer Science, SSM College of Engineering, Komarapalayam, Namakkal, Tamilnadu, India.*
[1] gobhikas08@gmail.com [2] atravin@gmail.com

***Abstract*— The main objective is to develop a Message Passing Interface (MPI) implementation: to preserve confidentiality of messages communicated among nodes of clusters in an unprotected network. The message passing interface (MPI) is a standardized means of exchanging messages between multiple computers running a parallel program across distributed memory. In this technique public, private and secret keys are used. Keys are displayed to the receiver only if they accept the request or else displaying of key is not possible in the receiver side and also it won't 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 environment of the Internet, providing authentication for large-scale distributed clusters becomes a non-trivial and challenging problem. In this paper, the security of the MPI protocol has improved by encrypting and decrypting messages sent and received among computing nodes using MD5 algorithm.**

Index Terms— Authentication, unconditional security, computational security, universal hash-function families, pervasive computing. ***(Key words)***

I. INTRODUCTION

Mobile computing is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away.

Otherwise Mobile computing is a generic term used to refer to a variety of devices that allow people to access data and information from where ever they are .It has several advantages such as Improve business productivity by streamlining interaction and taking advantage of immediate access, Reduce business operations costs by increasing supply chain visibility, optimizing logistics and accelerating processes ,Strengthen customer relationships by creating more opportunities to connect, providing information at their fingertips when they need it most and Gain competitive advantage by creating brand differentiation and expanding customer experience Increase work force effectiveness and capability by providing on-the-go access, And also improve business cycle processes by redesigning workflow to utilize mobile devices that interface with legacy applications.

To improve the efficiency of communication between the users, a technique of message passing interface is used. It is especially used to exchanging messages between multiple computers running a parallel program across distributed memory.MPI has been implemented for almost every distributed memory architecture) and speed (because each implementation is in principle optimized for the hardware on which it runs). MPI's goals are high performance, scalability, and portability.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

II. RELATED WORK

There are well-known techniques for message authentication [1],[2],[3],[4],[5],[6],[7] using universal hash functions. This approach seems very promising, as it provides schemes that are both efficient and provably secure under reasonable assumptions. It reports on the results of empirical performance tests that demonstrate that these schemes are competitive with other commonly employed schemes whose security is less well-established. To improve the authentication and security between the users MAC algorithm is used. but it results in redundancy problem. Another emerging technology is Radio frequency identification (RFID) which brings enormous productivity benefits in applications where objects have to be identified automatically. RFID tags must be equipped with a message authentication mechanism. Another application that is becoming increasingly important is the deployment of body sensor networks. In such applications, small sensors can be embedded in the patient's body to report some vital signs. Concrete security analyses of methods to encrypt using a block cipher, including the most popular encryption method, CBC.

It results in mathematical computation problem. Again, in some applications the confidentiality and integrity of such reported messages can be important. Then the message to be authenticated also encrypted, with any secure encryption algorithm, to append a short random string to be used in the authentication process. But it cannot preserve the data confidentiality in a message passing environment over an un-trusted network.

III. PROBLEM FORMATION

To preserve the confidentiality and integrity of messages, a block cipher based encryption algorithm is used to improve the computational efficiency. This might cause some problems in generating random strings. .So, another technique named Mac algorithm is used to send messages authentically but results in waste of resources as well problem in providing confidentiality in large scale distributed clusters.

IV. MPI PROTOCOL

MPICH is one of the most popular MPI implementations developed at the Argonne National Laboratory. The early MPICH version supports the MPI-1 standard. MPICH2 – a successor of MPICH - not only provides support for the MPI-1 standard, but also facilitates the new MPI-2 standard, which specifies functionalities like one-sided communication, dynamic process management, and MPI I/O.

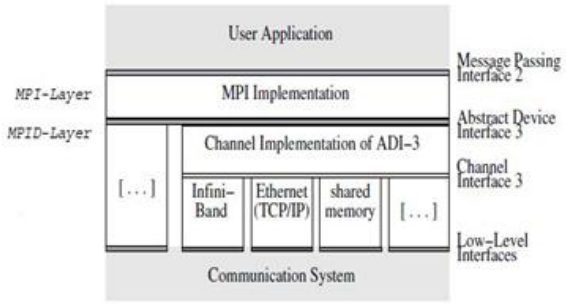

Fig. 1 Process flow of MPI system.

Fig.1 shows the hierarchical structure of the MPICH2 implementation, where there are four distinct layers of interfaces to make the MPICH2 design portable and flexible.

The four layers, from top to bottom, are the message passing interface 2 (MPI-2), the abstract device interface (ADI3), the channel interface (CH3), and the low-level interface. ADI3 - the third generation of the abstract device interface - in the hierarchical structure (in Fig. 1) allows MPICH2 to be easily ported from one platform to another. Since it is non-trivial to implement ADI3 as a full-featured abstract device interface with many functions, the CH3 layer simply implements a dozen functions in ADI3.

The TCP socket Channel, the shared memory access (SHMEM) channel, and the remote direct memory access (RDMA) channel are all implemented in the layer of CH3 to facilitate the ease of porting MPICH2 on various platforms. Unlike an ADI3 device, a channel is easy to be implemented since one only has to implement a dozen functions relevant for

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

with the channel interface. To improve the security of MPICH2, we implemented a standard MPI mechanism or ES-MPICH2 to offer data confidentiality services in message passing environments.

V. PROPOSED STRATEGIES

The proposed system solves the challenging problem of confidentiality services for large-scale distributed clusters, by enhancing the security of the MPI protocol by encrypting and decrypting messages sent and received among computing nodes.

The proposed system focuses on MPI rather than other protocols, because MPI is one of the most popular communication protocols for cluster computing environments. Among a variety of MPI implementations, we picked MPICH2 developed by the Argonne National Laboratory. The design goal of MPICH2, a widely used MPI implementation is to combine portability with high performance. We integrated encryption algorithms into the MPICH2 library. Thus, data confidentiality of MPI applications can be readily preserved without a need to change the source codes of the MPI applications.[8] MPICH2 is one of the most popular implementations of MPI. It is used as the foundation for the vast majority of MPI implementations including IBM MPI (for Blue Gene), Intel MPI, Cray MPI, Microsoft MPI, Myricom MPI, OSU MVAPICH/MVAPICH2, and many others.

To verify the integrity of the data, message digest algorithm (MD5) is used. It is widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function, MD4. The source code in RFC 1321 contains a "by attribution" RSA license.

The requirements for a good cryptographic hash function are stronger than those in many other applications (error correction and audio identification not included). For this reason, cryptographic hash functions make good stock hash functions--even functions whose cryptographic security is compromised, such as MD5 . MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}

.VI. IMPLEMENTATION AND RESULTS

A. Constructing message passing environments.

In this module, we construct the message passing environment to propose our efficient message passing interface using MD5. We implemented this module, from a standard MPI mechanism called ES-MPICH2 to offer data confidentiality for secure network communications in message passing environments. Our proposed security technique incorporated in the MPICH2 library can be very useful for protecting data transmitted in open networks like the Internet.

B. Message passing implementation protocol module

In this module we develop a Message Passing Interface (MPI) protocol which is a standardized and portable message-passing system designed by a group of researchers from academia and industry to function on a wide variety of parallel computers. The standard defines the syntax and semantics of a core of library routines useful to a wide range of users writing portable message-passing programs. The MPI interface is meant to provide essential virtual topology, synchronization, and communication functionality between a set of processes (that have been mapped to nodes/servers/computer instances) in a language-independent way, with language-specific syntax (bindings), plus a few language-specific features. MPI programs always work with processes, but programmers commonly refer to the processes as processors. Typically, for maximum performance, each CPU (or core in a multi-core

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

machine) will be assigned just a single process. This assignment happens at runtime through the agent that starts the MPI program, normally called mpirun or mpiexec.Fig.2 shows the secured data transmitted in the network.

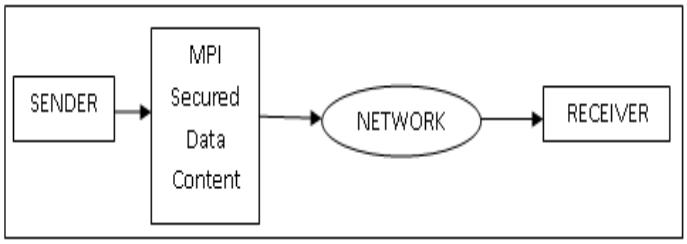

Fig: 2.Message Passing Technique

C. MD5 implementation module

In this module we implement, Message Digest 5 algorithm (MD5) is an approach, widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

D. Integrity checking evaluation module.

In this module we implement the integrity checking and evaluation process, while you can count on data integrity being addressed through multiple mechanisms for data.Fig.3 shows how we address the data integrity issues that require attention but occur after the data is sent. After data has been sent to destination, confirming the integrity of data is sent to destination only. Algorithm 1 represents how the operations are performed by MD5[9].

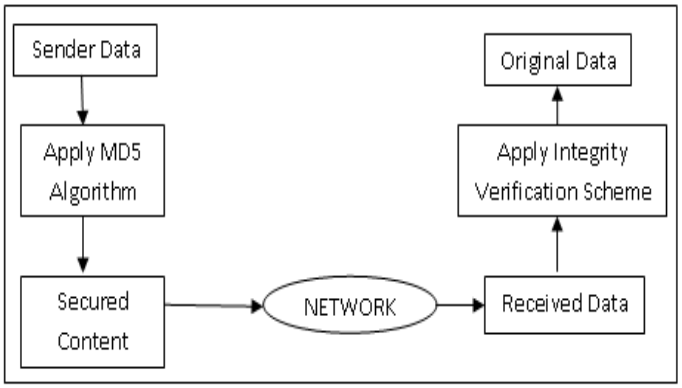

Fig: 3. Integrity checking evaluation module.

Algorithm 1 -MD5

1: // M= (Y0, Y1,……., Yn-1), Message to hash , after Padding
// Each Yi is a 32-bit word and N is a multiple of 16
MD5 (M)
//initialize (A, B, C,D) = IV
(A,B,C,D) = (0x67452301, 0xefab89 , 0x98badcfe , Ox10325476)
2: For i=0 to N/16 -1
// Copy block I to X
3: Xj = Y16i+j for j = 0 to 15
// Copy X to W
4: Wj = Xσ(j) , for j = 0 to 63
// initialize Q
5: (Q-4 , Q-3 , Q-2 , Q-1) = (A , D , C , B)
// Rounds 0 , 1 , 2 and 3
Round0(Q , W) Round1(Q , W) Round2(Q , W) Round3 (Q , W)
6: // Each addition is modulo 232
(A , B , C , D)=(Q60 + Q-4 , Q63 + Q-1 , Q62 + Q-1 , Q61 + Q-3)
7: next i
8: return A,B,C,D
9: end MD5
10: Round0(Q , W)
11: //steps 0 through 15 for i = 0 to 15Qi = Qi-1 + ((Qi-4 + F(Qi-1 , Qi-2 , Qi-3) + Wi+Ki) <<< si)
12: **next i**
13: end round()

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

F. Results

Finally this algorithm gives better result in securing messages in the large cluster environment. The process of exchanging message too faster as well more secure. Compare to other techniques this is more efficient in exchanging messages in the open environment more secure and also it verifies the integrity of the data. Each and every time it verifies the integrity of the user in the network. Unauthorized users cannot access the messages in the network.

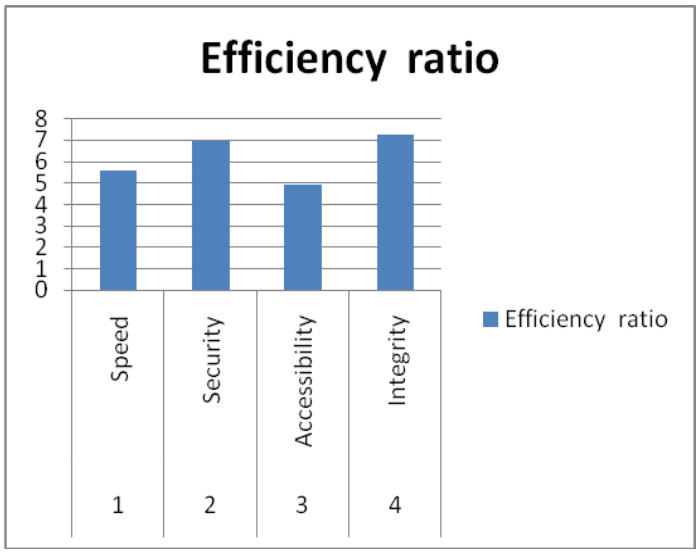

Fig. 4 Testing Strategies in ratio

TABLE I
Testing Efficiency Ratio

S.No	Testing	Efficiency ratio
1	Speed	5.6
2	Security	7.0
3	Accessibility	4.93
4	Integrity	7.26

VII. CONCLUSION AND FUTUTRE WORK

In this study, ES-MPICH2 framework is implemented, which is based on MPICH2. ES-MPICH2 is a secure, compatible, and portable implementation of the message passing interface standard. Compared with the original version of MPICH2, ES-MPICH2 preserves message confidentiality in MPI applications by integrating encryption techniques like MD5 into the MPICH2 library.MD5 offers confidentiality and integrity of the message. It produces better efficiency in transmitting messages in the large network.It will be more efficient in future.

VIII. REFERENCES

[1] L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.

[2] V. Shoup, "On Fast and Provably Secure Message Authentication Based on Universal Hashing," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 313-328, 1996.

[3] B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," IEEE Trans. Computers, 2012.

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '04), pp. 357-370, 2004.

[5] C. Tan, H. Wang, S. Zhong, and Q. Li, "Body Sensor Network Security: An Identity-Based Cryptography Approach," Proc. First ACM Conf. Wireless Network Security, pp. 148-153, 2008.

[6]M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. 38th Ann. Symp. Foundation of Computer Science (FOCS '97), pp. 394-403, 1997.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 4, 2015. ISSN: 2348-6600
Reference ID: IJCS-088 PAGE NO: 504-509.

[7] B. Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," Proc. 12th Int'l Conf. Information and Comm. Security (ICICS '10), 2010.

[8] D.Gangadhar Rao, Balusa Anil Kumar," Enhanced Security Mechanisms in MPI as ES-MPICH2",vol 1(IJCSDT '4) 2013.

[9] Piyush Gupta, Sandeep Kumar," A Comparative Analysis of SHA and MD5Algorithm Vol. 5 (3) ,, 4492-4495,2014.