Volume 1, No. 4, Nov-Dec 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secured Information Transfer in Networked Multi-Party Computation

Hemant Pal
Department of Computer Science
Shri Vaishnav Institute of Management
Indore (M.P.) ,India
hemantpal.scs@gmail.com

Abstract: In the current era of globalization for communication and computation we all are connected to one another directly or indirectly with the help of the Internet or intranet. One of the most challenging tasks is to protect confidential data the network. Private data should not be leaked to unauthorized agents. All people are worried about their credit card details, passwords or any other kind of private data before sending it from one machine to another. Current information security policies try to assurance that the end-to-end delivery of our personal data is safe. It means when we are working in client–server environment, our personal information should be delivered from client to the target server only. Traditional security mechanisms such as access control, firewall, antivirus, and encryption address the enforcement of information security policies. In this paper, we proposed a novel security mechanism that will make sure that the private data of client will not be hacked before reaching the server.

***Keywords*:** Information Security, Confidentiality, Noninterference, Dynamic IP addressing.

I. INTRODUCTION

One of the most challenging tasks is to protect confidential data over the network. There is little assurance that current computing systems protect data confidentiality, integrity, and are safe from hacker's eyes. In this paper, we discuss a security mechanism which takes an attempt to stop hacking using the concept of dynamic IP addressing for maintaining confidentiality of data.

Banks, Railways, Military, Medical, Engineering, Automobiles and financial information systems; as well as web-based services such as e-mail, and online shopping transactions are applications that always worried about their personal data. In these computations only client and server are present though the security of data is a doubtful case.

Here we propose the data security mechanism with a view towards the Secure Multiparty Computation (SMC) where many parties send and compute some function of their individual but private inputs. If we consider the case of SMC then in this scenario the security of data will be much more challenging. We use Dynamic Host Configuration Protocol (DHCP) for changing the IP address of the hosts involved in the process of computation.

II. CURRENT SECURITY STANDARDS

In current scenario the security and protection of confidential data are in the hands of firewall, access control, and cryptosystem. All these policies fall short in particular cases. It is necessary to analyze how these standard security mechanisms fall short.

In *access control mechanism* certain user name and password is required in order to open the file containing confidential data. Access control checks user name and password; and if they are correct then it opens the file. Once the file is opened *it takes no action for the propagation of data from one machine to another*. The accessing program may, through error or intentionally transmit the information to the hacker. All the programs in a large computing system are not trustworthy. To ensure that information is delivered to the correct server, it is necessary to analyze how information flows [1] within the using program and also how information is transferred from one machine to another.

Noninterference policy [2] states that confidential data i.e. private data should not interfere with public data so as to make our private data secured from malicious program. *Noninterference* takes care of data on the machine on which the program is installed; it does nothing about how information will flow from client to server. It mainly focuses on how information will flow within the program.

Firewall is used to restrict the use of un-authorized sites and undesired contents. Antivirus software tries to find out certain patterns in the data. Firewall and antivirus software have a little impact on the action of hacker.

Intrusion Detection System (IDS) [3] uses the concept of artificial intelligence. Based on the past experience it tries to find out network jam and unauthorized access to the server. Sometimes IDS are also called intelligent firewalls. If IDS identify the hacker then only certain action can be taken to protect our data on server. It also has no impact how information flows between client and server. IDS fall short if data is hacked before reaching the server.

III. PROPOSED WORK

In Multi-Party computation [4] many organizations participate to perform certain task. It is necessary to protect the channel secured so that the data of any organizations should not be hacked before reaching the expected server.

In this paper we are going to show a new Information security policy that takes an attempt to secure the data over intranet. Intranet is a private computer network that uses internet protocol technologies to securely share information within that organization.

To implement the proposed security policy we need at least 4 machines in which one machine acts as a client, one machine will act as a server and the remaining two machines will work on the be-half of the server.

It is assumed that all the 4 machines are inter connected. Let it "**A**" represents the client and "**B**" represents the server.

Let IP address of *A* is 123.123.123.123 and of *B* is 126.126.126.126 . Let *A* is connected with *B* and wants to sent his private data to *B* for further processing. *B* randomly take 2 machines to process the data of *A* as shown in Fig 1.

Let it IP of the two randomly selected machines B1 and B2 are 124.124.124.124 and 125.125.125.125 respectively. The IP of A and B are static while IP of those 2 randomly selected machines are dynamic in nature. Dynamic IP addressing is done by DHCP. The transmission of data from *A* to B will takes place as follows.

Data on the client machine *A* will be segmented into 4 numbers (let).

Now *B* will redirect its request to *B1, so A* is connected with *B1*. B1 send the request to *A* that send the first segment of data. As soon as B1 receives data , *B1* inform to *B* that data is received. Now under the guidance of *B*; *B1* will copy its data and other details regarding connection to *B2*.

Now a message will be dropped by *B2* to *A* that send second segment of data. At this time *A* is connected with *B2*.

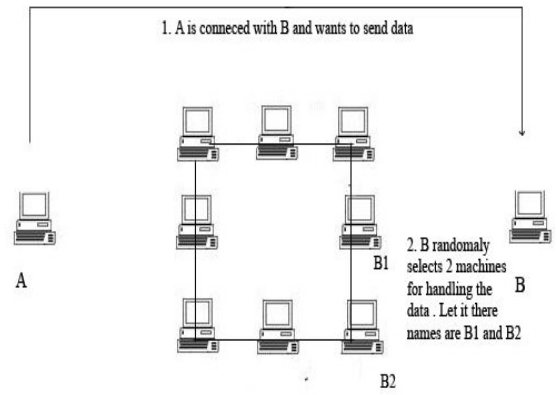

Fig. 1 Architecture of secured information transfer over netwok multi-party computation

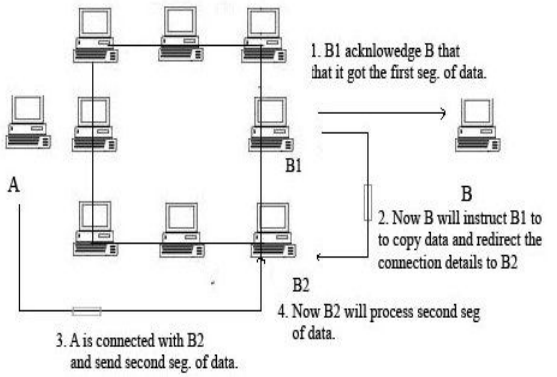

Fig. 2 Implementation of secured information transfer over netwok multi-party computation

Now at this time the IP of the *B1* will be changed dynamically using DHCP. Let the new IP of *B1* is 129. 127. 127. 127. and this IP will be sent to *B* for handling further actions. *B* will inform to *B2* that after taking second segment forward requests to *B1*. As soon as *B2* gets data it will copy its data and other details regarding connection to *B1*as shown in the Fig 2.

Now a message will be dropped by *B1* to *A* that send third segment of data and this process will be continued till all the segments are sent.

At last all the segments are collected by *B* and further transactions are done. In such manner proposed security policy protects confidential data.

In our proposed security policy dynamic IP addressing is done by DHCP. It may possible at any time two machines have same IP address; this is known as IP addressing conflict. It can be resolved by using different methods mentioned in [5] approaches for Resolving Dynamic IP addressing.

IV. MATHEMATICAL ANALYSIS

If any hacker wants to hack client private data then it will need to identify the IP address of those two machines. Let it we have IP in the range 123.123.123.1, 123.123.123.2, 123.123.123.100 . i.e we have 100 IP address then to find IP address of those 2 machines in pair will be calculated as follows:

Number of paired cases will be given by (123.123.123.1,123.123.123.2), (123.123.123.1,123.123.123.3), (123.123.123.1,123.123.123.4),…,(123.123.123.100,123.123.123.99) i.e. the total number of cases are 100*99=9900. Then to find out those 2 machines in pair will be given by 1/9900 ≈0.0001.

Hence form the above discussion it is found that if we goes on increasing the number IP address of machines between the client and server then the probability to find out those twos machines in pair will be much very less.

V. CONCLUSION

We have discussed that standard security practices are not capable of enforcing end-to-end confidentiality policies; mechanisms such as access control, encryption, firewalls and antivirus scanning do not address the fundamental problem: tracking the flow of information in computing systems is necessary to protect our confidential data from hacker's eye.

On the other hand, there is clear evidence of benefits provided by our proposed approach. It is verified by the mathematical analysis that the security provided by our solution is better and will increase as number of IP address in a pool are increases.

VI. REFERENCES

[1] Andrei Sabelfeld and Andrew C. Myers "Language-Based Information-Flow Security," in the proceedings of IEEE journal on selected areas in communications, vol.21,issue 1, ,jan-2003.

[2] J. A. Goguen and J. Meseguer, "Security policies and security models," in Proeedings of IEEE Symp. on Security and Privacy, Apr. 1982, pp. 11–20.

[3] Harshit Nayyar "Multi-scale Time Series Prediction for Intrusion Detection System," in the proceedings of University Of New Brunswick

[4] D. K. Mishra, M. Chandwani, "Extended Protocol for Secure Multiparty Computation using Ambiguous Identity,". In the proceeding of WSEAS Transaction on Computer Research, Vol 2, issue 2, Feb 2007.

[5] Schubert Foo, Siu Cheung Hui, See Wai Yip, Yulan He "Approaches for Resolving Dynamic IP Addressing" in the proceedings of Internet Research , 1997 ,Vol 7, Issue:3, Page: 208 - 216