ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

Securing and Compressing Transmission over LAN by using Public Key Cryptography

Gagandeep shahi[1], Charanjit singh[2]

Research Scholar, Dept. Of Computer Science Engineering, RIMT- IET, Mandi Gobindgarh, India[1]

Assistant Professor, Dept. Of Computer Science Engineering, RIMT- IET, Mandi Gobindgarh, India[2]

Abstract: Local Area Network used everywhere. Plain message and long size of the message are the big problems for the LAN security. So to protect the authoritative data on LAN users has to apply the cryptography on one of these architectures. Cryptography the area of computer science which developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption. Public key cryptography and Secret key Cryptography are types of cryptography. Public key cryptography provides the better security over the insecure computer networks. RSA and NTRU public key cryptography algorithms keep secrecy of private key between all users on the sensitive or insecure networks. Compression can be used with encryption to fast transmission over LAN. Simple String Compression Algorithm combine with NTRU and RSA & using Peer to peer approach can provide better security as well as short message size for fast transmission of the message over the LAN. Using peer to peer technique we can exclude the third party servers or central dependability which may be costly or may have poor security.

Keywords: Cryptography, Trusted Third Party, Peer to peer (P2P), Public Key Cryptography, Rivest Shamir Adlemen (RSA), Nth Truncated Ring Unit (NTRU), Simple String Compression Algorithm (SSCA) or Bit Reduction Algorithm

I. INTRODUCTION

Cryptography is the art and science of hiding important and secret information from being infringed upon by unauthorized persons as in [1]. In simple words cryptography is an approach that work like a safeguard of the message that unable the web thugs or middlemen to understand the actual meaning of the message who have no authentication. In public key cryptography or Different key cryptography, the receiver and sender apply the Different keys to encrypt and decrypt the message or recover the plaintext from cipher text and it's vice versa because transmitting the secret key on insecure network can also destroy the security of the network. This type of cryptography is also known as asymmetric encryption and decryption. RSA and NTRU are two public key cryptography algorithms. RSA algorithm is based upon the factoring difficulty of integers that why its security is high and encryption time is slow. On the other hand NTRU based upon the multiplication of matrices so it is a fast algorithm for encryption and decryption of the message because computer can perform fast arithmetic operation rather than factoring.

Compression/Decompression and Encryption/Decryption are encoding techniques with difference of motive one reduce the size another hide the sensitive information. Lossless compression on the other hand, manipulates each bit of data inside file to minimize the size without losing any data after decoding. This is important because if file lost even a single bit after decoding, that mean the file is corrupted [12]. That's way Lossless compression use to compress the crucial messages. Simple String Compression Algorithm (SSCA) or Bit Reduction Algorithm is lossless compression algorithm. The idea is, this algorithm reduces the standard 7-bit encoding to some application specific bit encoding system and then pack into a byte array. This method will reduce the size of a string considerably when the string is lengthy and the compression ratio is not effected the contents of the string [13].

II. PROBLEM DEFINATION

When we talk about the security of the Local Area network that may be the network of an organization with in the campus like colleges, industries etc we always depend upon the Central Security Server or third parties to send and receive the messages. Security of the central Server may be weak so that intruder can hack this Central Server and destroy all transmission. Transmission delay can be there due to cartelized approach For example if 'Alice' wants to send message to 'Bob' then it is not possible to send message directly without authentication of Centralized Server shown in Fig. 1. Cost of hire the third party security server may be very high .So there is a need of strong security technique that may not base upon Central Security Server. Long message size also causes the delay in transmission it may be due to apply cryptography on the message shown in Fig. 2.

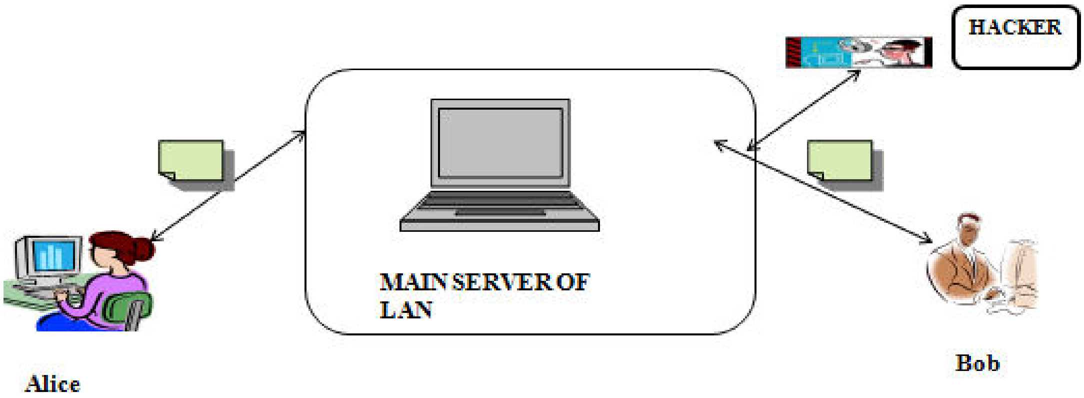


Fig.1 hacker destroying the security of center security server

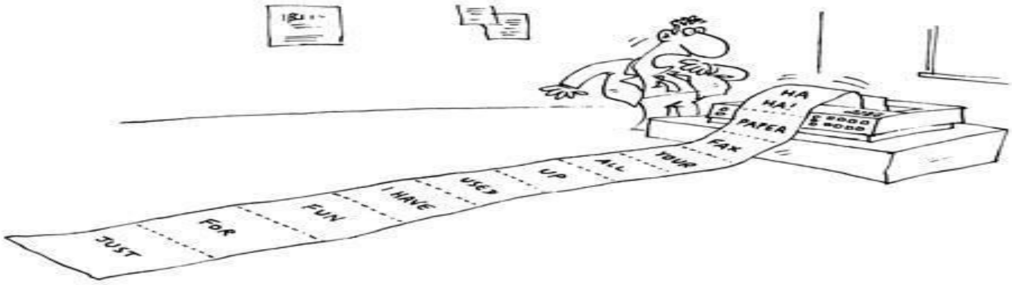


Fig.2 Long message size cause delay in transmission

III. IMPLEMENTATION APPROACHES OF CRYPTOGRAPHY

A. *Present Work*

Implementation Public Key cryptography techniques (RSA and NTRU) with combining compression(SSCA) using Peer to Peer on Local Area Network solve the problem of dependability on Central Security Server on LAN who is responsible for security of the message. This technique can improve the security of the message as well as fast transmission Shown in Fig.3.

In this research implementation of the algorithms on two or more PC's by using network Programming, The term network programming refers to writing programs that execute across multiple devices (computers), in which the devices are all connected to each other using a network. The java.net package of the J2SE APIs contains a collection of classes and interfaces that provide the low-level communication details, allowing you to write programs that focus on solving the problem at hand.

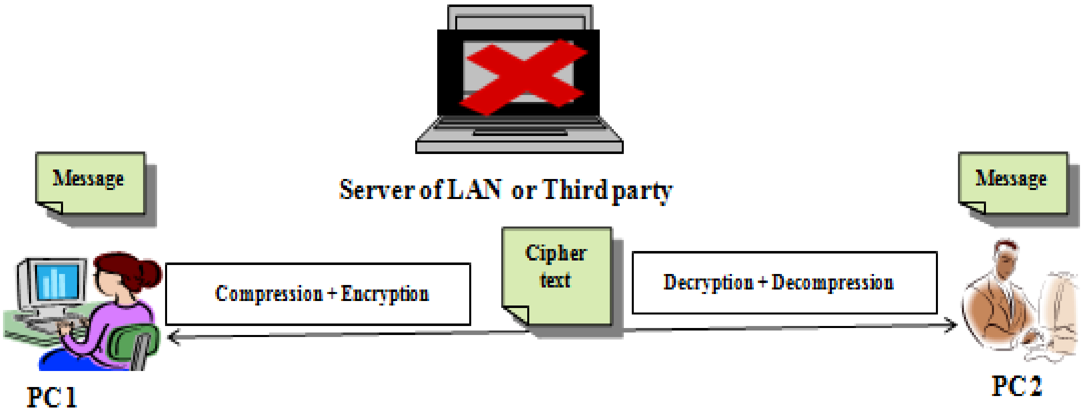


Fig.3 Combining public key cryptography and compression using P2P over LAN

B. Objectives

1) To Calculate the Encryption and decryption time of both the techniques.

2) Total Time of the program execution.

3) Packets will be analysed for delay.

4) Analyse the throughput of algorithms in both cases

C. Proposed Algorithm

1) Proposed algorithm at Sender side

- Input the message in the form of text file
- Compress the message with lossless compression technique
- Encrypt the message using public key cryptography technique
- Send the message in the form of cipher text to the sender

2) Proposed algorithm at Receivers side

- Receive the message in the form of cipher text file
- Decrypt the message using same public key cryptography technique that was applied at the sender side.
- Decompress the message with same compression technique that was applied at Sender side
- After this we will get the original message that was send by the sender.

D. Combining Simple String Compression Algorithm with RSA

This Combination of two techniques called the Simple String Compression Algorithm and RSA shown in the Block diagram Fig.4. Which combines the two encoding technique. if workstation1 want to send the text message to workstation 2 then it inputs the text file to proposed technique and proposed technique compress the size of the text with simple string compression and also encrypt the message with RSA in the form of cipher text so that intruder never understand the message and the transmission of the message can be speed up.

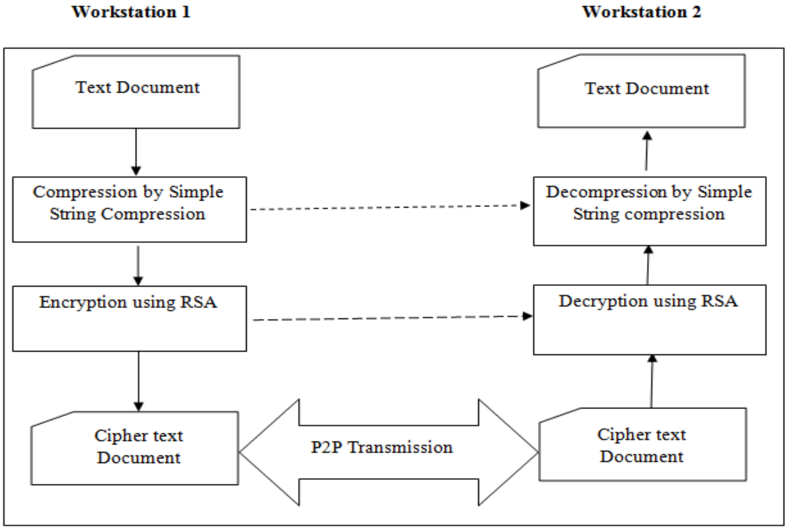
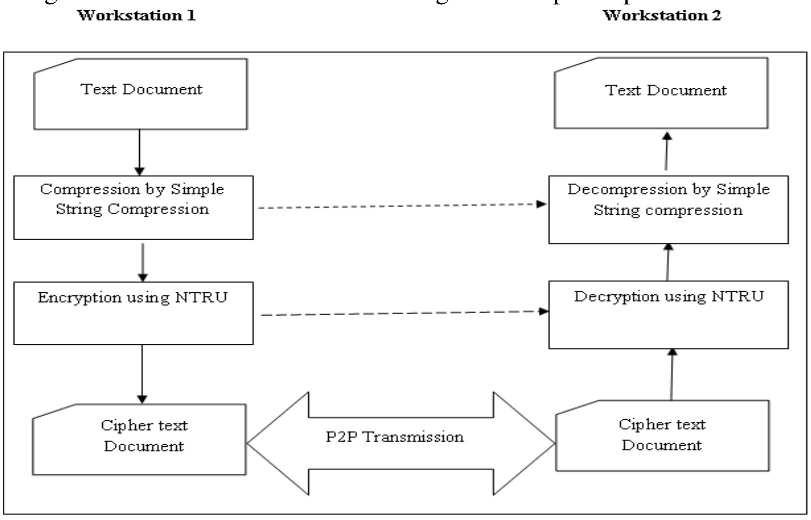


Fig.4 Block Diagram Combining SSCA with RSA

E. Combining Simple String Compression Algorithm with NTRU

This Combination of two techniques called the Simple String Compression Algorithm and NTRU shown in the Block diagram Fig.5. Which combines the two encoding technique. if workstation1 want to send the text message to workstation 2 then it inputs the text file to proposed technique and proposed technique compress the size of the text with simple string compression and also encrypt the message with NTRU in the form of cipher text so that intruder never understand the message and the transmission of the message can be speed up.



.

Fig.4 Block Diagram Combining SSCA with NTRU

IV. Results

In order to obtain statistically significant results several runs are required for different parameters. Simple String compression algorithm is applied on two public key cryptography algorithms called RSA and NTRU. In order to find out find out which algorithm is best from both algorithms results are calculate by several runs for different parameters. First two parameters called Original Size and Compressed size used to find out compressed size of text file. Second, Size of file and Time Spend used to find out Encryption and decryption time as well as compression time and total time to execution of both algorithms shown in following tables and graphs. Following graphs and tables are showing the all results of RSA and NTRU combined with Simple String Compression algorithms in terms of Encryption time, Decryption time, Compression time, overall time etc also analyzing the both algorithms by comparing these facts graphically.

Original message(kb)		4	8	12	16	20
SSC	**RSA**	2500	5120	7680	10240	12800
	NTRU	2500	5120	7680	10240	12800

V. CONCLUSION

Data security is a hot issue in this modern digital era. Cryptography fulfills the security issues like integrity of data, confidentiality of data, availability of data and verification/validation of the data. We have already discussed the various techniques of the cryptography with its two implementation approaches named as Trusted Third Party Cryptography Implementation Approach (TTPCA) Peer to Peer Cryptography Approach (P2PCA).According to the situation we can use these approaches with the help of available resources in our network.

ACKNOWLEDGMENT

First of all I want to thank the light of god who guided me throughout the way. I would also like to thanks an Assistant Professor Mr.Charnjit Singh for his great efforts of supervising and leading me to accomplish this fine work.

REFERENCES

1. Dr. Qais Faryadi (2013), “Does Data Security Matter? The Case for Cryptography”, the 2nd International Conference on Computer Science & Computational Mathematics (ICCSCM), 2013.
2. Ayushi (2013), “A Symmetric Key Cryptographic Algorithm’, International Journal of Computer Applications”, Vol. 1-NO.15, pp. 0975 – 8887, 2013.
3. Anoop (2005), “Public Key Cryptography-Applications Algorithms and Mathematical Explanations”, anoopms@tataelxsi.co.in, 2005.
4. Sumedha Kaushik**, Ankur** Singhal, “Network Security Using Cryptographic Techniques”, Volume 2, Issue 12, pp. 105-107, 2012.
5. Shafi Goldwassar, Silvio Micali and Ronald L. Rivest, “A Digital Signature Schemes Secure Against Adaptive Chosen-Message Attacks”, Society for Industrial and Applied Mathematics, Vol. 17, No. 2, 1988.
6. William Stallings, “Cryptography and Network Security Principal and Practice”, Pearson Education, Inc., publishing as Prentice Hal, 2011.
7. Scott M. Lewandowski, “Frameworks for Component-Based Client/Server Computing”, ACM Computing Surveys”, Vol. 30, No. 1, 1998.
8. Ernesto Damiani, De Capitani di Vimercati and Stefano Paraboschi, “A Reputation Based Approach for Choosing Reliable Resources in Peer to Peer”, Proceedings of the 9th ACM conference on Computer and communications security, ISBN: 1-58113-612-9, 2002.
9. Pankaj R. Patil and D.R.Patil, “Distributed private key for P2P network message security”, World Journal of Science and Technology, Vol. 2(3), pp. 122-126, 2012.
10. Tobin White, “Encrypted objects and decryption processes: problem-solving with functions in a learning environment based on cryptography”, Vol.72, issue.1, pp. 17-37, 2009.
11. Gunjan Gupta, Rama Chawla, “Review on Encryption Ciphers of Cryptography in Network Security”, Proceedings of the International Conference on Data Engineering”, Volume 2, Issue 7, ISSN: 2277 128X, 2012.
12. A.D. Suarjaya, “ A New Algorithm for Data Compression Optimization” , International Journal of Advanced Computer Science and Applications, Vol. 3, No.8, 2012.
13. R.S. Brar, B. Singh “A survey on Different Compression Techniques and Bit Reduction Algorithm for Compression of Text/Lossless Data”International Journal of Advance Research in Computer Science and Software Engineering” ,Volume 3, Issue 3, ISSN: 2277 128X 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 7, September 2013

BIOGRAPHY

Er. Gagandeep Shahi is a research scholar Pursuing Master of technology in Computer Science Engineering from RIMT- IET College Mandi Gobindgarh, Punjab (India). He received the degree of Bachelor of Technology in Computer Science Engineering from Ludhiana College of Engineering & Technology Katani Kalan Ludhiana; Punjab (India).He is also a Diploma holder in Computer Science Engineering from Guru Nanak Dev Polytechnic College Ludhiana, Punjab (India). He is having almost one and half year teaching experience. His area of interest is Network security issues faced by the users in the computer networks and RDMS.

Er. Charanjit Singh is highly qualified teacher with a rich experience of 9.5 years in Teaching & Administration in Educational Institutes. He is presently serving as Assistant Professor in Computer Science Department of RIMT-IET, Mandi Gobindgarh. Er. Charanjit Singh completed his M.Tech. in Computer Science & Engineering from Guru Nanak Dev college of Engineering & Technology, Ludhiana. His area of interest includes Distributed systems, computer networks, computer architecture and digital hardware design. He is pursuing his Ph.D. in Computer Science and Engineering.

.