International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

A HYBRID SECURITY APPROACH FOR SECURE COMMUNICATION IN P2P NETWORKS

Kamal[1], Vijay Birchha[2], Preetesh Purohit[3]
Research Scholar-CSE,Swami Vivekanand College of Engineering
Assistant Professor-CSE, Swami Vivekanand College of Engineering
Head-CSE, Swami Vivekanand College of Engineering
kamalsir@hotmail.com
vijaybirchha@gmail.com
preeteshpurohit@svceindore.ac.in

Abstract—Security is an approach to give safety and protection in coordination. It can be defined as the state to maintain liberated from hazard or security threats. Security policies not only provide safe and secure communication but also help to establish trust on processed information. This paper consist a security model to provide strong confidentiality, authentication and integrity in intranet network. Proposed model may use alternative solution os secure socket layer for local applications.

Proposed solution integrates the strength of symmetric key and public key cryptography to create a hybrid encryption policy. It uses RSA and Diffie Hellman key exchange algorithm along with RC4 to maintain confidentiality of information. Furthermore, SHA-1 has been implemented to maintain integrity of content.

The complete work has been implementing with java technology followed by server client architecture. A security model has been developed and implement using server socket concept to encrypt and communicate secure file between server and client application. Encryption and communication execution time has been evaluated to observe the performance of proposed solution.

Keywords—Hybrid Security Model; RSA; SHA-1; RC4; Server Socket Programming

I. INTRODUCTION

Security is the state or capability to provide isolation or privacy for information or any credential during communication or node end. In other words, It is a guarantee of safety and security from unauthorized or unwanted interrupt. Security is classified into six main categories whereas confidentiality, authentication and integrity are the major key players.

Here, cryptograph technique is used to provide data protection within application or public networks. Several desktop applications has been developed in recent years.These applications are classified as peer-to-peer because of the elimination of servers to mediate between end systems on which the applications run, and their network behavior is described as an overlay network because the peer protocols form a virtualized network over the physical network.

The study of conventional system concludes that there is big scope of improvement in security policy of highly security expected applications. To understand and develop a hybrid and secure security model work consider few security algorithms which are listed below:

1. RSA Algorithm Asymmetric Key Cryptography
2. Diffie Hellman Key Exchange Algorithm for authentication
3. RC4 Symmetric Key Cryptography
4. SHA-1 to achieve Integrity on information

II. PROBLEM STATEMENT

Study observes that security plays crucial role in communication and help a lot for trust building. The major problem with existing security scenarios is focus on single security

principles. Several applications have been developed with the aim to provide security during communication or work station end. The dark part of all applications is single principle concentration. Few applications provide great level privacy but less focus on integrity management and authentication approach.

The study conclude that in the public key infrastructure, encryption – decryption process can be performed with different key. Encryption with private key can be provides great level of authentication but suffer with confidentiality issue. Subsequently, encryption with public key can provide privacy but frail for authentication principle. Hybrid algorithm can be a good solution to overcome this problem.

Consequently, none of asymmetric algorithm helps to provide integrity.

A digital envelope uses two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

Either of the following methods may be used to create a digital envelope:

- Secret key encryption algorithms, such as Rijndael or Twofish, for message encryption.
- Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data. An example of a digital envelope is Pretty Good Privacy (PGP) - popular data cryptography software that also provides cryptographic privacy and data communication authentication. A digital envelope is also known as a digital wrapper.

The complete study explore that, there is no procedure to maintain integrity of message. So, proposed solution should provide a security model to achieve confidentiality with hybrid encryption policy. Subsequently, work expects to have great feature of integrity maintenance and authenticity of received information.

III. PROPOSED SOLUTION

This research work proposes an efficient technique to encrypt and decrypt plain text to keep information safe and secure from unwanted user interaction. It combines symmetric and asymmetric key cryptography algorithm to increase the strength of encryption process. Furthermore, encryption with private key in RSA will help to achieve authentication about sender. Subsequently, SHA-1 algorithm has been used to maintain integrity of content. A basic architecture of proposed system is shown in figure 3.1 and 3.2.

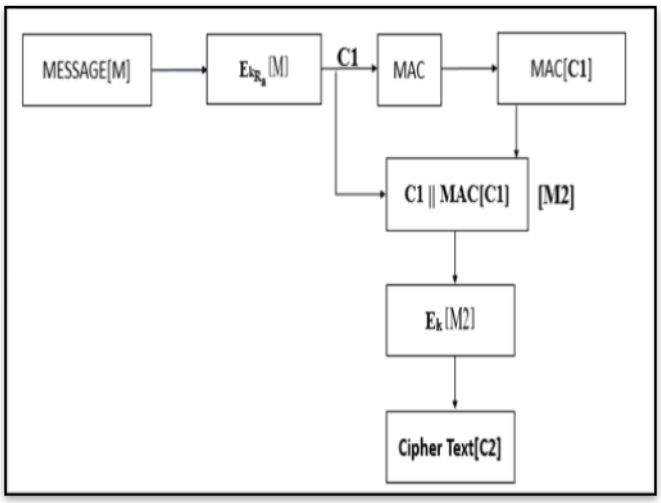

Fig.1. Encryption Process

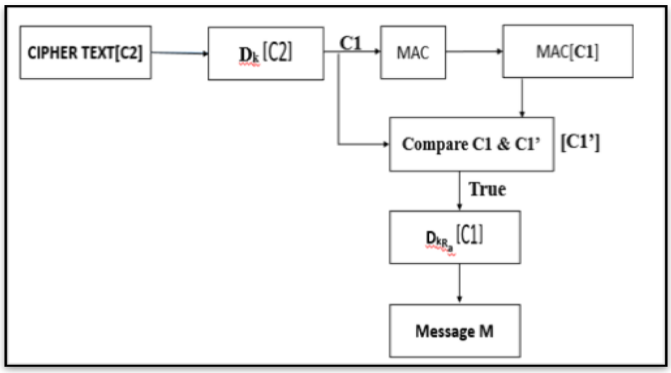

Fig.2. Decryption Process

Following security algorithms are used to achieve safe and secure communication.

1. RSA Algorithm [Asymmetric Key Cryptography]
2. Diffie Hellman Key Exchange Algorithm
3. RC4 [Symmetric Key Cryptography]
4. SHA-1[Secure Hash Algotihm-1]

Another wards, It also uses socket programming to establish communication between Server/Sender and Client/Receiver computers.The complete phenomena provide a very safe communication shown in Figure 3.3 & 3.4 shows insecure communication and attack.

This research work proposes an efficient technique to encrypt and decrypt plain text to keep information safe and secure from unwanted user interaction. It combines symmetric and asymmetric key cryptography algorithm to increase the strength of encryption process. Furthermore, encryption with private key in RSA will help to achieve authentication about sender. Subsequently, SHA-1 algorithm has been used to maintain integrity of content. Following security algorithms are used to achieve safe and secure communication.

1. RSA Algorithm [Asymmetric Key Cryptography]
2. Diffie Hellman Key Exchange Algorithm

3. RC4 [Symmetric Key Cryptography]
4. SHA-1[Secure Hash Algotihm-1]

Another wards, it also uses socket programming to establish communication between Server/Sender and Client/Receiver computers.The complete phenomena provide a very safe communication shown in figure 3.3 where figure 3.4 shows insecure communication and attack.

The study of all relevant existing system and present solution conclude that none of solution is available which gives all major principle of security like confidentiality, authentication and integrity. There is need to develop a solution which should give integrity and authentication with privacy presentation into strategic manner.

So, proposed solution should provide a strong environment to achieve security with all basic principles. Hybrid scheme can help to achieve this along with primary knowledge of existing solution. Figure 1 shows insecure communication and attack.

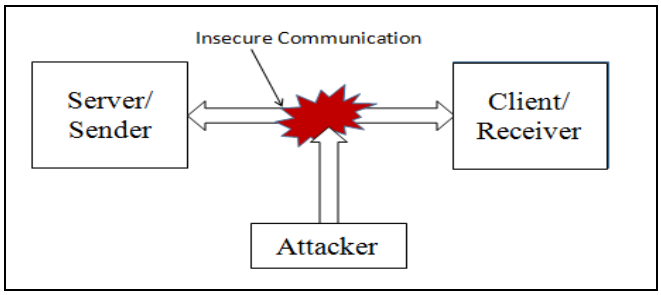

Figure 3: Insecure Communication

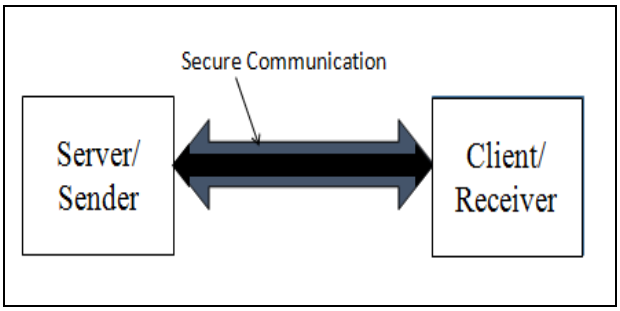

Fig.4. Secure Communication

Following steps are to be performed to establish secure communication and send text message from one node to another node.

Step 1: Receiver generates public key and private key named with [KU_b,KR_b] and assume P and Q to generate N for Diffie Hellman Key Exchange Algorithm.

Step 2: Receiver initiate Socket communication by sending request to sender and broadcast the set of its public key KU_b and N for further process.

Step 3: After receiving key set at sender end, it generates shared secret key for RC4 and SHA-1.

Afterwards, receiver closes the socket communication and wait for encrypted information.

Step 4: Sender initiate RSA encryption process to generate cipher text of Plain Text.

Step 5: Sender forward generated cipher text to SHA-1 function and generate SHA-1 output to maintain text integrity.

Step 6: Sender encrypt the value of RSA cipher text and SHA-1 output with RC4 algorithm to maintain privacy on SHA-1 output. The complete phenomena will give two layer confidentiality over plain text.

Step 7: Sender initiate connection with intended user and send complete encrypted data to Receiver.

Step 8: Receiver decrypt the received cipher text with RC4 shared key.

Step 9: Recalculate the SHA-1 value of received RSA cipher text.

Step 10: Compare the value of regenerated SHA-1 and received SHA-1. In case of same value it initiates RSA decryption process.

Step 11: After decrypting the received plain text will be generated.

The complete phenomena create a safe and secure environment to establish secure communication. Furthermore, multithreading in proposed application would help send text and file in simultaneously.

IV. RESULT AND OBSERVATIONS

The complete work proposed that an efficient technique is required to keep information safe and secure. It should avoid unwanted user interaction. Symmetric key cryptographic algorithms are best for instance communication because they do not required key transmission and can use same key for encryption and decryption purpose. Subsequently, it is also the major drawback of this existing algorithm, because attacker can get benefit of such steps and may compromise the information. Furthermore, asymmetric key cryptographic algorithm can be used to overcome this situation. It uses key pair where different key is used to perform encryption and decryption operation. The dark part of this trick is in case of leakage of private key whole system can be compromised. Other wards, it can't provide confidentiality and authentication into single shot. Interiority is also missing in both parts. To overcome this problems proposed solution consider four algorithms which not only belong to four different category but also the best mechanism in there department.

The research work carried out the analysis an integration of various security algorithms to maintain authentication, confidentiality and integrity. It will provide a safe and secure layer between sender and receiver to maintain privacy and originality during transmission. Java Technology is used to implement server-client based application using proposed solution. Following parameters are used to evaluate the performance of proposed solution.

1. Message
2. Size Time

8byte, 16 byte, 32 byte, 64 byte, 128, 256 byte plain text samples are used to estimate enhanced message size and consumed time. Enhanced Size and Consumed time estimation has been shown in table 5.1 and table 5.2.

Encryption Process (Message Size Estimation)

Table 5.1(a): Message Size Estimation (byte)

e-ISSN: 2394-8299
p-ISSN: 2394-8280

Plain Text Size	RSA Encryption [Plain Text]	SHA-1 of RSA Cipher Text	RC-4 Encrypted Hash Value Size	RC-4 Encrypted RSA-Data Size
8	2046	40	40	616
16	2043	40	40	616
32	2046	40	40	616
64	2046	40	40	616
128	2045	40	40	616
256	2045	40	40	616

Decryption Process (Message Size Estimation)

Table 5.1(b): Message Size Estimation (byte)

Encryption Process (Time Estimation)

Table 5.2(a): Time Consumption (Milliseconds)

Plain Text Size	RSA Decrypted Data Size	SHA-1 Hash Value Size	RC-4 Decrypted Hash Value Size	RC-4 Decrypted RSA-Data Size
8	2046	40	40	616
16	2043	40	40	616
32	2046	40	40	616
64	2046	40	40	616
128	2045	40	40	616
256	2045	40	40	616

Plain Text Size	RSA Encryption Time	SHA-1 Hash Generation Time	RC-4 Encryption Hash Value Time	RC-4 Encryption RSA-Data Time	Total Time
8	73.761718	0.286494	0.245117	1.683222	75.976551
16	67.319227	0.545779	0.230628	2.321977	70.417611
32	68.785707	0.249948	0.067618	3.171437	72.27471
64	71.278542	0.268059	0.09358	2.397445	74.037626
128	70.095819	0.22278	0.059166	2.054522	72.432287
256	75.447355	0.220968	0.057958	2.087123	77.813404

Decryption Process (Time Estimation)

Table 5.2(b): Time Consumption (Milliseconds)

Plain Text	RSA Decryption	SHA-1 Hash Generation Time	RC-4 Decryption Hash Value	RC-4 Decryption RSA-Data	Total Time

Size	Time		Time	Time	
8	0.374908	7.417703	276.1024	300.594908	584.489929
16	0.127111	14.299303	0.328533	311.975126	326.730073
32	1.257702	6.990553	2.456457	307.294363	317.999075
64	0.225448	6.941664	0.300038	292.193384	299.660099
128	0.112863	7.125486	0.285791	300.956686	308.480826
256	0.094146	7.329143	0.262883	304.591226	312.277398

Algorithm	**Description**
RSA Algorithm	Asymmetric Key Cryptography
Diffie Hellmen Key Exchange Algorithm	Symmetric Key distribution algorithm
RC4	Symmetric Key Cryptography Algorithm
SHA-1	Integrity Solution

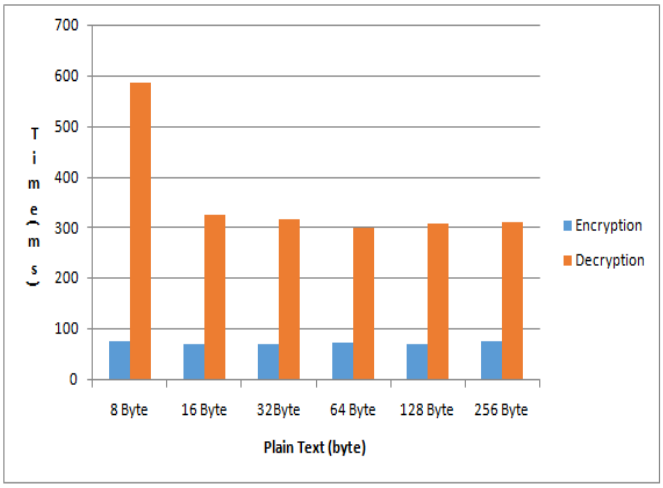

Fig.5. Comparison of Time Taken for Encryption and Decryption process

V. CONCLUSION

The complete work concludes that proposed solution will give an alternative security model than SSL and digital envelop to maintain security in intranet. SSL require HTTPs protocol, where proposed solution does not require any kind of protocol involvement in applications. Furthermore, the basic application of proposed solution is integration of security policy with local network based applications. It may helpful in such applications where privacy, authentication and integrity, all are primary demands.

REFERENCES

[1] Elichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval and Jacques Stern, "RSAOAEP is secure under the RSA assumption," Journal of Cryptology, 2002.

[2] Adrian Perrig, RobetSzewczyk, Victor Wen, David Culler and J.D. Tygar, "SPINS: Security protocols for sensor networks," Mobile Computing and Networking, Rome, Italy, 2001.

[3] Lai, Xuejia, and Massey, James L., A Proposal for a New Block Encryption Standard, Advances in Cryptology - EUROCRYPT '90, Lecture Notes in Computer Science, Springer-Verlag, 1991:389-404.

[4] Menezes, A., Van Oorschot, P., and Vanstone, Handbook of Applied Cryptography, S. 1996.

[5] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, New multiparty authentication services and key agreement protocols, IEEE Journal of Selected Areas in Communication, 18(4), 2000.

[6] Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang, "An efficient implementation of multi-prime RSA on DSP processor," University of Texas, Texas, USA, 2002.

[7] David Pointcheval and Jacques Stern, Security proofs for signature schemes, EUROCRYPT '96, Zaragoza, Spain, 1996.

[8] Bruce Scheneir, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.