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

SYSTEMATIC LITERATURE REVIEW FOR TEXT ENCRYPTION BY HYBRID CRYPTOGRAPHY

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 the paradigm where safety and privacy are the two major foundation steps. It can be defined as the position of environment which maintains the isolation of information and resources from unwanted interrupts. The basic purpose of security mechanisms is to maintain information safe and secure from security threats or internal hazards. A lot of research work has been performed to increase the level of security. Still a scope of improvement is observed due to growing nature of technology.***

This paper comprises the basic overview about the security principles and there requirement to integrate them with software solutions. Here, work also identified that security mechanisms are the essential component of any software development and can't be ignore to avoid overhead or implementation effort.

With rapid growth of security measure, attackers also increase their knowledge and increase their scope to crake the existing algorithms. Thus the study of existing algorithms and measure generate a requirement to increase the strength of security algorithm to avoid risk of security breaching. Hybrid cryptographic algorithm may be the replacement of existing technique to increase the level of security measures and tolerance against the attackers attempt to compromise the information.

This paper comprises the basic details about the security algorithms and also gives a model of hybrid algorithms to overcome the problem of week security system.

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

I. INTRODUCTION

Cryptography is the technique to convert a human readable text into non readable format. It helps to prevent information and communication from unwanted access or leakage.

Software construction is the routing process of technical world and several desktop and web applications are emerged in recent years that use internet or intranet as backbone to establish connection among nodes. These applications may be single node, server-client based or peer-to-peer applications which can perform transaction either in private environment or public network. People feel that only public environment is vulnerable for security threats and obtain security measures during public communication but, private security threats are more risky and complex to prevent. Public or outsider attacks can be prevent or avoid using firewall kind of mechanism but internal security threat can't be identified through such systems. Internal attack applies through trusted node from private environment where all nodes are identified and can be consider as trusted authority. Thus this paper gives detail about to maintain security during communication despite it is in public or private.The study of traditional system and existing environment conclude that a huge scope of improvement is expected in the field of confidentiality and authentication.

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

The complete security architecture based upon the concept of security principles. Researchers have defined six basic security principles for development purpose. All this are listed below [1] [2] .

1. Confidentiality
2. Authentication
3. Integrity
4. Access Control
5. Non Repudiation
6. Availability

1. *Confidentiality*
   It ensure about the isolated communication across the network. It claim then none of information is leakage or can be accessed through attackers.
2. *Authentication*
   This principle implements the concept of proof of identity to ensure that whether the user is valid or not.
3. *Integrity*
   It give promise to maintain the originality of content during transmission.
4. *Access Control*
   It implements the concept of "who can access what".
5. *Non Repudiation*
   It helps to avoid misunderstanding and improve to reduce denial of claim situation.
6. *Availability*
   It ensures to reduce deadlock situation and a lot the resource as per requirement.

II. RELATED WORK

Goshwe, N [1] et al. explore that resource sharing on data communication network is the primary requirement. Due to vulnerable nature of public network, security becomes the major concern. This paper presents an architecture using RSA Algorithm to increase the security against the individual message block level. Proposed Model allows sender to encrypt the message using private key and stored into database with secure manner.

Jamgekar, R. [2] et al., address that Security algorithm RSA can be used to establish confidentiality during file transmission level also. There are many situations, where plain text file transmission can become vulnerable for information leakage. A modified RSA algorithm has been used to encrypt the file text with highest security level. RSA is a asymmetric key based algorithm, which follows key pair of primary key and public key to perform security

operations. Once someone tries to decode the content, attacker will not be able to extract the content due to unavailability of security algorithm.

P. Srinivasarao[3] explore that use of security algorithms and cryptography in daily routine is increasing extremely; nowadays the computers machines are quicker and in future its speed will increase with rapid rate. Brute force attacks are used to crack the cryptographic algorithms. This paper displays the comparison between PSR algorithm and RSA Algorithm which are used in the encryption of plaintext into cipher text that are generally used in cryptography.

Mahajan, P. [4] address that confidentiality is the primary issue in network security. Subsequently, authentication is also becoming the major requirement for user based software's. This paper comprises the techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Singh, S.[5] et. al. state that DES and RSA are the two major algorithms to maintain confidentiality and authentication. Besides both algorithms are very strong to maintain security, still have certain loop holes. This paper gives an idea to integrate both algorithms to give very strong security mechanism.

III. PROBLEM STATEMENT

The key problem with presented cryptographic scenario is, can't get authentication and confidentiality in sole step. In public key infrastructure encryption and decryption process implemented with different key. Here, a key pair is used which consist private key and public key of each individual user. Private Key is the non sharable and public key is distributed through key distribution algorithms. As per the Asymmetric Key Cryptography if we encrypt the message with private key, anyone can decrypt the message by using its public key. This scheme implement authentication but cannot maintain the confidentiality. This principle implements the concept of proof of identity to ensure that whether the user is valid or not.

Furthermore, if we encrypt the message by public key, only intended recipient can decrypt the message. It helps to maintain the confidentiality but cannot authorize sender. To overcome the above problem we use to perform public key encryption after private key. So, only intended receiver would be able to decrypt the message and also authentic the sender by decrypting the received cipher message with public key. Subsequently, there is a procedure to maintain authentication and confidentiality by implementation digital envelop for communication.

Subsequently, a digital envelop is used to call a better level of security. It provide the safety of envelop into digital manner. It gives a pleasure to communicate data but encapsulated into envelop format. Thus another party can't view or access the sensitive information. It uses two layer of security through symmetric key cryptography and public key encryption. 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 like Rijndael or Twofish, for message encryption.
- Public key encryption algorithm like RSA with secret key encryption by receiver's public key.

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.

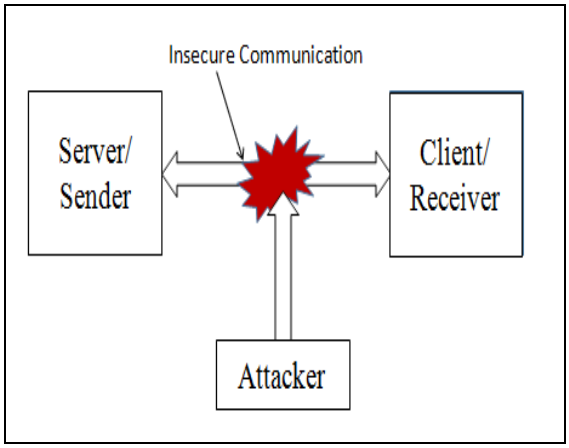

Fig.1. Insecure Communication

IV. PROPOSED SOLUTION

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

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

However, a question arise how this algorithms will interact with each other and what will be the procedure for the execution of proposed model.
Following steps will be performed to establish secure communication and send text message from one node to another node.

1. Receiver will 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.
2. Receiver will initiate Server Socket point by sending request to sender and broadcast the set of its public key N.
3. Afterwards, receiver stores the public key of sender at receiver end and generates shared key for RC4 and SHA-1.
4. Now, receiver will close the connection
5. Sender will invoke RSA procedure to start encryption process.
6. Sender forwards this cipher text to SHA-1 function to calculate integrity checksum.
7. Sender combines this digest with cipher text and encrypts the value with RC4 to maintain privacy against digest.
8. Sender will transfer data and close the connection
9. Receiver will decrypt incoming message with RC4 algorithm,
10. Receiver will calculate digest for received cipher text to check the integrity.
11. In case of successful checking it decrypts the cipher text with received key.

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.

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 2 & 3.

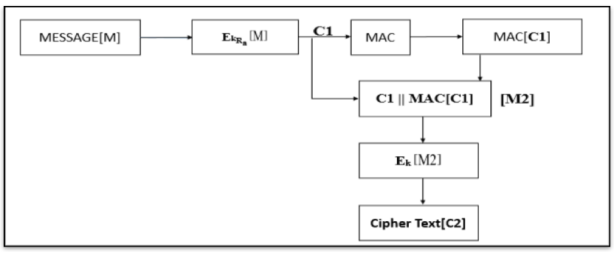

Fig.2. Encryption Process

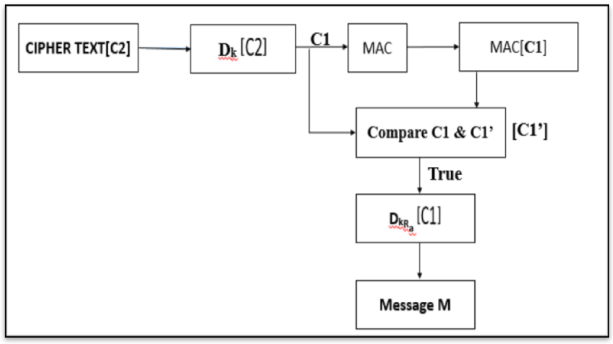

Fig.3. Decryption Process

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 4:

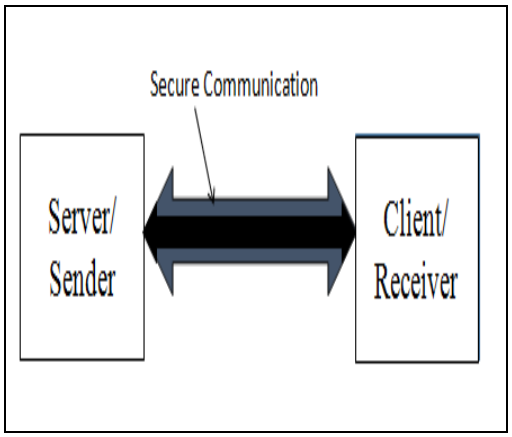

Figure 4: Secure Communication

V. RESULT AND OBSERVATIONS

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 will used to implement server-client based application using proposed solution. Following parameters will used to evaluate the performance of proposed solution.

1. Message Size
2. Time

8byte, 16 byte, 32 byte, 64 byte, 128, 256 byte plain text samples will be used to estimate enhanced message size and consumed time.

VI. 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] Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," International Journal of Computer Science and Network Security, vol. 13, July 2013.

[2] Rajan.S.Jamgekar, Geeta Shantanu Joshi "File Encryption and Decryption Using Secure RSA," International Journal of Emerging Science and Engineering, vol. 1, Issue-4, February 2013.

[3] P. Srinivasarao, P. V. Lakshmipriya, P. C. S. Azad, T. Alekhya, K. Raghavendrarao and K. Kishore, "A Technique for Data Encryption and Decryption," International Journal of Future Generation Communication and Networking, vol.7, No.2, pp.117-126, 2014.

[4] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13, Issue 15 Version 1.0, 2013.

[5] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar, "A Performance Analysis of DES and RSA Cryptography," International Journal of Emerging Trends & Technology in Computer Science.

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

[7] 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.

[8] 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.

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

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

[11] Eun- Jun Yoon, Kee –Young Yoo, "An Efficient Diffie – Hellman – MAC Key Exchange Scheme," IEEE, Fourth International Conference on Innovative Computing, Information and Control, pp 398 – 400, 2009.

[12] Xi aowen Kang, Yingjie Yang, Xin Du, "A Disaster – Oriented Strong Secure File System," IEEE, 3rd International Conference on Innovative Computing Information and Control, 2008.

[13] R . L. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public Key Cryptosystems," Technical Memo 82, Laboratory for Computer Science, Massachusetts Institute of Technology, April 1970.

[14] Sonal Sharma, Saroj Hiranwal, Prashant Sharma, "A NEW VARIANT OF SUBSET-SUM CRYPTOSYSTEM OVER RSA," International Journal of Advances in Engineering & Technology, Jan 2012.ISSN: 2231-1963.

[15] R.L. Rivest, A. Shamir and L. Adleman, "A Method of obtaining Digital Signatures and Public Key Cryptosystems," Communication of the ACM, 21, 2(1978), pp 120-126.

[16] Sattar J Aboud, "An efficient method for attacking RSA scheme", IEEE 2009.

[17] "A public key cryptosystem and a signature scheme based on discrete logarithms", Taher ElGamal 1998,Springer-Verlag.

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