Secure communication with Encryption of AES and RC4 hybrid algorithm with Hash Function

Ravinder Kaur[1], Minakshi Sharma[2], Pankaj Sharma[3]

[1]Research Scholar,*Department of Computer Science and Engineering*
Sri Sai College of Engg and Technology,Pathankot (Badhani), Punjab, India

[2]Professor, *Department of Computer Science and Engineering*
Sri Sai Collegeof Engg and Technology, Pathankot (Badhani), Punjab, India

[2]Assistant Professor, *Department of Computer Science and Engineering*
Sri Sai College of Engg and Technology, Pathankot (Badhani), Punjab, India

Abstract–Grid computing is a distributed network in which several processors distributed globally and sharing the computational resources to solve various problems. Security in every network is now a must and important part for the successful communication in network. Normally network security is at much higher level on outer part of the network than the inside part. This property of security sometime can act as hot cake for network intruders. Insider attacks combined with various worm attacks could prove to be the bottleneck and disaster for network. There is need of optimized approaches to handle such security issues. In our research we will focus on the combination of Advance Encryption Standard (AES) and Rivest Cipher version 4 (RC4) to provide strong combination of encryption to defend against discussed security concerns and then provide some hiding functions with help of hash functions such as MD5 or SHA1. Advance encryption standard (AES) provides solution for security with whitener (Whitening is used to enhance the security of the cipher) with multiple matrix in RC4 algorithm which is ten converted with hash function for best secure communication. Combination will prove to be best fit for providing security with secret key to each and every block of AES combined with whitened text. RC4 will produce multiple three layer matrix with different combination to enhance security which is finally interated with hash function for providing hashed data which will provide more security in communication.

Keywords –Advance Encryption Standard, Rivest Cipher, Message Digest level 5, SHA1, Grid Computing, Whiten Text.

1. INTRODUCTION

Security requirements within the distributed environment are based on the size of network and resources it require for communication. In now a day's many network services are tends to seek strong security measures as services are so distributed in nature that once it broke or corrupted, then it is difficult to recover and recovery cost is very high.

Cryptography is an art of encrypting a plaintext such that it is rendered unreadable to others except the person for whom the message is intended [1]. Encryption is the good solution for major types of attacks in the distributed network environment. Cryptography renders the message unintelligible to outsider by various transformations [2]. Data cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access [3].

Normally process of security includes two states of encryption and decryption. The process of encryption converts the present available plaintext into other form which is encrypted in nature and further this encrypted is used as cipher text. The process of

decryption converts the present encrypted cipher into the original material which was been encrypted. In nutshell, process of encryption is to convert data into some other form and process of decryption is to convert that changed form into its original form. The strict policy are there for converting the content to other form and strict policies are there to convert back to original state. A unique object is used for managing policies which is act as key. This unique key is used in both processes for encryption and decryption process in order to convert and generate the original text.

1.1. Symmetric Algorithm

Symmetric algorithms are classified as block cipher and stream ciphers algorithms. Advance encryption standard is a symmetric-key algorithm which uses same key for both processes of encryption and decryption and totally based on substitution-permutation concept which makes AES very strong against various attacks and misbehaviors. Normally AES is divided into block ciphers which further divide data into blocks and use to combines key with each to get encrypted and decrypted data.
Transformation rounds are used by AES which act as definite number of times to encrypt and decrypt data (whole process in reverse manner) depending on the bit length of unique key used by AES (10 for 128 bit, 12 for 192 bit and 14 rounds are used for 265 bit key).

1.2. Rivest Cipher

Rivest Cipher is also a symmetric key based cipher (known as stream cipher) like Advance Encryption Standard Algorithm. It is a stream cipher which means that the random key generated in RC4 is applied to each bit of the plaintext one at a time to get the encrypted text [3]. Increasing demand of computing in industry need strong encryption and RC4 is providing great solution for it.

1.3. Advance Encryption Standard

AES comes as pure replacement of rives cipher but acceptance of AES is low due to newness and it is block cipher which is not as popular as RC4. Moreover, RC4 is one of the fastest ciphers known in industry and AES is very slow compared to RC4. Now a day's, security issues continue to arise and it is the moment to look at an better approach for more security and proposed work will be used as combination of both encryption algorithm with different secret keys and RC4 with whitened text and different matrix combination. Combination will include the characteristics of time and speed into a new cipher.

In particularly for better secure communication, symmetric encryption is the better fit to network than the asymmetric encryption. Symmetric algorithms have good history of defending various type of misbehavior in network. Two of the best algorithm based on symmetric encryption are advance encryption standard and rivest cipher level 4. Our focus will be on providing combined security through algorithms with more security features in both AES and RC4 with hash functions.

With the growing trend of using computers and internet for all purposes, sending data securely has become highly risky. Hence, security is the growing need of the day which stream ciphers like Rc4 are unable to provide. WEP application uses Rc4 but Scott Fluhrer in his paper Weaknesses in the Key Scheduling Algorithm of RC4 [7] throws light on the risk factor. He shows how knowing a few bits of the key in the Rc4 cipher, can easily break the cipher and determine the output of the cipher with a high probability. It was shown that for a ciphertext attack, a key of arbitrary length could be easily recovered using this technique which renders the cipher highly insecure. AES has been suggested as a replacement on several occasions but AES being new and a block cipher, it is not as popular as Rc4 [1]. Moreover, AES is very slow compared to Rc4 which is one of the fastest ciphers known and is the major reason for its popularity. As security issues continue to arise, it is time to look at an alternate approach which is why the proposed algorithm can prove to be a cross between Rc4 and AES combining the characteristics of time and speed into a new cipher [2].
Rc4 combined with AES is highly likely to create a secure algorithm. RC4 can be combined with AES in various ways.

In our research, we will provide strong encryption scheme with combination of discussed encryption schemes. Further the integration of the both algorithm will be done with hash function in distributed grid network by securing the network.

2.PROPOSED WORK

In related study, hybrid solution for AES has been proposed. It includes combination of in rivest cipher 4 algorithm by introducing there tier layer implementation of temporary matrixes in the RC4. Combined algorithms will provide good results by improving secure communication in network. To avoid complex calculations and to provide a suitable and strong encryption mechanism, combination of AES and RC4 can be a suitable solution. The main area of improvement in network is faster processing and strong security key on different level of the network. AES security depends on the permutation-combination transformations that are called a number of times. On reducing this number the speed of the cipher will increase but at the same time the security will decrease and the cipher will be more vulnerable to attacks. This vulnerability needs to be compensated by other changes in the algorithm. In our research work, we will implement a hybrid algorithm Advance encryption standard (AES) which provides solution for security with whitener (Whitening is used to enhance the security of the cipher) with multiple matrix in RC4 algorithm and finally results will be converted with hash function for better experience of security. Combination of both will prove to be best fit for providing security with secret key to each and every block of AES combined with whitened text. RC4 will produce multiple three layer matrix with different combination to enhance security.

Our work will have huge significance in area where high security for communication is required. Previously proposed algorithms are providing security but previous work haven't consider the threats which could be launched from inside the network which makes previously proposed work vulnerable somewhere. This research will be suitable for both type of attacks (Insider and outsider) by providing harder security. For faster processing, we have also used less number of rounds in AES and rounds can be increased automatically by AES if we process bigger data sizes.

Our research has ample scope in the related area. Particularly talking about distributed systems, computing security, and proposed solution can provide a secure communication for distributed computing. Solutions which are already present are not suitable for distributed computing security because some provides security but increases the overhead which is not good for computing as distribution of resources is totally a managing job. Some of the security measures are less secure in term of large network implementation for distributed networks. Our proposed solution will have great scope due to agile secure communication with less overhead than other techniques.

3. CONCLUSION

The paper shows the brief idea to have secure communication in grid computing environment. It is our continuous study and we are going to implement it in Java environment representing it as Grid environment. Our main focus is to bring about security of the network to a good level so that, secure communication can be occurred.

REFERENCES

[1] Prabhudesai Keval Ketan and Vijayarajan V, ''An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption'', International Journal of Computer Applications, pp.12-17, Vol.54, No.12, September 2012.

[2] Nidhi Singhal1, J.P.S.Raina," Comparative Analysis of AES and RC4 Algorithms for Better Utilization," International Journal of Computer Trends and Technology, pp.177, Vol.2, July to Aug 2011.

[3] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir .M and Al-Nabhani.Y, "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal of Computing, Volume 2, Issue 3, pp.152-157, March 2010.

[4] Abd-ElGhafar, A. Rohiem, A. Diaa, F. Mohammed," Generation of AES Key Dependent S-

Boxes using RC4 Algorithm", 13th International Conference on Aerospace Sciences & Aviation Technology, pp. 26 – 28, Vol.3, May 2009.

[5] Kamal Jyoti," Enhanced Amalgam Encryption Approach for Grid Security: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[6] Luo Zhen, Li Zhishu, Ca Biao,"A Trust Infrastructure for Grid Security Module", IEEE, Journal of Information Processing Systems, pp. 345-347, Vol.6, Issue.2, June 2010.

[7] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli," Cyber–Physical Security of a Smart Grid Infrastructure", IEEE, Vol. 100, No. 1, January 2012.

[8] Alessandro Barenghi and Gerardo Pelosi," Security and Privacy in Smart Grid Infrastructures ", 22nd IEEE International Workshop on Database and Expert Systems Applications, Vol.3, Issue 9, 2011.

