Survey on Various Techniques for Network Security

[1]Er. Mehak Singla, [2]Er. Lavina Maheshwari
[1]Student, [2]A.P.
CSE, GRIMT, Radaur (Yamunanagar) , India

Abstract - **Cryptography or cryptology is the study of techniques for secure communication in the presence of third party which is known as adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or also the public from reading private messages; various aspects in information security such as data confidentiality, authentication, data integrity and non-repudiation are central to modern cryptography. The main objective of survey is comparative analysis of various encryption techniques ,their computation complexity, hardness of keys generated, extra overheads. In this paper, we investigate the security related issues and challenges in network security. Based on this research, the future scope of network security is forecasted. New trends that are emerging will also be considered to understand..**

Keywords - **Entropy, Cryptography, Encryption, Decryption.**

I. Introduction

There is an urgent need for some methods to face challenges in network security. To overcome this problem in network safety, the best answer is "Cryptography".It means maintaining the secrecy of confidential data to be transmitted by number of policies and algorithms. Cryptography is technique of hiding the data by changing into encoded form by sender and decoded by only user who has power to open it.

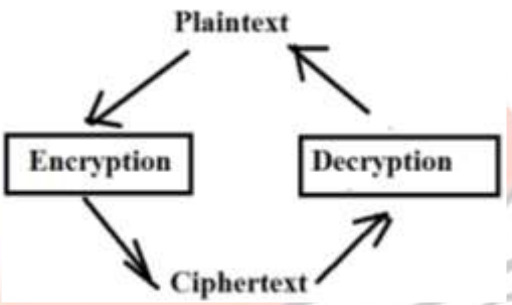

Figure-1

Security of data over the network is done by encryption/decryption process. Cryptography is the method of writing in undisclosed code so that only those for whom it is offered can easily read and process it. Data cryptography mainly is the scrambling of the content of the data, such as image,text, audio, video and so forth to make the data unreadable, hidden or meaningless all the way through transmission or storage is termed Encryption . The main determination of cryptography is to look after of data secured from attackers. The procedure of getting back the real data from encrypted data is Decryption, which restores the original data

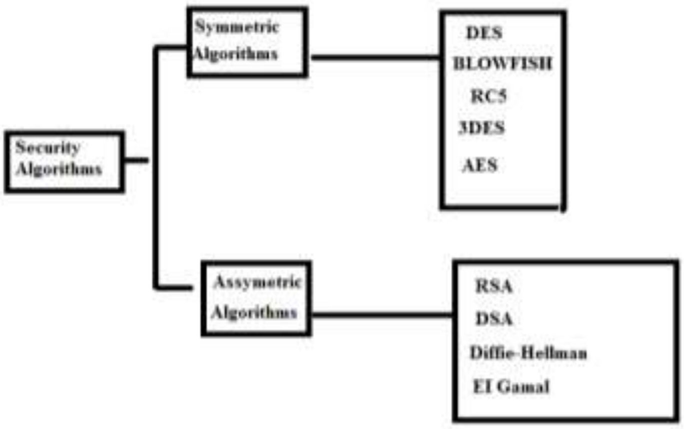

Figure 2-Security Algorithms

II. Cryptography Goals

There are various goals behind using cryptography. They are as follow:

- Authentication: It means that the data sender and data receiver should be authenticated before sending and receiving data.

- Confidential: It suggest that the user who is authenticates can only access the information or messages of other authenticated users.
- Integrity: It means that the data is totally free from any kind of modification between sender and receiver.
- Non-Repudiation: This function tells us that neither the sender nor the receiver can falsely deny that they have sent a particular message.
- Service Reliability: Secure systems can be attacked by the attackers, which may put affect the service that is provided to the user of the system.

Symmetric and Asymmetric encryptions

There are two types of techniques are used for encryption & decryption which is Asymmetric and Symmetric encryption techniques.

- Symmetric Encryption:In this type, same cryptography keys are used for the encryption of Plaintext & decryption of Cipher text. This encryption is very fast & very simpler but their main drawback is that both of the users need to transfer their keys in a secure way. In symmetric key cryptography, same key is shared, i.e. the same key is used in encryption and decryption, hence it is also known as single or secret key encryption. Symmetric key cryptography algorithms are very simple & require lesser execution time.
- Asymmetric Encryption:In this case, two keys are used. It is also called as Public Key Cryptography (PKC),because users tend to use these two keys: public key, which is known to all public and a private key which is only known to the user. In asymmetric key cryptography various keys are used for encryption and decryption, hence,it also known as public key encryption.

Comparative Analysis of Various Encryption Techniques

S.no	Author	Year	Technique Used	Findings
1	Ankit Garg, Kamal Kumar Sharma, Sharad Chauhan	Oct-15	Cryptool	entropy of the proposed AES is 4.69.
2	Kavita Sharma, Pardeep Tyagi, Abhinav Juneja	Jul-15	DES	takes lesser time to encrypt and decrypt,don’t enhance the mathematical complexions
3	Dhaval Vegad,Husain Ullah Khan	Apr-15	Modulo Arithmatic	user can also select their own files also by browsing,but nobody can alter the location of that file
4	Manpreet Kaur Grewal,Ms. Sukhpreet Kaur	Aug-14	J-Bit Algorithm	increased throughput,reduce the size of data
5	Bahar Saini	May-14	S-Box Rotation	entropy of proposed-AES is higher than AES.
6	N.Lalitha, P.Manimegalai, V.P.Muthukumar, M.Santha	Jan-14	Advance Hill Cipher Algorithm	proposed a secret text hiding approach,
7	Julia Juremi,Ramlan Mahmod,Salasiah Sulaiman, Jazrin Ramli	Nov-12	Round Key	key expansion algorithm together with S-box rotation,improve the security of AES by making its S-box to be key-dependent

III. LITERATURE REVIEW

A number of journals and research papers published during the above span 2009-201 have been studied. The ample aspects of the problem were studied.

- **Ankit G et. al (Oct. 2015)** This paper generate a key from a password given by the user to provide a better security to the block cipher. The symmetric encryption keys are long random strings of bits, and cannot be expected that anybody would actually remember them, let alone enter them using an onscreen keyboard. Whereas on the other side, all the users are familiar with the passwords, and thus a way to generate strong cryptographic keys based on humanly-manageable passwords is needed. New AES-like design has developed using C and results have analyzed using crypTool. The result has been analysed using various parameters of cryptool like entropy, histogram, N-Gram, autocorrelation
- **Kavita Sharma et. al (July 2015)** Cryptography is an emerging technology which uses the features of human vision to decrypt encrypted images. It does not require cryptography knowledge and complex computation. There are many challenges, which one face when design a security model. The requirements of the security model depend upon the type of data to be encrypted. There is main problem to be considered, is the computational speed of the encryption model. There are many security models, which provide high level of security. Such model increases the execution time for encryption. The effectiveness of the algorithms highly depends upon computational time or computational speed. There is a main issue to Mono-alphabetic Cipher, that it can be broken because same plain letters are encoded to same cipher letter and the underlying letter frequencies remain unchanged. This problem can be solved by assigning ample cipher letters or symbols to same plain letters. This can be implemented by a poly-alphabetic ciphering and deciphering technique. The proposed method is based on DES and it has similar properties and structure to DES with much smaller parameters. The proposed encryption algorithm receive an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of cipher text. The proposed algorithm takes an 8-bit block of cipher text and the same 10-bit key is used to produce that cipher text as input and produces the real 8-bit block of plaintext. A time effective symmetric key algorithm for small amount of data has been proposed. The performance of proposed technique

will be evaluated with text received and computation time. MATLAB R2013a will be used as an implementation platform.

- **Dhaval Vegad et. al (April 2015)** Encryption has come up as a better result and plays an important role in information security system. Various techniques are needed to protect the shared data. The recent work focus on cryptography to safe the data while transmitting in the network. Firstly the data which is to be transmitted from client to receiver in the network must be encrypted using the encryption algorithm.Moreover, by using decryption technique the receiver can view the original data. In this paper ,Author implemented a very simple algorithm for both encryption and decryption.
- **Manpreet Kaur Grewal et .al (Aug 2014)** AES is considered as a best encryption algorithm in terms of providing security to a network in passing data in form of audio, string,video and in any another form. However it yields a low throughput result in slowness and increasing energy dispensation of server. The Enhanced AES algorithm is proposed in this ,which works by using sequence counters and provides us better throughput as compare to conventional AES algorithm. The J-Bit Encoding is being a compression algorithm in lossless category which doesn't decline the quality but decrease the size of data to some extent. In this paper proposed a encryption algorithm integrated with J-Bit Encoding algorithm will provide the effective security measures and also increased throughput as a parameter and less bandwidth use as the actual size of data will not be sent along the network.
- **Bahar Saini (May 2014)** AES algorithm is considered as a secured algorithm. Still, some security issue lie in the S-box and key used In this paper, Author had tried to give focus on the S-box rotation to get highly secured information .The standard AES comprises of four stages while in the new design, it consists of five stages The extra stage is known as S-box rotation.
- **N.Lalitha et. al (Jan 2014)** Cryptography is a part of information security. They had very secure methods for both Steganography and cryptography – AES algorithm is a very safe technique for cryptography and the Steganography methods, which use frequency domain, are highly safe. Data hiding is a technique that is used to hide information in digital media such as audio,images, video etc. This idea is to apply both of them together with more security levels and to get a very highly safe system for data hiding. This paper mainly concentrate on to develop a new system with extra security characteristics where a meaningful piece of text message can be hide by combining security techniques like Steganography and Cryptography. The performance of a reversible embedding algorithm is measured by its payload capacity, complexity, visual quality and security.
- **Julia Jurem et .al (Nov 2012)** This paper presents a new AES-like design for key dependent AES by using S-box rotation. The algorithm involves key expansion algorithm with S-box rotation and this technique can be used to make the S-box key-dependent, hence providing a good security to the block cipher. Fixed S-box allows attackers to study about S- box and find weak points by using key-dependent S-Box method, it makes it very hard for attacker to do any offline analysis of the attack of one particular set of S- boxes. The cipher structure resembles the real AES, only the S-box is made key-dependent without changing any value. This new design is tested by the use of NIST Statistical Test and will be further cryptanalyzed due to algebraic attack in order to permit its evasion or subversion

IV. CONCLUSION

Various techniques for network security have been studied in Literature and found that technique Round key is used to improve the security of AES by making its S-box to be key-dependent.Inspite of this, Advance Hill Cipher Algorithm proposed a secret text hiding approach. Apart from that,by S-Box Rotation the result found that entropy of proposed-AES is higher than AES. whereas by using the J-bit algorithm, it increased throughput & reduce the size of data.By using Modulo Arithmatic, user can also select their own files also by browsing,but nobody can alter the location of that file.

V. REFERENCES

[1] Ankit Garg, Kamal Kumar Sharma, Sharad Chauhan, "Performance Analysis of Password-Based AES Encryption and Decryption Using Cryptool," International Journal for Advance Research in Engineering and Technology, Volume 3, Issue X, Oct. 2015 ISSN 2320-6802.

[2] Kavita Sharma1, Pardeep Tyagi2, Abhinav Juneja3,"Design And Evaluation Of Performance Of Cryptography Technique Based On Des", International Journal For Advance Research In Engineering And Technology, Volume 3, Issue Vii, July 2015 Issn 2320-6802.

[3] Dhaval Vegad, Husain Ullah Khan , Nimesh Ghosh," Character Based Encryption and Decryption using Modulo Arithmatic,",IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015.

[4] Manpreet Kaur Grewal1 Ms. Sukhpreet Kaur2," Encryption and Compression of Audio-Video Data Using Enhanced AES and J-Bit Algorithm", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 08, 2014.

[5] Bahar Saini, "Implementation of AES Using S-Box Rotation", Volume 4, Issue 5, May 2014 ISSN: 2277 128

[6] N.Lalitha1, P.Manimegalai2, V.P.Muthukumar3, M.Santha4, " Efficient data hiding by using aes & advance hill cipher algorithm", International journal of research in computer applications and robotics, Vol.2 Issue.1, Pg.: 1-13 January 2014.

[7] Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman, Jazrin Ramli," Enhancing Advanced Encryption Standard S-Box Generation Based On Round Key", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 1, No. 3.