International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network

[1]Ajay Kakkar, [2]M. L. Singh, [3]P.K. Bansal
[1]Thapar University, Patiala, India.
[2]GNDU, Amritsar, India.
[3]MIMIT Malout, India.

ABSTRACT

For a secured system it has been desired to make the combination of data and keys secured. One can hack the data by knowing the information about the radiations of a machine, key length, encryption time, number of stations and block size. Few algorithms creates dummy file which has been generated along with the encrypted data in order to misguide the hacker and acts as overheads. Short length keys are normally exposed to the hacker very easily that's why large key lengths have been preferred. For the encryption and transmission of data in Multinode Network (MN) various techniques are used. This paper covers the various techniques and algorithms used for the data security in MN.

Keywords: *Encryption, Key, Multinode network (MN), Hacker.*

1. INTRODUCTION

Data security is an essential part of an organization; it can be achieved by the using various methods. In order to maintain and upgrade the model still efforts are required and increase the marginally overheads. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. The information about the key is present in the encrypt data which solves the problem of secure transport of keys from the transmitter to receiver [1-2]. In case of practical system encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format cipher text with the help of key.

2. NEED OF CRYPTOGRAPHY

Computers are normally interconnected with each other in the Multinode Network (MN) and are exposed to the other networks and the communication channels therefore encryption is required to keep the data confidential from each other. Secured data communication is also an essential parameter for all the industries/ governments. There is a need of secured data transmission in defense, industries, universities, etc. Share markets, banking sector, etc are also requires encryption techniques to keep the electronic transfers of funds and access to bank accounts secured from the hacker [3,5]. It is also required for secure E-commerce in case of railways, medical and communication fields. The government requires strong encryption algorithms to keep the defense related documents, information regarding sensitive buildings/ dams/ military headquarters, etc secured from the other countries.

3. CRYPTOGRAPHY

It is a technique used to avoid unauthorized access of data. The encryption process consists of single or multiple keys to hide the data from the intruders. The original text before the encryption process is known as *Plaintext***.** The text obtain after encoding the data with the help of a key is known as *cipher text*. For example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

This type of arrangement is known as *substitution ciphers*. The key in such is L8 it represents left shit by 8 bits and it is known to sender and the receive [1,4,8]. The encryption process has the power to change/upgrade the key at any time and information of changed or upgraded key has been made known to both the parties. The encryption, decryption, and key are shown in the figure 1.

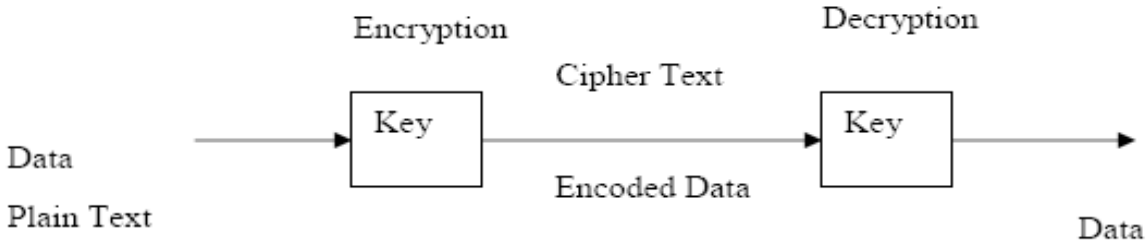

Figure 1: block diagram of cryptographic model

4. TYPES OF CRYPTOGRAPHY

The cryptography techniques are classified on the basis of their key selection. The section shows the merits and merits of various cryptographic techniques.

4.1 Symmetric (Private) Cryptography

When same key is used to encrypt and decrypt the message then it is known as symmetrical key cryptography. It is also known as private key cryptography; users have the provision to update the keys and use them to derive the sub keys. It is much effective and fast approach as compared to asymmetrical key cryptography. In symmetrical key cryptography; key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place [4,6]. There are few challenges in the technique; i) the key should be transmitted over the secure channel from sender to receiver. The point is that if the secure channel already exits then transmit the data over the same channel, what is the need of encryption in such case. Practically no secured channel exits therefore key has been transmitted along the data which increases the overheads and effective bandwidth gets reduced. Secondly, the channel noise put harm to the key and data during the transmission.

4.2 Asymmetric (Public) Cryptography

Whitfield Diffie, Martin Hellman, and Ralph Merkle laid public key cryptography in June 1976. The encryption algorithm uses different keys for encryption and decryption, i.e; each user has a pair of cryptographic keys (a public key for encryption and a private key decryption) [7, 9-11]. This illuminates the need of transportation of key from sender to receiver. The method is more secured as compared to private key cryptography but it consumes more power and takes more processing time therefore extra hardware is required. Due to increase in the computational unit the overheads are high in public key cryptography.

4.3 Modern Cryptography

A combination of both public key and private key cryptography is known as modern cryptography. A pair of public and private keys has been used to encrypt and decrypt the data [10,14]. The technique has the salient features of private key; fast speed, easy to process and features of public key such as secured, avoid key transportation, provide the power to the users to generate their own keys of variable length. Users also have the flexibility to upgrade the key at any interval of time. In this technique; certification authority has been used to keep the track of the entire system and keys.

4.4 Cryptographic Algorithm

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also named as cryptographic algorithm. There are many cryptographic algorithms available in the market to encrypt the data. Their strengths depend upon the cryptographic system. Any computer system which involves cryptography is known as cryptographic system, the strength of encryption algorithm heavily relay on the computer system used for the generation of keys [11,16]. The computer systems take the responsibilities sending the secret information over the web with the help of cryptographic hash functions, key management and digital signatures. Crypto systems are composed from cryptographic primitives such as encryption algorithm, number of keys, hash and round functions, memory elements, real time operating system, etc. Some important encryption algorithms are discussed here:

4.4.1 Data Encryption Standard (DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations [1,18].

4.4.2 International Data Encryption Algorithm (IDEA)

IDEA is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991. It uses 128 bit key length which operates on 64 bit blocks. It consists of a series of eight identical transformations based upon bitwise exclusive-or, addition and multiplication modules. It is based upon symmetric cipher and has very weak key design method therefore security level of the algorithm is very poor as compared to the DES. IDEA not becomes so much popular due to its complex structure [1,7,19].

4.4.3 Blowfish

It is a freely available symmetric block cipher designed in 1993 by Bruce Schneier. It includes key dependent S-boxes and a highly complex key schedule which produces overheads. It has a 64 bit block size and a variable key length from 1 to 448 bits. The technique uses the concept of sub keys; these are generated by the algorithm itself. It is a very fast approach for encrypting the data with same keys. When keys are changed then new key under goes from pre-processing operation which consumes more time [1].

4.4.4 Triple DES (TDES)

It was developed in 1998 and derived from DES. It applies the DES cipher algorithm three times to each of the data blocks. It has a key size of 168 bits but provides at most 112 bits of security remaining 56 bits are utilized in the keying options. The standards define three keying options; K_1, K_2 & K_3 and are given as:

First keying option: All the three keys are independent.

Second keying operation: K_1 & K_2 are independent, and $K_3 = K_1$.

Third Keying option is all the three keys are identical $K_1 = K_2 = K_3$.

The block size used in the algorithm is 64 bits and 48 DES equivalent rounds have been used to encrypt the data. The security of TDES is effective but the main limitation of the standard is that 56 bits are not actually used for the encryption [1].

4.4.5 Advanced Encryption Standard (AES)

It is a symmetric key encryption standard adopted by the in US government in 2001. It was designed by Vincent Rijmen and Joan Daemena in 1998 later inspected by National Institute of Standards and Technology (NIST) as U.S. FIPS in November, 2001. Various security checks had been performed in the procedure and AES was declared the best encryption standard out of 12 participated standards and the use of AES becomes effective in May, 2002. It has 3 different key sizes: 128, 192 and 256 bits used for the encryption of the 128 bit block size data. It includes three different default rounds depending upon the key length i.e. 10 for a 128 bit key size, 12 for a 192 bit key size and 14 for a 256 bit key size. The design of sub key has been designed by considering the side channel and cache timing based attacks [1].

4.4.6 Twofish

It was derived from blowfish by Bruce Schneier in 1998. It is freely available in the public domain as it has not been patented. It is a symmetric key block cipher having key sizes 128,192 and 256 bits used to encrypt the 128 bit block size data in 16 rounds. The algorithm making use of S- Boxes and makes the key generation process very complex and secured [1].

4.4.7 RSA

RSA is a public key system designed by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman in 1978. The RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. Two distinct prime number say p & q has been selected randomly and then by using the mathematical properties such as Eular's function, Chinese remainder theorem, hamming weight and exponential functions key has been generated and then encryption process takes place. Decryption has been done in the receiver section by using the public key concept. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the system's overheads by taking more processing time [1].

4.4.8 Diffie-Hellman

Whitfield Diffie and Martin Hellman introduce the key exchange technique in 1976. In 2002, Ralph Merkle's contributed his work in the key exchange program and the technique named as *Diffie Hellman Merkle key exchange*. In order to tackle man in the middle attacks the Diffie Hellman introduces password authenticated key agreement (PAKE) which was based on generating matrix [1,14]. When hacker uses single password attack in the iteration; immediately the key structure becomes changed, thus allows only maximum of single password attack in the each iteration by the hacker. This technique helps in achieving better security even in the presence of weak password.

4.4.9 Elliptic Curve Cryptography (ECC)

In 1985, Neal Koblitz and Victor S. Miller suggested the use of ECC for the encryption of data. There are four ECC techniques and stated as: the elliptic curve Diffie Hellman key agreement scheme which uses the key exchange approach suggested by Diffie Hellman scheme and based upon the public key cryptography. Second, the Elliptic Curve Integrated Encryption Scheme (ECIES) in which encryption and key generation takes place in one step. Third scheme was based upon the digital signature algorithm and is known as Elliptic Curve Digital Signature Algorithm. MQV key agreement scheme has been used in

the ECMQV. The security pattern of ECC is quite remarkable and does not affect by the side channel attacks [1,13]. Variable key lengths have been used for the encryption and are varied in accordance with the data blocks to provide sufficient amount of cover the data.

4.4.10 Pretty Good Privacy (PGP)

In 1991 the Philip Zimmermann developed Pretty Good Privacy (PGP) public key cryptography programs. The algorithm was supported by Linux and Window operating systems. It combines the private and public key cryptography to maintain the appropriate confidential level. The technique can be used to encrypt the e-mail messages with the help of hash and MD5 [1,12].

4.4.11 Public key infrastructure (PKI)

It is an unsymmetrical cryptography technique used to encrypt the e- mails. The public keys of the users are covered up with the certificates created by trusted third party. From the root level different keys were designed for different users and are always kept unknown from each other [15]. The first key was generated by the algorithm for the encryption and always kept secret; the second key was generated by the CA on the request of the users and publicly circulated. The user can update their keys and the duplicate copy of the new key was stored at CA.

5. CRITERIA OF A CRYPTOGRAPHIC ALGORITHM

The security of the model has been analysis on the basis of their encryption algorithm and the key management [16]. It has been observed that the encryption algorithm have their own characteristics; one algorithm provides security at the cost of hardware, other is reliable but uses more number of keys, one takes more processing time. This section shows the various parameters which plays an important role while selecting the cryptographic algorithm.

5.1 Level of Protection

The techniques have been compared on the basis of that how much:

- CPU time would be required by a machine for a given processing speed to generate the key, encrypt and decrypt the data.
- The amount of memory required to hold the data in encryption process.
- Number of users accommodated by the model.
- Time required by the model to recover the data in case of key failure.
- Time available to the hacker to produce various type of attacks

5.2 Complexity

Key generation and encryption techniques are usually based upon the mathematical properties of numbers and functions. Higher order polynomial cause complex system as a result the probability of error is increased. If the keys are based upon orthogonal principle then same key must be selected at the receiver to recover the data. Let us take a case in which A is the data stream which has been encrypted by the key B. At the receiver side same key has used to decrypt the data; if key has been changed from B to B' then one cannot recover the data as shown in case-2.

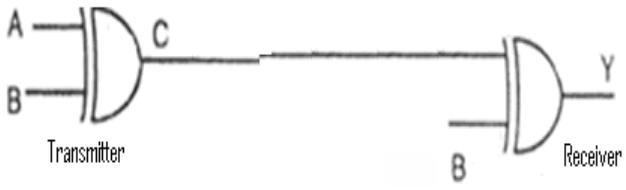

Figure 1.2. Encryption and decryption by using same key

Case-1: Using same key B for encryption and decryption

$$C = A\overline{B} + B\overline{A}$$
$$Y = C \oplus B$$
$$Y = \left(\left(A\overline{B} + B\overline{A}\right)\right) \oplus B$$
$$Y = A$$

Case-2: Using different key for encryption B and decryption B'

$$C = A\overline{B} + B\overline{A}$$
$$Y = C \oplus B'$$
$$Y = \left(\left(A\overline{B} + B\overline{A}\right)\right) \oplus B'$$
$$Y = \left(A\overline{B} + B\overline{A}\right)\overline{B'} + \overline{\left(A\overline{B} + B\overline{A}\right)}B'$$

This is not equal to the original data, $Y \neq A$

5.3 Design Issues

The selection of algorithm also depends upon the requirement of security level. If short data sequences are present within the organization and moderate security level is required then one can make use of symmetrical key cryptography [17]. On the other hand if average security level is needed over the web then pretty good privacy may be selected. For highly secured model one can make use of DES or AES having more number of round functions. The known numbers of attacks up to 2006 are given as: 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys therefore DES and AES can be used to sufficient amount of security level.

5.4 Available Algorithms

Few encryption algorithms are patented and are not freely publicly available. Moreover, there are some legal liabilities are also associated with these encryption algorithms. While selecting an encryption algorithm it has been taken care that which algorithm is suitable and publicly available for the encryption purpose.

5.5 Overheads

Cryptography requires continuous efforts to achieve security; initially efforts are required in the generation of keys. Once the keys have been generated the next step is to encrypt the data and send it over the web. There are various overheads which are associated with in the cryptography and are given as:

- Financial overheads: a lot of money has been invested to keep the documents secured from the enemy.
- Less Channel bandwidth: the users have been able to utilize only limited bandwidth due the presence of additional bits caused by keys.
- More Heat Dissipation: While encrypting the data with multiple keys having large lengths results in significant amount of heat dissipation has been observed. This will put up a limitation on the use of On-chip components which are highly desirable for the fast encryption process.
- Power consumption: the powerful processors consume more power in the key generation process as a result node capacitance, charge sharing and leakage current exist in the model. These parameters are responsible for the loss of data and cause station failure.
- Delay: the encryption process takes time to convert the plain text into cipher text which causes delay and increases latency. Few encryption algorithms also require additional padding techniques which also consumes more power and time.

6. KEY MANAGEMENT

In modern key cryptography every user wants to send or receive secured electronic mail. Users have their own keys and it is required to keep their keys and information about their data must be kept secret from each other. In practice, the keys used by the individual user are different from each other. But in a networked environment, the user might need to use an e-mail from multiple computers having different operating systems. The padding techniques are also the main cause of delay which results in timing collisions in dynamic multiuser system. It creates the need of key sharing scheme. Number of keys, length of keys and their generation and transportation are concerned with security level of data. The aim is to make the entire model secured; all the nodes should be monitored continuously in order to make the combination secured. During the attacks there are few possible outcomes, hacker can be

- Able to break the other node,
- attacks the other nodes but does not get succeeded; at this time the attacked node get failed due to the efforts done by the hacker,
- Attacks the node and succeeded to break it but not able to access the data (due to presence of second key), in such case the hacker corrupts the data as a result the accuracy and reliability of data decreases.

The best method to encounter the problem is that to use multiple keys for individual nodes. When the failure rate of the first key is increased then use the second key for the re-encryption the data. At the same time generate the new key as a replacement of the first key. The probability of failure of both key is very less, in rare cases it exits and such cases are handled; either by employing more number of keys or data sequences is divided into small sequences. In such cases the short length data sequences are used in order to provide sufficient time to the algorithm to generate the new keys.

7. CONCLUSION AND FUTURE SCOPE

The study of various techniques and algorithms used for the secured communication in MN has been done. From the related work it has been observed that the strength of model depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer key length and data length consumes more power and results in more heat dissipation. So, it is not advisable to use short data sequence and key lengths because by using powerful software's one can hack the short keys very easily and able to break the system. Once one can determine the failure rate of keys then encryption process takes place. All the keys are based upon the mathematical properties and their strength decreases wrt time. So, basically it is a tradeoff between key length and security level. For the task the optimal selection of keys makes the model optimized. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data.

REFERENCES

[1] Ajay Kakkar, Dr. M. L. Singh, Dr. P. K. Bansal, "Efficient Key Mechanisms in Multinode Network for Secured Data Transmission", International Journal of

Engineering Science and Technology, Vol. 2, Issue 5, 2010, pp.787-795.

[2] Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9.

[3] Diffiee, W., and Hellman, M., "New Directions in Cryptography", IEEE Transaction Information Theory IT-22, (Nov. 1976), pp. 644-654.

[4] Jason Crampton, "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Volume 6879/2011, pp. 245-261.

[5] Jason H. Li, Bobby Bhattacharjee, Miao Yuc, Renato Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks" Future Generation Computer Systems 24 (2008) pp.860–869.

[6] Jiannong Cao, Lin Liao, Guojun Wang, "Scalable key management for Secure Multicast Communication in the Mobile Environment" Pervasive and Mobile Computing Vol. 2 (2006), pp.187–203.

[7] Jung-Wen Lo, Min-Shiang Hwang, Chia-Hsin Liu, "An Efficient Key Assignment Scheme for Access Control in a Large Leaf Class Hierarchy" Information Sciences Vol. 181, 2011 pp. 917–925.

[8] Lepakshi Goud. T, "A Routing-Driven Public key Crypto System Based Key Management Scheme for a Sensor Network", International Journal of Advanced Engineering Sciences and Technologies, 2011, Vol. No. 6, Issue No. 2, pp. 246 – 255.

[9] Lein Harn, Hung-Yu Lin, "A cryptographic key generation scheme for multilevel data security", Computers & Security Vol. 9, Issue 6, 1990, pp. 539-546.

[10] Ohta, K., Okamoto, T., and Koyama, K., "Membership Authentication for Hierarchical Multi groups Using the Extended Fiat-Shamir Scheme", in Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT'91), 1991, pp. 446–457.

[11] Chu-Hsing Lin, "Dynamic Key Management Schemes for Access Control in a Hierarchy", ELSEVIER Computer Communications Vol. 20, 1997, pp. 1381-1385.

[12] Michael Luby and Jessica Staddon, 'Combinatorial Bounds for Broadcast Encryption", EUROCRYPT '98, LNCS 1403, 1998, pp. 512-526.

[13] Pinkas, "Efficient State Updates for Key Management," Proceedings of ACM Workshop on Security and Privacy in Digital Rights Management, Nov. 2001, pp. 910 - 917.

[14] K. Lee and D. Griffith, "Hierarchical Restoration Scheme for Multiple Failures in GMPLS Networks," Proc. 31st International Conference on Parallel Processing Workshops (ICPPW '02), Aug., 2002, pp. 177-182.

[15] V. R. L. Shen and T. S. Chen, "A Novel Key Management Scheme Based on Discrete Logarithms and Polynomial Interpolations", Computers & Security, Vol. 21, No. 2, 2002, pp. 164–171.

[16] Sheng Zhong, "A Practical Key Management Scheme for Access Control in a User Hierarchy, Computers & Security, Elsevier Science Ltd., Vol. 21, No 8, 2002, pp. 750-759.

[17] Elisa Bertino, Ning Shang, and Samuel S. Wagstaff Jr., "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, 2008, pp. 65-70.

[18] Mikhail J. Atallah, Marina Blanton, Nelly Fazio and Keith B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies", ACM Transactions on Information and System Security, Vol. 12, No. 3, 2009, pp. 1-43.

[19] Vijay Sivaraman,1,2 Diethelm Ostry,2 Jaleel Shaheen,1,2 Antoni Junior Hianto,1 and Sanjay Jha1,2 "Broadcast Secrecy via Key-Chain-Based Encryption in Single-Hop Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking Volume 2011, pp. 1-12.

