ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

A Study on Cryptographic Techniques for Secured Data Sharing in Network

S. Charumathy[1], A. Lalitha [2]

P.G. Student, Department of CSE, Valliammai Engineering College, Kattankulathur, Tamil Nadu, India[1]

Associate Professor, Department of CSE, Valliammai Engineering College, Kattankulathur, Tamil Nadu, India[2]

ABSTRACT: The present generation is more concerned about security in every field. In case of networked environment the privacy of data is of importance. This privacy can be ensured through encryption of data. The cryptography [1] is the way of changing the original data into unreadable format through the use of encryption and decryption technique. The main purpose of doing so is that the data being sent is not disclosed to unrecognized users like hackers. The plaintext is the message transmitted through network. Encryption is a technique to morph the message being transferred between two or more users. There are different techniques for doing cryptography. This survey paper analyses the advantages and disadvantage of all available algorithm**.**

KEYWORDS – Networked environment, Encryption, Decryption.

I. INTRODUCTION

The cryptography [1] is the way of changing the original data into unreadable format through the use of encryption and decryption technique. The main purpose of doing so is that the data being sent is not disclosed to unrecognized users like hackers. The plaintext is the message transmitted through network. Cipher text is the unreadable format of the message being sent. The sender will create the message and use encryption technique and change the format of message, and then sends it to the other users. The receiver of the message will use the decryption technique to get the original message. Generally there are two basic standards as symmetric and asymmetric encryption techniques. In symmetric technique both the source and the target user will use the same key for encryption and decryption. In asymmetric technique the sender will use the receiver's public key for encrypting the message and the receiver will use his own private key for decrypting the message.

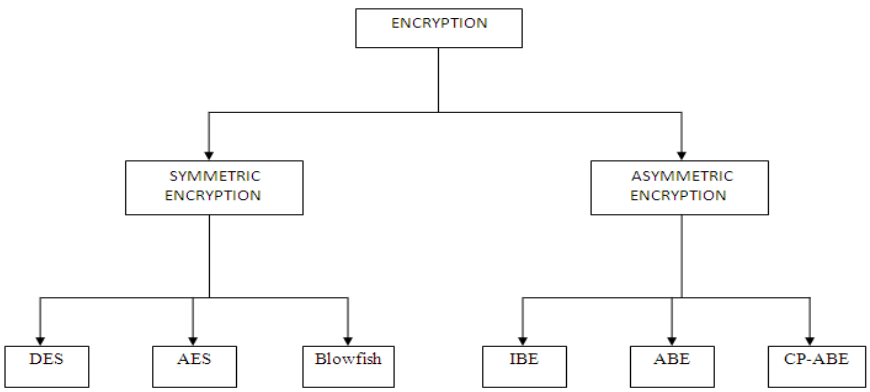

Figure 1.Classification of Encryption Algorithm

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

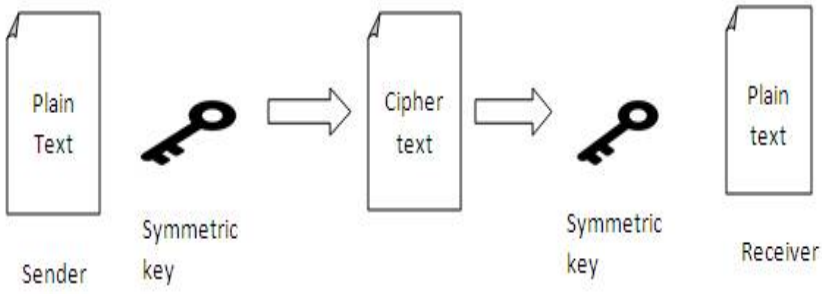

Figure 2.Symmetric Encryption Technique

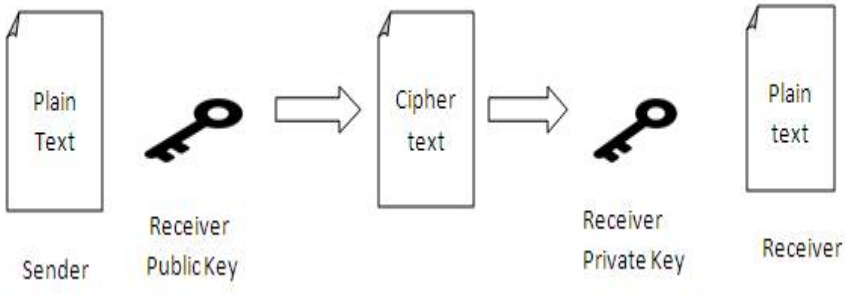

Figure 3.Asymmetric Encryption Technique

II. GOAL OF CRYPTOGRAPHY

The main goal of cryptography is to provide the **NAIC2A** following:

- ✓ **Non-repudiation:** It is the process of preventing the sender from refusing the message being sent.
- ✓ **Authentication:** It is the process of ensuring the identity of the users connected in the network. It responds to the question "Who can send the message".
- ✓ **Integrity:** It is the process of securing the message from changes while in transmission.
- ✓ **Confidentiality:** It is the process of assuring the intended users that no middleman can view the content of the message. It responds to the question "who can see the message".
- ✓ **Availability:** It is process of confirming the presentence of data in the storage for future references.
- ✓ **Access control:** It has a list of users with their rights to access the file.

III. ANALYSIS OF VARIOUS ALGORITHMS

3.1 SYMMETERIC ALGORITHM

3.1.1 DES

DES stands for Data Encryption Standard. National Institute of Standards and Technology derived it for the first time. The base for this is jucifer cipher used by IBM [2].

The input to this algorithm is 64 bit of block, from which only 56 is chosen by using permutation. The leftover 8 bit is either not considered or used to check parity. This 56 bit is future divided into two 28 bit blocks namely left half and rights half. In each round of the technique these two 28 bits blocks are swapped from the left. Then it randomly selects

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

48 bit key from these two blocks. The result is a 64 bit block of cipher text. The decryption follows the same step but, in a reverse order.

ADVANTAGES:

- ✓ It is famous for its secret key. Hence it is used in critical application.
- ✓ It has been proven that DES provides strongly defend against hacker.

***DISADVANTAGES**:*

- ✓ The size of the key is very small.
- ✓ The whole key space can be found within a day span of time.

3.1.2 TRIPLE DES

3DES [9] is the extension of DES algorithm. It repeats the steps of DES for three times to offer more security. The key length used in DES is not sufficient due to the advancement in the technology. Therefore 3DES uses 64 bit key for encryption. First the data is encrypted using the first key, then by second and third keys. The decryption is similar but executed in reverse order.

ADVANTAGES:

- ✓ It is simple to experiment.
- ✓ It increases the security of the algorithm by doing repeated steps of DES.
- ✓ It can be implemented both in software as well as in hardware.

***DISADVANTAGES**:*

- ✓ It has very low performance.
- ✓ This algorithm will take more time for execution.

3.1.3 AES

It is also derived by National Institute of Standards and Technology. It is type of non feistel cipher [10] for a 128 bit block of data. There are options to select the key size corresponding to the number of rounds. That is it can be 10, 12 or 14 with key size of 128,192,256. It has s-box for substituting each byte in a block. After this the rows are shifted in random. Then each of these rows is multiplied with the corresponding matrix of the derivation. Finally the key is XORed with the original data.

ADVANTAGES:

- ✓ AES is developed in order to overcome the disadvantages of the previous algorithms.
- ✓ It is much more flexible and faster in execution.
- ✓ It is secured, so it is used in all critical and bulk processing application.

DISADVANTAGES:

- ✓ It is very much difficult to implement in application.
- ✓ Since it provides a wide choice of very long keys it can be difficult to remember the key.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

3.1.4 BLOWFISH

It is also a popular algorithm for protecting data against vulnerability attacks. It takes input with variable length from 32 to 448 bit block. Blowfish was derived in the year 1993. Initially it was developed by Bruce Schneier [3]. It is a type of feistel cipher which repeats the same simple function for 16 times. The algorithm executes faster when implemented in 32 bit processor with more cache space. It has key expansion and data- encryption part. The key expansion will convert the 448 bit block into 4168 byte block of data. Data encryption part is where the data gets encrypted.

ADVANTAGES:

- ✓ It is the fastest and compact algorithm to use.
- ✓ Till date there is no attack prevail in this algorithm.

DISADVANTAGES:

- ✓ The key has to be brought outside the band especially not through the unsecured channel.
- ✓ Key management is difficult when number of user increases.

3.2 ASYMMETRIC ALGORITHM

3.2.1 IDENTITY BASED ENCRYPTION(IDE)

IDE is an algorithm which allows anyone to generate their own key using values like ASCII. Here a third party will be trusted to produce these keys for the user. Initially only the main public key is given to the user. With the help of this key any person can encrypt there data. When requesting for the data the user has to get the private key from the third party. Therefore all users can encrypt data before the distribution of keys to other user in the network. It was derived by Shamir [4], Boneh et al [5]. There are different types of IDE called fuzzy identity based encryption by Sahai et al [8].

ADVANTAGES:

- ✓ It eliminates the need for public key distribution infrastructure.
- ✓ It has a feature like setting lifetime for the message by the user.

DISADVANTAGES:

- ✓ The privacy of the data depends on the private key generator.
- ✓ There is a need to provide a secure channel for transmitting the message.

3.2.2 ATTRIBUTE BASED ENCRYPTION (ABE)

In this algorithm both the private and public key depends on the attribute of the user. The decryption takes place only when the attribute being set matches with the cipher of the message [7]. It can be used in application encrypting the log. It was derived by Amit Sahai and Brent Waters [6].

ADVANTAGES:

- ✓ It is resistant to collision
- ✓ The number of keys used can be reduced by using the broadcast encryption.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

DISADVANTAGES:

- ✓ It is not efficient and not existent for attribute reuse.
- ✓ The owner has no right to choose who can access the data.

3.2.3 CIPHER TEXT-POLICY ATTRIBUTE BASED ENCRYPTION (CP-ABE)

It was derived by Bethencourt et al. It provides encryption for critical access control list of users. It make use of attributes of the user to generate the private key. That is the owner can specify who can access the original data being stored. It provides high security by continuously changing the user attribute of the stored data. In this method each key is fine-grained. The users can separately insert their own attribute.

ADVANTAGES:

- ✓ It allows for scalability of users.
- ✓ Provides more security than other algorithms.

DISADVANTAGES:

- ✓ The implantation of this algorithm is very much complicated.
- ✓ Setting the semantic threshold is difficult.

IV. CONCLUSION

This paper closely examines all the popularly used encryption techniques. It has shown a brief description of every algorithm with their corresponding benefits and drawbacks. In symmetric encryption the BLOWFISH algorithm is better than others. In case of asymmetric algorithms the CP –ABE is better. It is sure that both these algorithm will provide a strong mechanism against attacker.

REFERENCES

[1] E. Surya C. Diviya, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks,2010.
[2] Mitali, Vijay Kumar and Arvind Sharma, "A Survey on Various Cryptography Techniques",International Journal of Emerging Trends & Technology in Computer Science,2014.
[3] Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.
[4] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.
[5] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.
[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput.Commun. Security, 2007, pp. 195–203.
[7] B. Balamurugan and P. Venkata Krishna. Extensive Survey on Usage of Attribute Based Encryption in Cloud. In Proceedings of Journal Of Emerging Technologies In Web Intelligence, VOL. 6, NO. 3, 2014, pp.263-272
[8] A.Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, 2005, pp. 457 473.
[9] Singh, S preet, and Maini, Raman "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communication,vol.2,No.1,January-June 2011,pp.125- 127.
[10] A.Himani Agrawal and Monisha Sharma, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology vol.3,No.12,December 2012.