International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 02, February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

ANALYSIS OF ENCRYPTION ALGORITHMS IN EHEALTH SERVICES

Shilpa Srivastava[1], Dr. Namrata Agrawal[2]

[1]Research Scholar, Uttarakhand Technical University, Dehradun, (India)

[2]NIFM, Faridabad, (India)

ABSTRACT

Encryption Algorithm play a crucial role in securing the communication. The study is devoted to the analysis of different symmetric key encryption algorithm required for securing the ehealth communication. The algorithms-DES,RC4, IDEA,3DES,AES have been compared on different parameters like number of rounds, block size, key size etc. Later on we suggest the use of different encryption algorithms for different kind of communication based on the sensitivity involved.

Keywords*: *Encryption Algorithm, Block Size, Key Size, Rounds, Symmetric Key.

I. INTRODUCTION

Encryption algorithms can be classified as asymmetric and symmetric key algorithms. Generally asymmetric key algorithms are more subjected to shortcut attacks. It takes less time as compared to brute force attack [1] whereas on the other hand Symmetric key algorithms are found to be more robust.

II. ENCRYPTION ALGORITHM

The backgrounds of different encryption algorithms required for securing the communication in ehealth services has been a part of discussion in this section. We consider an algorithm to be secured if it is very hard to crack it or the only effective attack against it is brute force.The brute force attack becomes infeasible if the search space is very big or number of possible keys is large . Some major encryptionalgorithms have been analysed in this section. They have been compared on the basis of key length and block size. The algorithms being discussed are DES, 3DES, AES, Blowfish, IDEA andRC4.

- ***DES***

This algorithm was developed by IBM in 1975. It is a block cipher with a particular structure. And having 64 bits data block.DES has a fixed key length having size 56 bits for 16rounds. This algorithm can be cracked easily when performed an exhaustive attack by trying all possible keys, on alarge distributed network of computers and recovered the key inless than 23 hours[2].

- ***3DES or TripleDES***

In 1978 IBM introduced an algorithm 3DES which can be considered as an extension of DES. Its functionality is same as of DES , the only difference is that instead of 16 rounds it operates on 48 rounds. It supports 112 bits and a block size of 64 bits. The longer key size makes the 3DES more secure than DES.

- ***AES***

This encryption standard is also known as Rijindael. AES is a substitution/permutation network cipher derived from theSquare cipher. It operates on a block cipher having size 128 bits andvaried key sizes(128, 192 and 256 bits) . The number of rounds also vary(10,12 0r 14). It is an iterative cipher which uses byte substitution, row shifting and column mixing. The shifting operations in AES algorithm makes this algorithm very fast. The process of encryption/decryption increases the speed of AES.AES can be broken by brute force in theory but not possible with current technology [3]. The authors of [4] also did a statistical analysis on AES and were unable to find any weaknesses.

- ***Blowfish***

This algorithm was designed by Bruce Schneier in 1993. It is a Feistel network block cipher which uses a variable key length size between 32-448 bits (128 bits by default) and 64 bits block size for operations on 16 rounds. The authors[5] summarized the cryptanalysis on Blowfish by various researchers.

- ***IDEA***

International Data Encryption Algorithm (IDEA) supports 128 bit key length for 8 1/2 rounds. This is due to the main non-linear part of the cipher that is based on multiplication with a chosen master key and the linearity of the key scheduling [6].

This algorithm is a block cipher and operates on 64bit blocks blockcipher.

- ***RC4***

The encryption algorithm Rivest Cipher 4 (RC4) was developed byRon Rivest. The algorithm makes use of variable key length ranging between 40 to 2048 bits. It is a stream cipher and having variable block size. The speed of encryption anddecryption varies in this encryption algorithm. RC4encryption and decryption time are directly related to theencryption key length and to the size of the data file if the datais large enough[7].

III. E-HEALTH SERVICES

A new healthcare paradigm that combines the existing healthcare system with ICT such as the internet and mobile devices to provide a patient centered health care service.IT revolution in healthcare has presented an opportunity for universal access to medical services and information at a very low cost.According to Dr. T. E. Bell (IEEE spectrum 2006) the effective and efficient use of engineering can lower the costs provided it is focused on early detection of the disease.

The power of the Internet to advance telemedicine was first brought to light by a seminal event in April 1995. An SOS e-mail message was sent through the Internet requesting international help for a Chinese university student, who was suffering from an unknown severe disease. This led to the first recorded Internet diagnosis of Guillian-Barré syndrome.

IV. SECURITY IN E-HEALTH SERVICES

E-health - a web service oriented implementation of next generation information systems enables health care administrators members, medical professionals and patients to organize , share and access to medical services. due to the development of web technologies, security and privacy issues are rising over traditional medical

services.These requirements can be met by providing health care security issues over web services. Web services should be used in such a way that timely and not too cumbersome access to health care records be provided without compromising patients privacy. The next section focus on the analysis of different encryption algorithms for providing security in the ehealth data transmission.

V. ENCRYPTION ALGORITHM FOR E-HEALTH COMMUNICATION

The system resources like processing time, bandwidth ,CPU processing power can be better utilized by using different combination of encryption algorithm. Following are some criteria:-

- ***Key Size****:* the longer key size makes the system more secured as compared to the shorter key sizes.
- ***Block Size****:* the larger block sizeimparts more security to the system.
- ***Rounds****:* the more number of rounds performed, the more secure the cipher is.

Based on the properties of algorithms discussed abovewe can make use of cryptographic algorithms for different type of communication. For eg; the interaction between doctor and the patient needs highest level of security so AES and Blowfish can be applied.

Similarly the general data or the public data which does not demand for high security , DES can be applied. The application of single algorithm to the whole system is wastage of resources which is not required for all kind of communication.

VI. CONCLUSION

In this chapter different encryption algorithms have been anayzed. There characteristics have been compared in terms of block size, rounds and key size. It has been observed that AES and Blowfish are highly secure and also complex so require high system resources. We have analyzed that securing the overall system with a single algorithmleads to the wastage of resources. In Ehealth there is different kind of communication. Some needs very high security and some needs very general security. So instead of using single algorithm we can use multiple algorithms accoring to the level of sensitivity of communication.

REFERENCES

[1]. M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shinomura, E. Thompson, M. Wiener, “Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security,” January, 1996. Available: http://www.schneier.com/paper-keylength.html

[2]. http://distributed.net/16

[3]. S. Tillich, C. Herbst, “Attacking State-of-the-Art Software Countermeasures-A Case Study for AES,” Proc. of the 10th international workshop on Cryptographic Hardware and Embedded Systems, pp. 228 – 243, 2008.

[4]. P. Hellekalek, S. Wegenkittl, “Empirical Evidence Concerning AES,” ACM Transactions on Modeling and Computer Simulation (TOMACS), Vol. 13, No. 4, pp.322-333, October 2003.

[5]. B. Schneier, “The Blowfish Encryption Algorithm – One Year Later,” Dr. Dobb‟s Journal, September 1995. Available:http://www.schneier.com/paper-blowfish-oneyear.html.

[6]. A.Biryukov, J. Nakahara, B.Preneel,J.Vandewalle, " New Weak Key Classes of IDEA, " Springer Berlin Lecture Notes in Computer Science, Vol.2513, pp. 315-326,2002.

[7]. A. Mousa, A. Hamad, "Evaluation of the RC4Algorithm for Data Encryption, "Proc. Of International Journal Computer Science & Applications, Vol.3, No.2, June 2006.