ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Improved AES for Data Security in E-Health

Aashmeen Jammu
Department of Electronics & Communication
Punjabi University, Patiala, India

Dr. Harjinder Singh
Department of Electronics & Communication
Punjabi University, Patiala, India

Abstract- In the last few years, there is transformation in quality of e-healthcare services provided by healthcare organizations. The patients' data is recorded in the digital form on the systems and communicated on the wireless network. Provision of security and resolving wireless attacks such as replay attack, eavesdropping, denial-of-service attack is the major concern. In the paper, improved AES algorithm is designed with one time padding of data to resolve reply attack on the wireless network. The simulation of algorithm is done in MATLAB 2014a. The performance and comparative analysis is done on the basis of different parameters such as avalanche effect, correlation factor, and execution time between existing and improved AES.

Keywords:*E-health security, attacks, AES, replay attack.*

I. INTRODUCTION

1.1 Overview of E-Health Care

Due to advancement in the technology the healthcare infra-structure is changing. The patients' record or databases are stored in electronic format enabling easy access of patient's record to the internet. The combination of electronic database and connection with internet provides an interface through which doctors remotely monitor patients [1] and improves the quality of health care. But, there are number of attacks on internet such as replay attack, denial of service attack *etc*. So, security and privacy of patients are of huge concern. In other words, due to advancement in medical field, the sensors are input on patients that sense the patients' health information and communicate information to doctors and hospital through wireless network as shown in fig 1. So, securing the sensor information on wireless network security is required.

1.2 Security Issues in E-Health Care [2]

In the e-healthcare, the following are the security issues:

- Unauthorized Patient Records

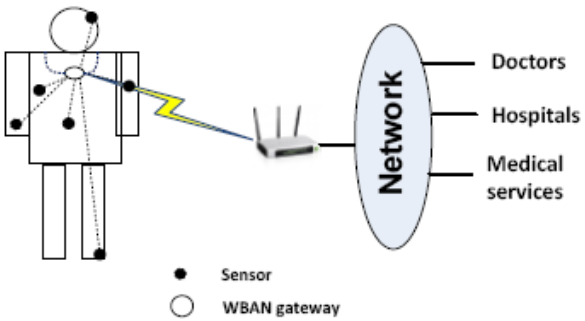

Fig.1 Block Diagram of Wireless Network in E-health Care

In e-healthcare, the patients' data is recorded in digital form and stored in databases. If roles and privileges are not properly defined between different users, then anyone can access database and may carry out any modification or action on it. As a result, data integrity and confidentiality are leaked.

- Attack Established on Host Estates

In three forms, the attack can be established on host estates. These are:

- Hardware Concession: The hardware concession generates serious concern for patients' data integrity.
- Software Concession: In software concession, the third party application installed by patient on software update enables the share of information on the network and also changes or malfunction the patient monitoring system.
- User Concession: In the user concession, there is unauthorized access of network and devices of the patients.

Because of this concession, there is loss of integrity of patients' information on the network.

1.3 Overview of Cryptography Algorithms for E-Health Care

To provide security and privacy on e-health care for patients' database, cryptography is used. Generally in cryptography, mathematical modeling is done to encrypt the data in another form so that it is difficult to understand. Cryptography has two types:

- Symmetric Cipher: In symmetric cipher, same key is used for encryption and decryption purposes and used for data encryption on the e-health care network. The key signifies a shared as well as a secret network between the communicating parties to maintain secrecy.
- Asymmetric Cipher: In the asymmetric ciphers, two key pairs are used. The keys are termed as public key and private key. The data is encrypted using public key and at the receiver side, users can only decrypt the data using private key. So, asymmetric ciphers are used for authentication purposes in e-health care.

The rest of the paper is organized as follows: Section 2 describes the related work done in this field and Section 3 presents motivation for proposed work, our contribution, working of improved algorithm, and their block diagram. In Section 4, proposed performance analysis is done on the basis of avalanche effect, execution time, and correlation factor. Conclusion is done in section 5.

II. LITERATURE SURVEY

In this section, e-health care security issues and encryption algorithms are discussed.

Puneet Kumar and Shashi B. Rana [3], worked on AES algorithm for data security. They designed a modified AES algorithm to provide more security. In this, one time padding (OTP) is done using polybius square matrix and increased number of rounds.

Hoang, *et al.* [4], worked on message encryption and authentication at MAC level, using AES forward cipher function with 128-bit key and cipher block chaining modes. They have designed ultra-low power 8-bit AES encryption core. Their implementation shows that their proposed AES-CCM IP core has lower power consumption and high resource efficiency.

Omar Cheikhrouhou [5], explained that wireless sensor network consists of large number of sensor nodes in an unattended harsh environment and exposed to different attacks such as replay attack, denial of service attack *etc*. In this paper, they worked on survey of secure group communication on wireless network and defined different approaches like centralized, contributory and hybrid. They also defined some research directions on which further work can be done.

III. Motivation and Proposed Work

In this section, motivation and proposed work are defined on the basis of literature survey.

Motivation and Contribution

The author **Puneet Kumar and Shashi B. Rana** [3] worked on AES algorithm and increased data security using OTP and increased number of rounds. For OTP, they are using non-linear function S-box. This increases the memory requirement and by increasing the number of rounds, execution delay also increases as compared to existing AES algorithm. Further, **Omar Cheikhrouhou** [5] defines that under unattended harsh environment wireless sensor nodes are exposed to different attacks.

In our proposed algorithm, replay attack is resolved by using random OTP on each iteration of message communication without using any extra non-linear S-box which reduces memory requirement as compared to existing modified AES algorithm [3].

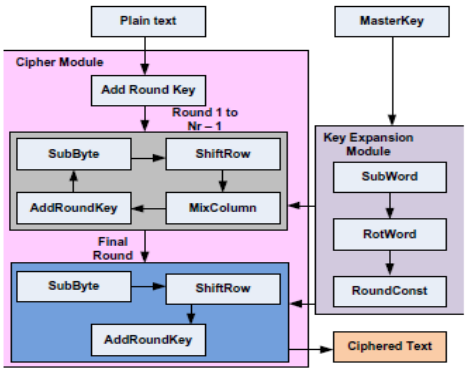

Fig.2 Block Diagram of AES [6]

3.1 Overview of AES Algorithm

The advanced encryption standard (AES) algorithm is based on substitution permutation network (SPN). It is approved by the national institute of standard and technology (NIST). AES is a symmetric block cipher which encrypts and decrypts the data using the same key.

In AES, the block cipher size is 128 bits. The key size is variable and is of 128 bits, 192 bits, or 256 bits. According to the size of key, the number of rounds varies like 10, 12, or 14 rounds [6-7]. The 128 bits are arranged into 4x4 matrices and each element of matrix is 1 byte long. The basic block diagram is shown in figure 2.

The steps of AES are as follows:

- Add Round Key: In this step, the input message of 4x4 matrix is XORed with 4x4 matrix of key. This is the first step in encryption process.
- Sub Byte: It is basically a substitution box. The sub byte performs a non-linear transformation on input data. The input data bytes are substituted with S-box values. The S-box of AES algorithm is based on Galois field. The construction of S-box has two transformations. The first transformation is performed by taking the multiplicative inverse in the finite field. In the second case, affine transformation is performed over GF(2).
- Shift Rows: In the AES algorithm, shifting of rows is done to create diffusion. In 4x4 matrix, first row is not shifted but 2^{nd}, 3^{rd}, and 4^{th} rows are rotated by 1 byte, 2 bytes, and 3 bytes.
- Mix Columns: In this, each column is multiplied with a polynomial. The multiplication process is modeled on the basis of Galois field. The mix column transformation can be expressed as follows:

$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

3.2 Improved AES algorithm: The improved AES algorithm includes work on one time padding (OTP) or initialization vector (IV). The advantage of OTP is that, encryption technique cannot be cracked after random padding is done. In OTP, modulo addition of each bit of plaintext is done with random bits of OTP. The OTP or IV generation for our work is shown in fig 3 and is as follows:

- The 128 bit input seed for IV is taken and arranged into 4x4 matrix.
- To create the non linearity with seed point, the IV is passed through S-box.
- Its XORing is done with original key.
- To create fast diffusion, the matrix rows are swapped.
- The correlation factor between the seed point and the updated IV is measured. The result shows that there is minimum correlation between the two matrices.

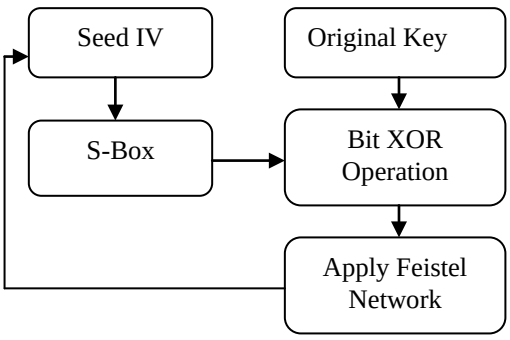

Fig.3 Block Diagram for Random IV Function

IV. Simulation Results and Performance Analysis

The algorithm is simulated in MATLAB 2014a and different performance parameters are measured.

- Execution Time to Encrypt Data

The *execution time* or CPU *time* of a given task is defined as the *time* spent by the system *executing* that particular encryption process.

- Correlation

Correlation is used to measure the level of security of encrypted information. Correlation is given as [8]

$$r(x,y) = \frac{Cov(x,y)}{\sqrt{var(x)}\sqrt{var(y)}}$$

Cov(x,y): Covariance between input and encrypted text

Covariance is given as:

$$Cov(x,y) = \frac{1}{N}[(x(i) - E(x))(y(i) - E(y))]$$

E(x) and E(y): Mean value of x and y

In ideal case, there is zero correlation between plain text and encrypted text.

- Avalanche Effect: The avalanche effect is a desirable property for algorithm security. It defines that, if any one bit changes in the data stream then there should be significant change in cipher data [8]. So, output significantly changes by flipping a single bit of input.

The execution time, correlation and avalanche effect for existing and improved AES are shown in table I and table II.

Table I Performance Analysis Parameters for Existing AES Algorithm

Plaintext	Key	Ciphertext	Execution Time(sec)	Correlation between Plaintext and Ciphertext	Avalanche Effect and Correlation between Two Ciphers
$\begin{bmatrix} 1 & 23 & 35 & 14 \\ 57 & 2 & 13 & 68 \\ 79 & 12 & 3 & 90 \\ 11 & 24 & 46 & 4 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 219 & 105 & 71 & 192 \\ 38 & 180 & 27 & 97 \\ 120 & 80 & 26 & 212 \\ 8 & 210 & 153 & 228 \end{bmatrix}$	6.21	0.0216	50.78% 0.0575
$\begin{bmatrix} 1 & 23 & 35 & 14 \\ 57 & 3 & 13 & 68 \\ 79 & 12 & 3 & 90 \\ 11 & 24 & 46 & 4 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 152 & 184 & 94 & 225 \\ 219 & 99 & 161 & 135 \\ 92 & 1 & 153 & 118 \\ 167 & 160 & 53 & 211 \end{bmatrix}$	6.12	-0.1853	
$\begin{bmatrix} 101 & 87 & 34 & 204 \\ 48 & 102 & 203 & 49 \\ 59 & 202 & 103 & 68 \\ 201 & 44 & 97 & 104 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 47 & 75 & 252 & 207 \\ 71 & 69 & 84 & 136 \\ 123 & 142 & 101 & 246 \\ 175 & 82 & 40 & 227 \end{bmatrix}$	6.10	0.0623	50% -0.1198
$\begin{bmatrix} 101 & 87 & 34 & 204 \\ 48 & 102 & 203 & 49 \\ 59 & 202 & 104 & 68 \\ 201 & 44 & 97 & 104 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 127 & 136 & 165 & 85 \\ 10 & 27 & 126 & 85 \\ 84 & 5 & 138 & 87 \\ 43 & 88 & 216 & 77 \end{bmatrix}$	6.09	-0.22	
$\begin{bmatrix} 8 & 35 & 64 & 19 \\ 27 & 99 & 115 & 82 \\ 47 & 83 & 219 & 204 \\ 108 & 17 & 54 & 5 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 62 & 184 & 169 & 159 \\ 214 & 170 & 227 & 127 \\ 190 & 152 & 123 & 149 \\ 36 & 122 & 229 & 129 \end{bmatrix}$	6.12	-0.0632	53.9063 -0.4729
$\begin{bmatrix} 8 & 35 & 64 & 19 \\ 27 & 99 & 115 & 82 \\ 47 & 83 & 219 & 205 \\ 108 & 17 & 54 & 5 \end{bmatrix}$	$\begin{bmatrix} 64 & 92 & 45 & 13 \\ 73 & 30 & 7 & 86 \\ 25 & 47 & 52 & 30 \\ 12 & 4 & 41 & 99 \end{bmatrix}$	$\begin{bmatrix} 159 & 164 & 11 & 90 \\ 170 & 79 & 33 & 4 \\ 67 & 245 & 196 & 215 \\ 197 & 226 & 12 & 215 \end{bmatrix}$	6.12	0.1054	

Table II Performance Analysis Parameters for Improved AES Algorithm

Plaintext	Key	Ciphertext	Execution Time(sec)	Correlation between Plaintext and Ciphertext	Avalanche Effect and Correlation between Two Ciphers
$\begin{bmatrix}1 & 23 & 35 & 14\\57 & 2 & 13 & 68\\79 & 12 & 3 & 90\\11 & 24 & 46 & 4\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}201 & 213 & 42 & 223\\68 & 102 & 33 & 16\\248 & 254 & 27 & 253\\29 & 254 & 14 & 178\end{bmatrix}$	6.17	0.08	52.34% -0.4118
$\begin{bmatrix}1 & 23 & 35 & 14\\57 & 3 & 13 & 68\\79 & 12 & 3 & 90\\11 & 24 & 46 & 4\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}19 & 62 & 194 & 104\\200 & 140 & 112 & 161\\218 & 82 & 118 & 75\\76 & 114 & 228 & 120\end{bmatrix}$	6.15	0.48	
$\begin{bmatrix}101 & 87 & 34 & 204\\48 & 102 & 203 & 49\\59 & 202 & 103 & 68\\201 & 44 & 97 & 104\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}136 & 128 & 141 & 144\\54 & 219 & 30 & 134\\32 & 157 & 170 & 65\\172 & 210 & 170 & 139\end{bmatrix}$	6.05	0.054	52.34% -0.08
$\begin{bmatrix}101 & 87 & 34 & 204\\48 & 102 & 203 & 49\\59 & 202 & 104 & 68\\201 & 44 & 97 & 104\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}61 & 29 & 187 & 202\\63 & 11 & 196 & 142\\79 & 177 & 213 & 59\\13 & 87 & 113 & 109\end{bmatrix}$	6.10	0.26	
$\begin{bmatrix}8 & 35 & 64 & 19\\27 & 99 & 115 & 82\\47 & 83 & 219 & 204\\108 & 17 & 54 & 5\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}167 & 229 & 94 & 206\\39 & 95 & 0 & 99\\255 & 234 & 114 & 74\\121 & 140 & 227 & 210\end{bmatrix}$	6.09	0.44	50.78% -0.46
$\begin{bmatrix}8 & 35 & 64 & 19\\27 & 99 & 115 & 82\\47 & 83 & 219 & 205\\108 & 17 & 54 & 5\end{bmatrix}$	$\begin{bmatrix}64 & 92 & 45 & 13\\73 & 30 & 7 & 86\\25 & 47 & 52 & 30\\12 & 4 & 41 & 99\end{bmatrix}$	$\begin{bmatrix}247 & 71 & 192 & 41\\198 & 142 & 127 & 87\\91 & 83 & 171 & 212\\40 & 200 & 86 & 122\end{bmatrix}$	6.18	0.11	

The results show that the improved AES has better security and approximately same execution time as existing AES.

V. CONCLUSION

In this paper, encryption algorithms are surveyed for e-health attacks. Based on survey, motivation is defined and an improved AES algorithm that resolves replay attack on the wireless sensor network is proposed. The performance analysis for the improved AES algorithm is done on the basis of execution time, avalanche effect, and correlation factor. The results show that the improved AES is more secure by using approximately same resources as compared to existing AES algorithm and has almost same execution time with IV.

VI. REFERENCES

[1] Pardeep Kumar and Hoon-Jae Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Network: A Survey," Sensors, Vol. 12, pp. 55-91, December 2011.

[2] Patience E. Idoga, Mary Agoyi, Elizabeth Y. Coker-Farrell, and Gazi L. Ekeoma, "Review of Security Issues in E-Healthcare and Solutions," IEEE conference on HONET-ICT, pp.118-121, October 2016.

[3] Puneet Kumar and Shashi B.Rana, "Development of Modified AES Algorithm for Data Security," Optik Journal, Vol. 127, pp. 2341-2345, November 2015.

[4] Van-Phuc Hoang, Thi-Thanh-Dung Phan, Van-Lan Dao, and Cong-Kha Pham, "A Compact, Ultra-Low Power AES-CCM IP core for Wireless Body Area Network," IFIP/IEEE International Conference on Very Large Scale Integration, November 2016.

[5] Omar Cheikhrouhou, "Secure Group Communication on Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, Vol. 61, pp. 115-132, November 2015.

[6] Umar Farooq and M. Faistal Aslam, "Comparative Analysis of different AES Implementation Techniques for Efficient Resources Usage and Better performance," Journal of King Saud University-Computer and Information Sciecne, 2016.

[7] Daemen, J., Rijmen, V., 2000. The block cipher Rijndael, 1820, 277–284.

[8] Gaurav Bansod, Narayan Pisharoty, and Abhijit Patil , "BORON: an ultra lightweight and low power Encryption Design for Pervasive Computing," Frontiers of Information Technology and Electronic Engineering, Vol. 18, pp. 317-331, 2017.

