International Journal of Engineering & Technology, *7 (2.20) (2018) 64-66*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Light weight encryption algorithms for wireless body area networks

CH. Radhika Rani[1], Lakku Sai Jagan[2], Ch. Lakshmi Harika [3], V.V. Durga Ravali Amara [4*]

[1]Professor, Department of Computer Science & Engineering, K L E F Deemed to be University,
Vaddeswaram, Guntur (Dt), Andhra Pradesh, India.
[2]IV/IV B.Tech CSE Student, K L E F Deemed to be University, Vaddeswaram, Guntur (Dt), Andhra Pradesh, India.
[3]IV/IV B.Tech CSE Student, K L E F Deemed to be University, Vaddeswaram, Guntur (Dt), Andhra Pradesh, India.
[4]IV/IV B.Tech CSE Student, K L E F Deemed to be University, Vaddeswaram, Guntur (Dt), Andhra Pradesh, India.
**E-mail:amararavali96@gmail.com*

Abstract

Wireless Body Area Network (WBAN) emerges as a major network in today's world. WBAN comprise of sensors used for applications like health monitoring, military, etc. These sensors are embedded within or out of the body. Security is a major factor in WBAN's and hence it is essential to provide security for patient's data. So we study about various encryption algorithms in this paper to provide security. The WBAN comprise of body sensors in which the energy resources are limited and since consumption of energy will be more it is essential to go for light weight algorithms to provide security and decrease energy consumption.

Keywords: *WBAN, security, lightweight encryption algorithms, Blowfish.*

1. Introduction

WBAN is designed for many applications like military, health applications, industries, etc. In health care monitoring we have to provide safety[22] to the data related to health parameters (temperature, BP, heartbeat, etc) [1-2]. In WBAN we use some Encryption Algorithms to provide Security [12]. As the resources of body sensors are very limited in WBAN we go for lightweight encryption algorithms. By using the lightweight encryption algorithms [14,15] the consumption of energy will be low, and security is provided. There are many Encryption Algorithms [8] like DES, 3DES,AES,Blowfish, SIT, RSA[22], DSA, ECC, Diffie-Hellman key Exchange etc.

Encryption

It is basically a mechanism which is used for converting understandable text to some complex textual content. This mechanism will help us to protect the private data from intruders. To make this encrypted text readable, we use keys to know the data we have encrypted.

2. Related work

There are mainly two categories of encrypting algorithms namely[23] Symmetric Encryption which is also called as secret key Algorithms [3,21] and Asymmetric Encryption Algorithms which is otherwise called as public key. There are two primary uses that these algorithms provide:

- Authentication
- Confidentiality

Symmetric encryption algorithms

Symmetric Algorithm [11] is defined as the algorithm that makes use of parallel key equally for encoding and decoding the data. This symmetric algorithm encodes and decodes various algorithms like AES, DES etc. It is a cryptographic algorithm and known as secret key algorithm. The Symmetric algorithms are:DES [4,5], 3DES,AES [19], SIT and Blowfish[4,5].

Asymmetric encryption algorithms

This kind of algorithms uses two dissimilar keys notable as a secret key and public key(Open) which are used for both enciphering, deciphering the data. The general Public key might be shared with anyone, trusted or may not be trusted party, but Private key is shared only with authorized persons. These are few examples of Asymmetric Algorithms: DSA algorithm, RSA[14] algorithm, Elliptic Curve Cryptography[18], Diffie Hellman Key Exchange Algorithm. All these asymmetric algorithms are used for providing signature and verification of the authenticated users. Our prime objective is on Data Encryption and decryption. Hence, we need to choose an algorithm from a set of Symmetric Encryption algorithms which are less complex and faster.

DES [10] is a symmetric algorithm which uses the similar key to encode and decode the data. It uses a input key of size 56 bits plus 8 parity bits and a block range of 64 bit.

3DES is a symmetric algorithm which uses three keys to encipher and decipher the information. It uses a input key of size 168,112 or 56 bits. Table1 shows the differences between DES and 3DES.

Table 1: DES and 3DES

DES	3DES
i) DES means Data Encryption Algorithm and it uses a key size of fifty-six bits.	i) 3DES means Triple Data Encryption Algorithm and it uses a input key size of 168 bits, 112 bits or 56bits.
ii) Its uses 64 bits as block size.	ii) Its block size is of 64 bits.
iii) It takes 16 rounds for translating the data	iii) It takes 48 rounds for translating the data
iv) It works with a single key to encode and decode the data.	iv) It uses three different keys to encode and decode the data.
v) DES provides security	v)3DES is safer than DES
vi) DES is a slow processor	vi) 3DES is much slower processor than DES.

AES is a secret key algorithm which is also referred as symmetric block cipher, uses a single key for both decryption and encryption. AES Algorithm unlike the DES doesn't have a static block size and key size. Key size may vary among128,192,256. However Standard AES has fixed input block size of 128bits.Based on the keys used, AES is categorized as AES-128, AES-192 or AES-256.

- AES is extra protected than DES
- Supports larger key sizes than 3DES does.
- The 128-bit block range of AES makes it less open to attack via birthday problem than 64 bit block size of 3DES.

However, AES is difficult to implement in software in a manner of together safety and performance.

Secure Internet of Things (SIT) is one of the encryption algorithms which are symmetric block cipher and they contain a key length of 64bit and plain-text. This algorithm comprises of encryption rounds inside the encryption Process. Every encryption encircling is dependent on certain numerical functions to make doubt and diffusion. As the rounds go on increasing the security also increases, but inversely the energy consumption will increase. A Cryptographic algorithm is usually meant for altering the data from readable form to protected form which are to take on an average 10 to 20 rounds to have the encrypting process well-built. However, SIT algorithm is restricted to have only the rounds, to increase the liveliness efficacy, every round of encryption comprises scientific operations which perform the operation on a data of four bits this algorithm utilizes the festal network community of diffusion functions. As WBAN's requires high security, this SIT Encryption cannot provide the required security since the number of rounds is only five and the Key size is also 64 bit only.

Blowfish Algorithm is an algorithm used for symmetric encryption algorithmic mechanism. Blowfish Feistel block cipher which comprises of 16rounds in encipher and 64bits as a block size. The key length can be from 32-448 bits and this algorithm provides better security than the other algorithms.

So, we are proposing this algorithm for obtaining data security in WBAN.

3. Model work and analysis

Blowfish algorithm

Blowfish Algorithm is a symmetric encryption algorithmic mechanism. This is a Feistel block cipher [9] which comprises of 16 rounds and 64 bits block size. The key length can be from 32-448 bits. There are two important things to learn about the architecture of blowfish algorithm [6].

i) Blowfish uses 4-large S-tables which requires embedded RAM.

ii) The second important thing is it has a recursive key length schedule. This Algorithm has been constructed in a way that it has the consideration with:

Fast: This Blowfish Algorithm encrypts the data on microprocessors with 32 bits at a speed rate ofTwenty- six (26) clock cycles as per every byte.

Compact: This algorithm can route in a less time of 5k memory.

Simple: In this blowfish algorithm we use some simple operations like addition, XOR, a Lookup table with 32-bit operands.

Secure: This Algorithm provides security and it is appropriate for every application where the key would not get changed frequently, like the communication link or a self-regulating file encryptor.

A symmetric type block cipher algorithm such as blowfish algorithm that uses the input key length as 32-448 bits to encipher the information. It has a block size of sixty-four (64) block bit.

This Blowfish Algorithm has two segments [7]:

i) Key Expansion

ii) Data Encryption

i) Key expansion

In the key expansion, it translates the key size of 448 (Four forty-eight) bits into numerous sub key arrays totaling all them into 4168 bytes. Huge number of sub keys is used for blowfish algorithm.

The p-array called the sub key array it comprises of 18 arrays and a size of thirty two (32) bit sub keys.

P1, P2, P3, - - - - - - - - P18

Blowfish algorithm has four s-boxes with 32 bit size which comprises of Two fifty six (256) entries each.

I.e. in the from of

[S1, 0], [S1, 1], - - - - - - - - - - [S1, 255]
[S2, 0], [S2, 1], - - - - - - - - - - [S2, 255]
[S3, 0], [S3, 1], - - - - - - - - - - [S3, 255]
[S4, 0], [S4, 1], - - - - - - - - - - [S4, 255]

Generating the sub keys

Using Blowfish algorithm, the sub keys are produced in the subsequent way.

Step 1: Basically set the P-exhibit and in this manner the S-encloses arrange with an inflexible string. The string we have given that contains of the hexa-decimal digits of Pi (less the underlying 3).

P1= 0*243f6a88, P2=0*85a308d3...... etc.

Step 2: After that XOR P1 with the initial 32 bits of the info key, XOR P2 with the second 32-bits of the information key and in like manner for every one of the bits of the information key (conceivably up to P14). Over and again duplicate these procedures until all the P-exhibit has been XORed with all the key bits.

Step 3: Encipher all the zero strings by the blowfish calculation using the sub keys made in the step1 and step2.

Step 4: The output is produced in step3. In this step substitute P1 and P2 with the yield produced in the step3.

Step 5: Using the blowfish algorithm we will encrypt the output produced in step3 with the improved sub keys.

Step 6: Substitute P3 and P4 with the result of the Step5.

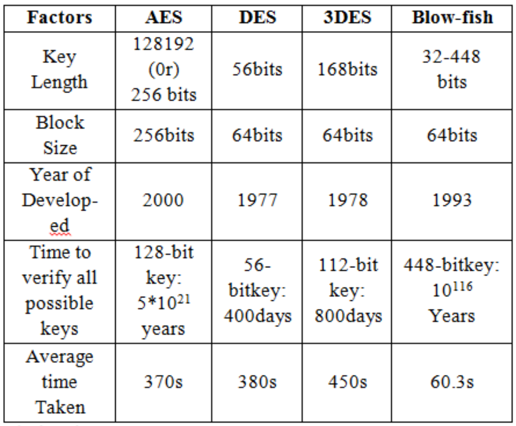
Step 7: Prolong the process, Till every entries in the P-array are substituted and all the four S-boxes also.

ii) Data encryption

In data encryption first, we have to divide the key into two parts i.e., xRIf the key is 64 bit we must divide the 64-bit key size into halves that are xL=32 and xR=32 The Blowfish which is used as encryption algorithm is described as follows:

i)First divide the input X into two 32-bit halves i.e,xL, xR

Table 2: Different Factors of Various Encryption Algorithms



Factors	AES	DES	3DES	Blow-fish
Key Length	128192 (0r) 256 bits	56bits	168bits	32-448 bits
Block Size	256bits	64bits	64bits	64bits
Year of Develop-ed	2000	1977	1978	1993
Time to verify all possible keys	128-bit key: $5*10^{21}$ years	56-bitkey: 400days	112-bit key: 800days	448-bitkey: 10^{116} Years
Average time Taken	370s	380s	450s	60.3s

ii)i=1;

iii) While i<=10

iv) xL= xL XOR Pi

v) xR = F(xL) XOR xR

vi) Swap XL and xR

vii) Swap XL and xR (undo the last swap)

viii) xR = xR XOR P17

ix) xL = xLxor P18

x) Recombine xL and xR.

Benefits of the Blowfish encryption algorithm

- Blowfish algorithm has a simple structure which is very effective, and it is a fast cipher.
- This Blowfish algorithm generates some sub keys which very large and these produce a huge benefit for providing security.
- In Blowfish the people are unable to hack the key because we create and generate a large and it is more difficult to be hacked.
- When the sub keys are generating in these sub keys each pair of sub keys changes slightly. This prevents the attackers from knowing out how the sub keys are getting generated.
- Blowfish is especially hard against attacks because of the density of the sub key generation.

Comparison of Algorithms based on time taken for execution

Table 2 shows the comparison of algorithms[17] based on the time of execution, from which we can say that blowfish takes less time to encrypt and it is the best algorithm for encrypting the data in wireless body area networks.

4. Conclusion

From the study of various encryption algorithms, we can notice that Blowfish is the best Encryption Algorithm compared to other algorithms. It is also known that Blowfish Algorithm doesn’t have any security weak points which makes it excellent standard Encryption Algorithm for WBAN’s. This Algorithm is also not yet been cracked and it is the fastest encryption algorithm.

References

[1] Daojing SC & Shaohua, A Novel and a Lightweight System to Secure Wireless Health Sensor Networks”, *IEEE Journal Of Biomedical AndHealth Informatics*, Vol.18, No.1, (2014), pp.23-32.

[2] Trcek, D & Brodnik A, “Hard and soft security provisioning for computationally weak pervasive computing systems in e-health”, *IEEE Wireless Communications*, Vol.20, No.4,(2013), pp.22-29.

[3] Surya E & Divya C, “A Survey on Symmetric Key Encryption Algorithms”, *International Journal of Computer Science & Communication Networks*, Vol.2, No.4, (2012), pp.475-477.

[4] Coppersmith D, “The Data Encryption Standard (DES) and its strength against attacks”, *IBM journal of research and development*, Vol.38, No.3, (1994), pp.243-250.

[5] Nie T & Zhang T, “A study of DES and Blowfish encryption algorithm”, *IEEE Region 10 Conference Tencon*,(2009), pp.1-4.

[6] Manap C & Kara O, “A novel class of weak keys for blowfish algorithm”, *Fast Software Encryption*, (2007), pp.167-180.

[7] Nakahara J, “A linear analysis of Blowfish and Khufu”, *International Conference on Information Security Practice and Experience*, (2007), pp.20-32.

[8] Nadeem A & Javed MY, “A performance comparison of data encryption algorithms”, *First international conference on Information and communication technologies*, (2005), pp.84-89.

[9] Schneier B, “Description of a new variable-length key, 64-bit block cipher (Blowfish)”, *International Workshop on Fast Software Encryption*, (1993), pp.191-204.

[10] DES federal Information Processing Standards Publication 1981 and the Guidelines for Implementing and Using the Nbs Data Encryption Standard Uspateent 3798359: Block cipher Cryptographic SystemFiestel: Horst, Mar. 19,1974.

[11] Agrawal H & Sharma M, “Implementation and analysis of various symmetric cryptosystems”, *Indian Journal of science and Technology*, Vol.3, No.12,(2010), pp.1173-1176.

[12] Saleem S, Ullah S & Yoo HS, “On the security issues in wireless body area networks”, *JDCTA*, Vol.3, No.3,(2009), pp.178-184.

[13] Durresi A, Paruchuri V, Kannan R & Iyengar SS, “A lightweight protocol for data integrity in sensor networks”, *Proceedings of the Intelligent Sensors, Sensor Networks and Information Processing Conference*, (2004), pp.73-77.

[14] Kamel I & Juma H, “A lightweight data integrity scheme for sensor networks”, *Sensors*, Vol.11, No.4, (2011), pp.4118-4136.

[15] Dhakar RS, Gupta AK & Sharma P, “Modified RSA encryption algorithm (MREA)”, *Second International Conference on Advanced Computing & Communication Technologies (ACCT)*, (2012), pp.426-429.

[16] Raju GVS & Akbani R, “Elliptic curve cryptosystem and its applications”, *IEEE International Conference on Systems, Man and Cybernetics*, Vol. 2, (2003), pp.1540-1543.

[17] Daemen J & Rijmen V, “Rijndael: The Advanced Encryption Standard”, *D r. Dobb's Journal*, (2001).

[18] Singh SP & Maini R, “Comparison of data encryption algorithms”, *International Journal of Computer Science and Communication*, Vol.2, No.1,(2011), pp.125-127.

[19] Sathya D, Kokilavani S & Krithika S, “Providing Security to Medical Data”, *Wireless Communication*, Vol.8, No.2,(2016), pp.86-89.

[20] Singh S & Bisht N, “A comparative study of asymmetric and symmetric algorithms”, *International journal of Innovative Research in science, engineering and technology*, Vol.4, (2015).

[21] Kaur G & Mahajan M, “Evaluation and Comparison of Symmetric key algorithms”, *International Journal of Science, Engineering and Technology Research (IJSETR)*, Vol.2, No.10,(2013).

[22] Singh G, “A study of encryption algorithms (RSA, DES, 3DES and AES) for information security”, *International Journal of Computer Applications*, Vol.67, No.19, (2013).