International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31555-31564
© Research India Publications
http://www.ripublication.com

A Novel Approach for Secure Data Gathering in Body Area Network Using PRESENT Algorithm

Blessed Prince. P* Dr.K.Krishnamoorthy[2] Anandaraj. R[3] Jeno Lovesum S.P[4]

[*]Department of Information Technology, Karunya University, India
[2]Department of Computer Science and Engineering,
Sudharsan College of Engineering, India
[3]Department of Information Technology, Karunya University, India
[4]Department of Computer Science and Engineering, Karunya University, India
**blessedprince@gmail.com*

Abstract

Recent development in mobile technologies has made the developers to design numerous healthcare applications which allow the patient to upload their health information to the third party server for diagnosis. Such healthcare applications collect patients' health information from wearable body area sensors and offers high security to the data while storing it into the cloud server. But there is a chance that, sensitive health data can be subjected to malicious attacks while transferring from sensor to the personal devices. Hence, in this paper we have used the PRESENT algorithm (an ultra lightweight cryptographic algorithm) to provide high security to data involved in a Body Area Network. From the result analysis we ensure that, our model is highly compatible with the resource constraint networks in terms of security and power consumption. Also our approach replaced traditional zigbee communication protocol with wi-fi mechanism to achieve flexible and long distance data transmission.

Key words – Mobile technology, healthcare, security, body area network, cloud server.

I. INTRODUCTION

Advancement in recent computing models like mobile computing and cloud computing has bought wide range of changes in the field of e- healthcare. A large number of applications has been developed to offer real time health monitoring services or to have a remote diagnosis. These applications collect patients' health

information like ECG signals, oxygen saturation in blood, pulse rate, glucose level, body temperature and etc... These information being the sensitive data, are transferred to the remote stations with high security.

The primary part of these e-healthcare applications were data gathering phase. In which patients' were made to wear bio sensors, and using wireless transmissions like Bluetooth or Wi-Fi the health information were sent to mobile devices. According to HIPAA federal act, 1996 healthcare applications should offer confidentiality and integrity to the patient health information. With the view of satisfying HIPAA constraints, such e-healthcare applications implements security algorithm over the health information. These security algorithms encrypt the health data before uploading it to the remote server.

Even though the existing healthcare applications offers security to the health data which resides in their personal devices like mobile phone or laptop, There is a high demand for securing the health information during collection phase itself because modern healthcare applications (as stated earlier) collects the health information from wearable body sensors through wireless transmission. Wireless transmission is vulnerable to various attacks like eavesdropping, node compromising etc… Hence it is mandatory to regulate the data gathering phase by implementing cryptographic algorithm before collecting it in the mobile devices.

Wireless Body Area Network (WBAN) resembles a wireless sensor network with various bio sensors, hence it can be categorized as a resource constraint network. We proposed a new approach to perform secure data gathering using an ultra lightweight, secret key cryptographic algorithm called PRESENT. Which is highly compatible for chip based applications and consumes low power in order to increase the efficiency of resource constraint networks. PRESENT algorithm takes key of about 80 bit and generates a cipher, the same secret key can be shared with the authorized device to perform decryption. Interesting factor about PRESENT is that, the key size can be expanded to 120 bit for higher degree of security.

The remaining part of the paper is organized as follows, section II contains the related works about body area networks, followed by implementation of PRESENT algorithm in Section III. Section IV explains the performance results of the proposed model and conclusion.

II. RELATED WORKS

This section describes the various works associated with secure data gathering in body area networks.

Axel York Poschmann Bochum in 2009, states that, In the body area network an adversary has physical access to or control over the devices, which enables the whole field of physical attacks. Also obtaining high throughput is usually not an issue but energy, power and area can be constraints. Thus is it mandatory to implement an encryption algorithm during data gathering phase to avoid malicious attacks also algorithm should be compatible with resource constraint networks like body area network.

Siva Sangari et al [1] in 2014, proposed a lightweight security mechanism for sensor data gathering using skipjack algorithm. It achieves the data encryption in 25 micro seconds. But skipjack algorithm adopts the symmetrical structure which leads to slide attacks [2].

HEIGHT, a lightweight cryptographic algorithm is proposed by Hong et al in 2006 [3]. It works in 64 bit states and takes 128 bit long message as key and generates a cipher in 32 rounds. In addition HEIGHT equals GE value of about 3.048.

Lim and Korkishko proposed an 64 bit state algorithm known as mcrypton in 2006 [4], mcrypton extends adds flexibility in key size of 64 bit. 96 bit and 128 bit long. Mcrypton performs encryption in 13 rounds.

In 2006 another lightweight cryptographic algorithm called Scalable Encryption Algorithm (SEA) has been proposed [5]. It offers better security alike above mentioned algorithms by taking 96 bit key size. Wheeler and Needham proposed an lightweight algorithm called Tiny Encryption Algorithm [6]. TEA algorithm takes 128 bit long message as key and performs cryptographic mechanism in 64 rounds.

III DATA SECURITY USING PRESENT ALGORITHM

In this paper we adheres the objective of secure data gathering in a wireless body area network. The designed body area network collects data from multiple body area sensors and dumps it to the centralized collector node through wireless medium. To encapsulate the health data during transmission, we selected an ultra-lightweight cryptographic algorithm called PRESENT with the following constraints,

- Sensitive data processing
- Long distance communication
- Hardware based cipher generation
- Faster and simple implementation

In this paper we illustrates the clear cut architecture of PRESENT algorithm with a reference to research work of Axel Poschmann (2009) on lightweight cryptographic, a cryptographic engineering for pervasive world [7]. PRESENT algorithm is a block cipher, which takes each block of size 64 bits and key size of about 80 bits. As an additional feature the size can be increased to 128 bits long.

PRESENT is an iterative algorithm which performs encryption and decryption in 32 rounds. And each round is provided with an 80 bit long round key. Figure 3.1 shows the encryption routing of the PRESENT algorithm along with a short notation to substitution and permutation layers.

```
generateRoundKeys()
for i = 1 to 31 do
    addRoundKey(STATE,K_i)
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,K_32)
```

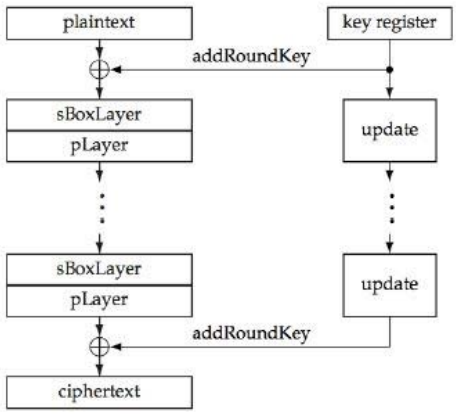

Fig 3.1 Encryption routine of PRESENT

Initial process of PRESENT algorithm involves the generation of addRoundKey. This process takes 64 bit message block as input and generates a round key K.

$$K_i=K^i_{63}.....K^i_0$$

$$b_j=b_j \oplus K^i_j$$

Where 1<i<23 & 0<j<63

During the encryption process, PRESENT alters the position of every bits in the given input according the pre defined S box. The algorithm uses 4 bit to 4 bit S box, which shows the better improvement in avalanche of chance. The Fourier co-efficient of S box can be represented as,

$$S^w{}_b(a) = \sum_{x \in F}(-1)\hat{}(b, S(x)) + (a, x)$$

The securely designed S box satisfies following condition,

- $\{x \in F^4_2 \mid S(x) + S(x + \Delta_I) = \Delta_O\} \leq 4$
- $\{x \in F^4_2 \mid S(x) + S(x + \Delta_I) = \Delta_O\} \leq \Phi$
- For every non-zero $a \in F^4_2$ and $b \in F^4_{2,} \mid S^w{}_b(a) \mid \leq 8$
- For every non-zero $a \in F^4_2$ and $b \in F^4_{2,} \mid S^w{}_b(a) \mid \leq 4$

Where,
Δ_I = Small difference in non-zero input,
Δ_O = Small difference in non-zero output
Table I shows the S box used in PRESENT algorithm to achieve ultra lightweight encryption process.

Table I PRESENT S-BOX

X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Focusing on efficient hardware implementation, algorithm is designed with minimum processing elements. Thus pLayer can be generated as follows,

$$P(i) = \{i.16 \bmod 63, i \in 0,1,\ldots.62\}$$

$$\{63\ I = 63\}$$

On achieving successful encryption, the cipher information is transferred to the sink, where decryption starts. Figure 3.2 illustrates the decryption routing of PRESENT algorithm.

```
generateRoundKeys()
addRoundKey(STATE,K32)
for i = 31 downto 1 do
   invPLayer(STATE)
   invSBoxLayer(STATE)

   addRoundKey(STATE,Ki)
end for
```

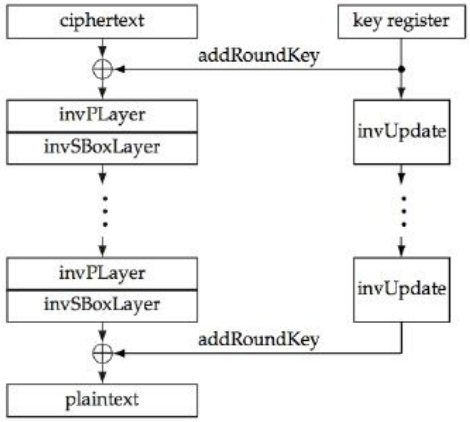

Fig 3.2 Decryption routine of PRESENT

PRESENT algorithm makes decryption flexible by inverting the substitution and permutation layer.

IV IMPLEMENTATION

In this research contribution, we designed a hardware architecture for secure gathering of sensitive health information using ultra lightweight cryptographic algorithm called PRESENT. This section explains the hardware and software implementation, required to achieve secure data gathering. On focusing the hardware implementation, we considered a set of body area sensors which collects and sends the sensitive data to the centralized controller which in turn performs encryption and transmits health data

into the network. The wireless communication channel is created using Wi-Fi signals and data packets were controlled by a local router to dump the collected data in a patients hand held devices.

HEALTH SENSORS

To collect sensitive health information from patient, we mounted two body area sensors namely micro sphygmomanometer and temperature sensors. These health sensors can act as collector nodes and dumps the sensitive information to the micro controller. Figure 4.1 explains the diagrammatic representation of proposed hardware implementation.

MICRO SPHYGMOMANOMETER

We used sphygmomanometer to measure the blood pressure of a patient and dumps the BP value to the handheld devices. The unit of measurement adopted by sphygmomanometer is mmHg.

TEMPERATURE SENSOR

Another sensor component called temperature sensor is integrated to our controller board to measure the active body temperature of the patient.

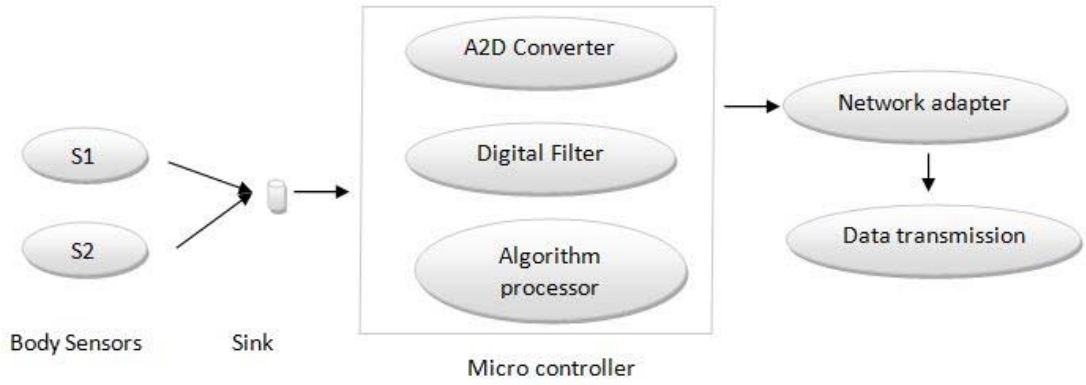

Fig 4.1 Block representation of proposed hardware model

By referring to figure 4.1, it has been observed that the sensors s1 and s2 collects the sensitive health information and sends the data to a centralized node called S. Micro controller performs primary signal processing mechanisms like digital conversion and filtering over the collected data. After successful processing, the health information were encrypted and transmitted into the network using integrated network adapter.

Also to perform cryptographic mechanism, we implemented the ultra lightweight algorithm PESENT in the algorithm processor. Our software implementation abides with the implementation requirement listed in [8].

V PERFORMANCE ANALYSIS

Body Area Network belongs to resource constraint network. It is important to maintain the low power consumption technology for any resource constraint environments. In our work we have created a hardware to depict how the interaction among sensor nodes takes place in a Body Area Network. While collecting the data from the sensor to the system the sensor data are made secure by using PRESENT algorithm which is an ultra-light weight cryptographic algorithm. The hardware is designed in such a way to provide high security to sensitive data while transferring it to the handheld devices. We compare the performance of PRESENT algorithm with likely designed other lightweight algorithms and we estimated the computational time, memory consumption of the PRESENT algorithm. Figure 5.1 illustrates the encryption time consumed by the PRESENT algorithm.

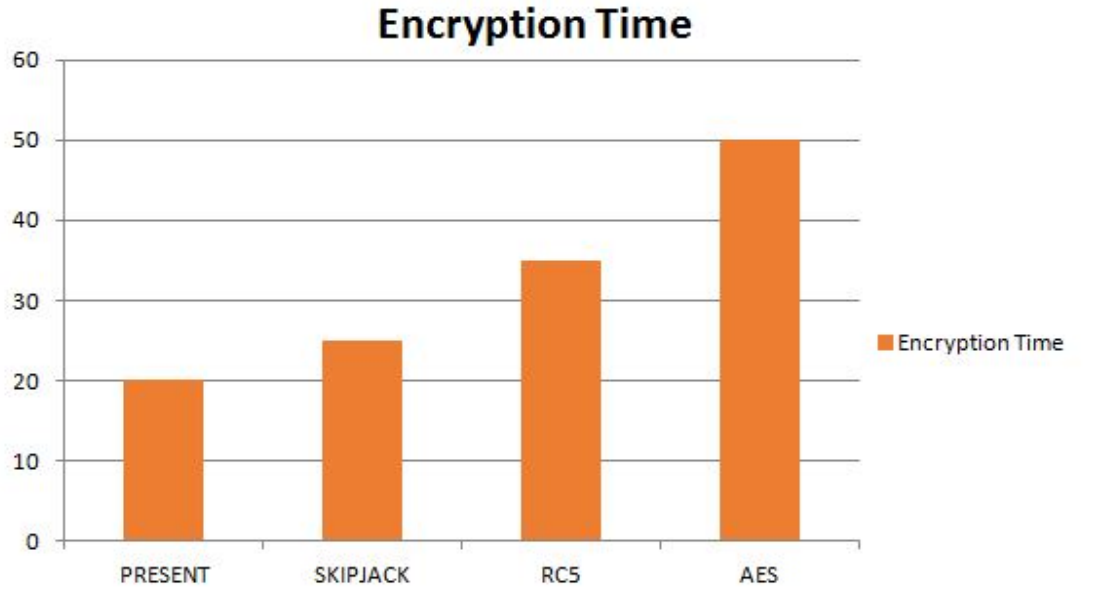

Fig 5.1 Encryption time of various lightweight algorithms

From figure 5.1, It has been observed that, PRESENT algorithm takes minimum encryption time of about 20 µs which is 2.5 times less than the AES computational time. And figure 5.2 explains the memory consumed by PRESENT for performing cryptographic mechanisms and it has been observed that, processing of PRESENT algorithm can be done by consuming very low memory of about 1500 bytes. The result seems to be the lowest value, when compared to other resource constraint implementations like skipjack, SEA and TEA.

Even though we obtained desirable results on computational time and memory consumption using PRESENT algorithm, Based on the GE property of light weight algorithms from Figure 5.3 it is inferred that PRESENT consumes minimum GE value of 1.5 GE.

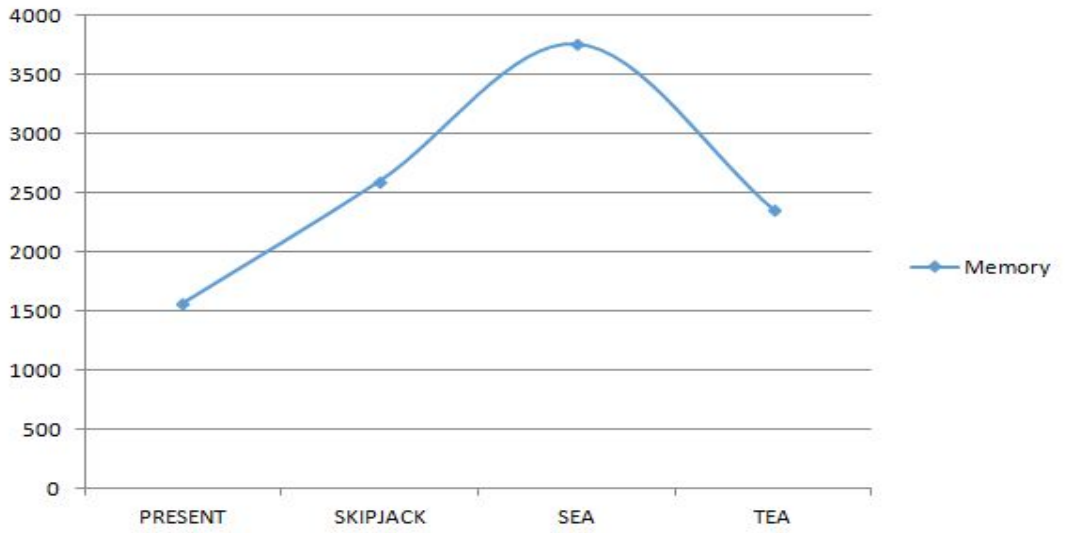

Fig 5.2 Memory consumption in bytes

Software implementation.

The notation explicitly means that the algorithm takes 80 bit long key for message processing. Cryptographic linearity principle conveys that, there exists an increase in GE values, when increasing the key size. Figure 5.3 defines the GE Vs Key size relation of various algorithms.

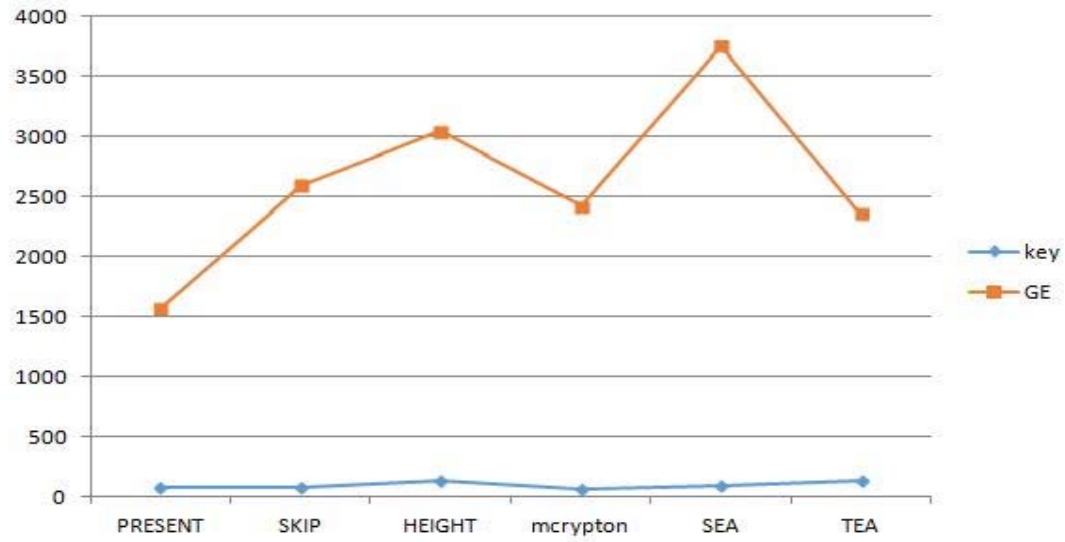

Fig 5.3 GE Vs Key size relationship

Also we inferred that, PRESENT structure consumes maximum area value of 1.5067 GE for efficient operation.

VI CONCLUSION

In this paper we have explained how high security can be provided to the sensitive data while transferring it from the sensor nodes to the handheld devices, and this has been demonstrated using the hardware that we created for collecting the data from the sensor nodes, the ultra lightweight cryptographic algorithm PRESENT has been integrated into the controller board to achieve secure data transmission between sensor nodes and patients mobile device. To enable faster and long distance communication, we replaced the traditional low distance Bluetooth architecture and zigbee architecture with Wi-Fi communication protocol. We analyzed the performance of PRESENT algorithm in terms of computational time and memory utilization. The result analysis shows that for resource constraint devices the PRESENT algorithm best suites since the algorithm takes only 25 μs on an average for encryption and maximum of 1500 bytes of memory is only consumed.

VI REFERENCES

[1] A Siva Sangari and J Martin Leo Manickam, Lightweight security and authentication in wireless body area networks, Indian journal of computer science and engineering, Vol 4 No 6, Jan 2014.

[2] Lars Knudsen and David Wagner, On a structure of skipjack, Discrete applied mathematics, Elseiver Science, 111 (2001) 103-116, 2001.

[3] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In L. Goubin and M. Matsui, editors, Cryptographic Hardware and Embedded Systems — CHES 2006, number 4249 in Lecture Notes in Computer Science, pages 46–59. Springer-Verlag, 2006.

[4] C. Lim and T. Korkishko. mCrypton - A Lightweight Block Cipher for Security of Lowcost RFID Tags and Sensors. In J. Song, T. Kwon, and M. Yung, editors, Workshop on Information Security Applications — WISA 2005, volume 3786 of Lecture Notes in Computer Science, pages 243–258. Springer-Verlag, 2005.

[5] F.X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater. SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, Smart Card Research and Applications, Proceedings of CARDIS 2006, volume 3928 of Lecture Notes in Computer Science, pages 222–236. Springer-Verlag, 2006.

[6] D. Wheeler and R. Needham. TEA, a Tiny Encryption Algorithm. In B. Preneel, editor, Fast Software Encryption — FSE 1994, volume 1008 of Lecture Notes in Computer Science, pages 363–366. Springer-Verlag, 1994.

[7] Axel York Poschmann, Lightweight cryptography, a cryptographic engineering for a pervasive world, Research work at Ruhr-University Bochum, Germany, February 2009.

[8] Christophe Oosterlynck and Philippe Teuwen Python version of PRESENT implementation, 2008.