SECURITY AND PRIVACY IN IOT BASED HEALTHCARE

Dr. A. Sivasangari

Professor, Department of CSE

Sathyabama Institute of Science and Technology

Chennai- 600119.

JUPITER PUBLICATIONS CONSORTIUM
INDIA

Jupiter Publications Consortium
22/102, Second Street, Virugambakkam
Chennai - 600 092. www.jpc.in.net
Email: director@jpc.in.net

Acknowledgments:

Any trademarks, service marks, product names, or named features are assumed to be the property of their respective owners and are used only for reference. There is no implied endorsement if we use one of these terms.

Published by:

Jupiter Publications Consortium, [August, 2024]

SECURITY AND PRIVACY IN IOT BASED HEALTHCARE

Dr. A. Sivasangari

ISBN 978-93-86388-62-9

ISBN: 978-93-86388-62-9
First Published: 20th August 2024
DOI: www.doi.org/10.47715/978-93-86388-62-9
Price: 250/-
No. of. Pages: 102

Jupiter Publications Consortium
Chennai, Tamil Nadu, India
E-mail: director@jpc.in.net
Website: www.jpc.in.net

Name of the Monograph:
Security and Privacy in IoT based Healthcare

Authors:
Dr. A. Sivasangari

ISBN: 978-93-86388-62-9
Volume: I
Edition: First

Published by:
Jupiter Publications Consortium
director@jpc.in.net | www.jpc.in.net

Printed by:
Magestic Technology Solutions (P) Ltd, Chennai, India.
info@magesticts.com
www.magesticts.com

Jupiter Publications Consortium
Address: 22/102, Second Street, Venkatesa nagar,
Virugambakkam, Chennai, Tamil Nadu, India.
Website: www.jpc.in.net

ABOUT THE AUTHOR

Dr. Sivasangari A. earned her B.E. from Kalasalingam College of Engineering in 2003, followed by an M.E. from the Government College of Engineering in 2007, and completed her Ph.D. at Sathyabama Institute of Science and Technology in 2017, specializing in Wireless Body Sensor Networks. Presently, she serves as a Professor in the Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology, where she plays a pivotal role in both academic and research initiatives. Her scholarly interests are wide-ranging, encompassing the Internet of Things (IoT), Big Data Analytics and Security, as well as Web Development. Dr. Sivasangari is the principal investigator on a project funded by the Department of Science and Technology (DST) and also serves as a co-investigator on additional projects supported by DST and the All India Council for Technical Education (AICTE).

Beyond her research, she has mentored student startup projects under the DST Technology Business Incubator (TBI), offering invaluable guidance to emerging entrepreneurs. With her extensive expertise and unwavering commitment to her field, Dr. Sivasangari has established herself as a distinguished figure in academia, continually advancing the frontiers of technological research and innovation.

PREFACE

The rapid evolution of the Internet of Things (IoT) has revolutionized healthcare, enabling a new era of personalized and efficient medical services. Among the many advancements, Wireless Body Area Networks (WBAN) stand out as a critical component, providing continuous monitoring and real-time data exchange that can significantly enhance patient care. However, the integration of IoT in healthcare also introduces complex security and privacy challenges, which must be meticulously addressed to protect sensitive medical information and ensure the safety of patients.

This monograph, Security and Privacy in IoT-Based Healthcare, delves into the multifaceted aspects of securing WBANs and IoT systems in medical contexts. The work is structured to guide the reader through the foundational concepts and applications of WBAN, progressing into an in-depth analysis of the various security mechanisms that have been developed to safeguard these systems.

Chapter 1 provides a comprehensive introduction to the subject, beginning with an overview of biosensors and the diverse applications of WBANs, both medical and non-medical. It further explores the critical issue of security, detailing the different levels and facets of protection necessary to counter the myriad threats faced by these systems. The chapter concludes by outlining the motivation and objectives that drive this research, setting the stage for the subsequent chapters.

In Chapter 2, a thorough literature survey is presented, examining existing security schemes, including biometrics, cryptography, and fine-grained access control mechanisms. This chapter serves as a foundation for understanding the current state of the art and the gaps that this research aims to address.

PREFACE

Chapters 3 and 4 introduce two novel security algorithms developed as part of this research: the ECG Hummingbird Algorithm and the Modified Feather Lightweight Block (MFLB) Cipher. These chapters provide detailed insights into the design goals, key generation processes, encryption and decryption techniques, and the experimental results that demonstrate the efficacy of these algorithms. The ECG Hummingbird Algorithm, in particular, is designed for secure data transmission in WBANs, while the MFLB Cipher offers a robust lightweight solution for resource-constrained IoT devices.

This monograph is intended for researchers, practitioners, and students who are interested in the intersection of IoT, healthcare, and cybersecurity. It aims to contribute to the ongoing discourse on securing healthcare systems in an increasingly connected world, offering both theoretical and practical insights that can be applied to current and future technologies.

I extend my gratitude to all those who have supported this research, particularly my colleagues and mentors, whose guidance has been invaluable. I also hope that this work inspires further research and innovation in securing IoT-based healthcare systems, ensuring that technological advancements continue to serve humanity without compromising privacy and security.

Dr. Sivasangari
August 2024

ABSTRACT

The integration of the Internet of Things (IoT) into healthcare has led to significant advancements in patient monitoring and care through Wireless Body Area Networks (WBANs). However, these innovations also present substantial challenges in ensuring the security and privacy of sensitive medical data. This research explores the various security threats and vulnerabilities associated with WBANs and IoT-based healthcare systems, proposing novel solutions to enhance data protection. The study introduces the ECG Hummingbird Algorithm, designed for secure data transmission in WBANs, and the Modified Feather Lightweight Block (MFLB) Cipher, which offers a lightweight encryption solution suitable for resource-constrained IoT devices. Experimental results demonstrate the effectiveness of these algorithms in mitigating security risks while maintaining system efficiency. This work contributes to the growing field of cybersecurity in healthcare, offering practical approaches to safeguarding patient information in an increasingly interconnected world.

Keywords: Internet of Things, IoT, healthcare, Wireless Body Area Networks, WBAN, security, privacy, ECG Hummingbird Algorithm, Modified Feather Lightweight Block Cipher, encryption, data protection.

Contents

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In the late 90's, several professional groups strove to build Wireless Personal Area Networks (WPAN) at Massachusetts Institute of Technology (Sana Ullah et al 2010). Several information devices were linked to the human body and electric field sensing was employed to find out the status of the human body. However, the technique is expensive and consumes more power. Besides, the communication system does not satisfy the requirements of the healthcare system such as flexibility, mobility and privacy. The Wireless Body Area Networks (WBAN) with smaller energy consumption, which in turn improves the lifetime of the network, overcomes these pitfalls. In 2006, a Wireless Next Generation (WNG) was formed to examine the future directions of research. An interest group for WBAN (IG-WBAN) was found. The committee members of IEEE 802 WG15 agreed on IG-WBAN as Study Group WBAN (SG-WBAN). In 2008, SG-WBAN was approved as Task Group (TG6) under 802.15. The openings were closed for WBAN application in 2008 by TG6 and all the submitted applications were accumulated into a single document. In 2010, the communication standard of WBAN was presented by IEEE 802.15.6 and approved in 2012. Owing to the advancement of wireless technology, WBAN gains the spotlight of research.

The revolution of inexpensive and the energy efficient sensors paved the way for the success of WBAN. WBAN is a special type of network that comprises wireless smart sensors, which are implantable or wearable by humans (Ming Li et al 2010). Human health monitoring has been significantly flourished, owing to the current developments in sensor technology and wireless communication. The wireless technology is a boon, such that the sensors sense the health data of the patient remotely. The modern lifestyles of humans have increased the threat of fatal diseases such as diabetes, cardiac disease, and high blood pressure. Hence, the patients have to be cautious to cope up with the associated risks. This makes monitoring of health condition of patients continuously, irrespective of location and time.

Though WBAN relies on sensors, it is different from Wireless Sensor Network (WSN) in terms of deployment, data transfer rate, and mobility. IEEE 802.15 defines WBAN as a communication standard optimized for low power devices and the wearable sensors placed either of or inside a human body to serve a variety of applications including medical, consumer electronics or personal entertainment and other. WBAN is a boon to the society as it provides a remarkable solution to the remote healthcare system. WBAN is an inexpensive mean to improve the quality of life. The wireless physiological sensors are used for measuring the medical information of the patient which is transmitted through a wireless medium to the remote users. It is important to protect the data from attackers. Hence, the sensors are employed for tracking the health status of the patient.

The integrity and confidentiality of medical data must be protected from hackers. Unauthorized access of health data leads wrong diagnosis and treatment. The personal server can be a personal computer or a smartphone. The personal server forwards the medical data to the medical server through the Internet. At the other end, the medical server has the health data and several authorized physicians for treating the patients.

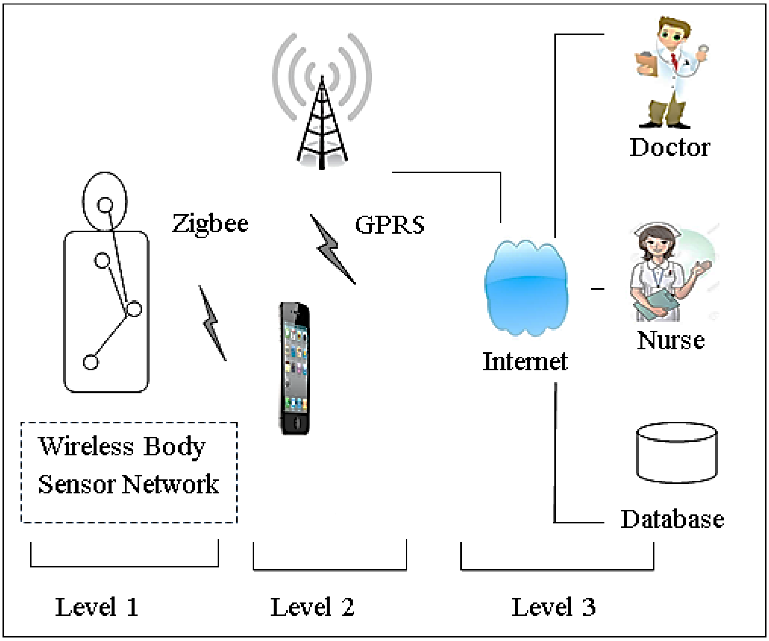

Figure 1.1 Three Level architecture of WBAN

The medical server has to enforce strict access control policy. The intended physician alone can gain access to the health information of the patient.

The death rate of humankind is escalating every year, owing to several life-threatening diseases. The death rate can be minimized when these diseases are figured out at an early stage. Early detection of diseases is not possible in all cases. However, continuous tracking of a person's health data can be the solution to the aforementioned issue. The most feasible solution to continuous tracking problem is WBAN, which employs wearable or implantable sensors for monitoring the health parameters of a human. WBAN is one of the best remedial solutions and enhances the quality of human life. Thus, it is an inexpensive mean to improve the quality of life. WBAN is accepted as the best solution for remote healthcare monitoring applications. WBAN is a boon to the society, which can save several lives. This type of network allows the physician to provide proper treatment to the patient, irrespective of the time and location of the patient.

The health data of the patients are stored in a medical database, enable maintenance of historical health records. This medical database serves as the primary component through which disease diagnosis is made possible (Chen et al 2011). Hence, the data in the medical database must be protected by all means, as it is the underlying foundation for further process. The physician would end up in the wrong diagnosis or prescription if the provided medical data is incorrect or altered in between. Mostly, the health data of the patients are preferred to be stored in a distributive manner, in order to escape from the effects of single point of failure. Therefore, enforcement of security mechanism the entire system is a essential requirement. Data tamper is a very serious issue in WBAN, as the health data reflects on the treatment and diagnosis of the patient. Data tamper may lead to the wrong diagnosis, which is a serious threat. Therefore, an effective security mechanism is needed for WBAN. The data that is to be transmitted must be in an unintelligible format, which can be achieved by encryption.

The most important difference between WBAN and WSN are coverage and the data rate. The wireless communication range of WBAN lies from one to two meters and the data rate is restricted below 1 Mbps. The nodes in WBAN are associated with the human body. They can be up to 20, but the number of nodes in WSN can exceed the value of 1000. Nodes in WSN are scattered over a large area, but the nodes in WBAN are placed on the human body as described by Agrawal et al (2004) and Anastasi et al (2009). In WBAN, the keys are derived from physiological signals of the human body. The generated key values can exhibit randomness properties of key generation.

The nodes in WBAN are severely constrained with respect to communication ability, memory and computational overhead. Recharging or replacement of batteries is not possible due to the implantable nature of the nodes. The routing attacks are not concentrated in WBAN due to its communication range. WBAN deals with the health records of patients, which are private and confidential, and so, a strict security mechanism must be enforced in the WBAN application. On the contrary, the security of other wireless networks depends on the nature of the application. WBAN nodes track the physiological signals of the patient at regular time intervals, whereas WSN follows the strategy of event-based tracking. The data transmission in WBAN must be as fast as possible to ensure freshness in medical data. The faster transmission could be achieved at the cost of more energy consumption.

1.2 BIOSENSORS AND APPLICATIONS OF WBAN

Biosensors are the vital elements of WBAN. They play the intermediary role between the human and the network. The main task of biosensors is to gather the necessary health parameters from the patient, which enables the physician to diagnose the disease at the right time. Biosensors are wearable and implantable into the human body. WBAN improves medical services and thereby the quality of human life. Some of the commercial biosensors available in the market are presented below.

The accelerometer is responsible for tracking the position of a human. Some of the common positions of human are walk, run, sit, stand and body at rest. This type of sensor is highly useful in the healthcare and amusement based applications. Gyroscopes are meant for determining direction and this is achieved by the theory of conservation of angular momentum. Human mobility can be tracked by the combination of accelerometer and a gyroscope. Human respiration is the process of inhalation and exhalation. The responsibility of this type of sensor is to determine the degree of carbon-dioxide exhaled and level of oxygen inhaled in the process of human respiration. ECG is a map that defines the functionality of the human heart. Any cardiac diseases can be diagnosed with the help of ECG (Ali et al 2010). This is achieved by fixing several electrodes over the skin, especially around the chest. As these sensors can present live data to the physician, the abnormalities can easily be managed all at once.

Electroencephalography (EEG) is employed to diagnose brain death, sleep disorders and so on. This is accomplished by ionic current experienced by the neurons of the brain. Electromyography (EMG) is an effective means to diagnose neuromuscular disease. When the muscle cells are triggered electrically or neurologically, the muscle cells produce an electric potential. EMG measures the generated electric potential and can be exploited to diagnose neuromuscular diseases. Nerve and muscle disorders cause reaction in the muscle in abnormal ways. WBAN finds its applicability in both medical and non-medical applications. Some of the medical applications of WBAN are remote health tracking, detection of diseases etc. Non-medical applications include real-time streaming of data, amusement based applications, emotion detection and personal item tracking. The Figure 1.2 shows the applications of WBAN.

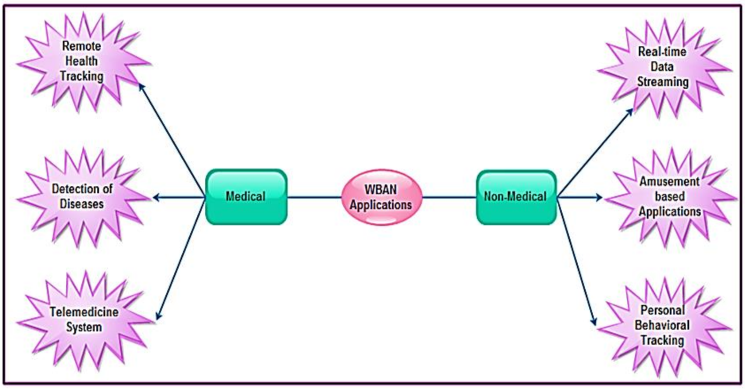

Figure 1.2 Applications of WBAN

1.3 Medical Applications

Remote health monitoring is the most popular application of WBAN. It is meant to track the health condition of the patient continuously. Some of the widely employed health parameters are heart beat rate, body temperature, blood pressure, ECG, EEG and glucose rate (Ali et al 2010). The patients can be monitored at all time irrespective of their present location. This remote monitoring result in timely observation of patients, which in turn saves the life of patients.

achieves fine grained access control and security. Besides, the proposed work consumes lesser encryption time and provides a solution for secure key exchange. The security analysis of the proposed scheme proves its strength and efficiency against other techniques.

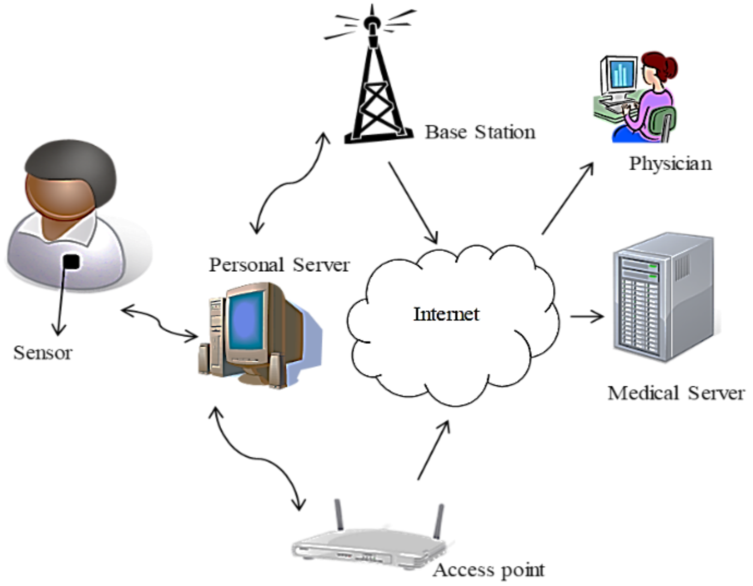

Figure 4.1 Typical Architecture of MFLB Model

WBAN prompts the patients' health information transmitted via an open wireless channel and helps reaching the monitoring station through several intermediary devices. The monitoring station tends to diagnose the disease with respect to the health data being transmitted. Thus, considerable attention must be rendered for the security of the health data.

The motivation and design goals of the proposed MFLB model is discussed in section 4.2. The proposed MFLB model is presented in section 4.3. The performance analysis of the proposed MFLB model is explained in section 4.4. Finally, the contribution of the proposed work is explained in section 4.5.

4.2 MOTIVATION AND DESIGN GOALS

On the other hand, the sensors involved in WBAN are energy constrained requiring the introduction of, a lightweight security mechanism for improving the lifetime of the network. Security must be offered to the patients and the physicians via a lightweight security algorithm along with the key management technique. The medical information should be kept confidential to ensure access to the health information for the intended patients and doctors alone. Proper authentication system must be incorporated to prevent unauthorized access to data. The patient's information must be strictly restricted to the authorized users. There is a need to design the security mechanism for access control and data encryption. This chapter provides medical information on the patient encrypted by a lightweight block cipher, which is based on Feistel Cipher structure. The proposed model achieves the key management in WBAN.

The objectives of the proposed MFLB model is:

- To derive the key values from the ECG signal and achieve the secure key management in WBAN.
- To provide the secure data transfer between the sensors to remote users.
- To design a fine grained access control mechanism for providing the authorized access in WBAN.

4.3 MFLB MODEL

The proposed MFLB model considers a heterogeneous wireless body sensor network. The WBAN is composed of several sensor nodes, SH, sink node (mobile phone), BS, Healthcare Service and Alert (HSA) system.

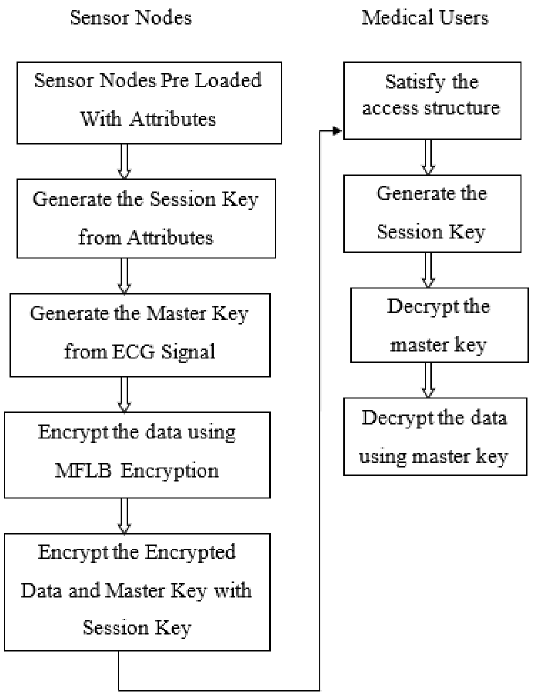
Sensor Nodes
Medical Users
Sensor Nodes Pre Loaded With Attributes
Generate the Session Key from Attributes
Generate the Master Key from ECG Signal
Encrypt the data using MFLB Encryption
Encrypt the Encrypted Data and Master Key with Session Key
Satisfy the access structure
Generate the Session Key
Decrypt the master key
Decrypt the data using master key

Figure 4.2 Proposed MFLB Model

The SH is responsible for collecting the data sensed by the sensors implanted in the patient's body. It transmits the collected data to the sink, which forwards the data to the HSA via the BS. In case, a patient needs immediate attention, the doctors owing necessary authorization can access the information from HSA. The MFLB model is depicted in Figure 4.2.

The main goal of MFLB model is to transfer the medical information with security and privacy. The attackers could be either external attackers or network users who are not authorized to access the medical data. The hackers eavesdrop all the traffic information in WBAN. The sensor nodes are preloaded with a set of attributes, which are patient ID, type of data and type of users. Each user is assigned an access structure and corresponding secret key SK. Medical information is encrypted by using key values generated from the ECG signal. The session key is derived by applying hash value for the attributes, which are preloaded in sensor nodes. The SH collects the encrypted information from all sensor nodes and sends it to the remote server. The medical users who satisfy the access policy are allowed to access to the patient information. The user derives the session key from their attributes and decrypts the master key, which is used for deriving the medical information.

The security architecture comprises encryption and decryption modules and a key exchange module. In the encryption module, the health information obtained from the sensor nodes are encrypted before transmitting the information over the wireless medium. Encryption is done by using 128-bit keys generated by exploiting the ECG signals. The key generation module provides a secure key exchange for ensuring authentication and is achieved by a trusted third party who is responsible for health care information monitoring and key distribution. In the decryption module, the authorized person is prompted to decrypt the encrypted health information by using the 128-bit key.

MFLB model is employed for encrypting medical data. It is based on the Feistel structure. The proposed scheme performs encryption by two steps, namely, key generation and encryption .These steps are explained in the following sections.

4.3.1 Key Generation

Symmetric cryptographic algorithms generate keys by using standard key generating functions. In this work, biometric features are used for key generation, to ensure the generated cryptographic keys are unique. The ECG signal is utilized as a biometric feature for ensuring WBAN communication. Hence, ECG signal IPI is used as a biometric feature. The inter-pulsed interval is the time interval between the successive RR of the ECG signal.

For instance, Entity Identifier (EI) is used as a method to secure wireless communications instead of maintaining a dependence on cryptographic keys. IPIs of heartbeats are measured as a biometric trait when generating an entity identifier. In general, the master node in a WBAN sends a synchronization signal to ask for the network-wide EI generation. Once other nodes receive this synchronization request, they begin to record at least one cardiovascular signal. Thus, each node calculates a series of IPIs, and distinctive keys can be generated via concatenation in each block of EIs.

ECG signal processing can be divided into two stages such as pre-processing and feature extraction. The pre-processing stage removes noise from the ECG signal and extracts peak values from the ECG signal. The IPI values can be extracted from the signal. Uniform quantization is performed in the ECG signal. The steps involved in the key generation are as follows. The ECG signal of a specific node is measured and sampled at a frequency of 1000 Hz. The maximum amplitude of the signal is estimated. The difference between the R peaks is estimated, and is called as IPI. The IPI is converted into a binary string to form a 128-bit key. Thus, the 128 bit is generated by exploiting the IPI of an ECG signal and the generated key is very secure, as it depends on the ECG that cannot be predicted.

4.3.2 Encryption and Decryption

The medical information to be transmitted over the BSN should be encrypted for secure transmission of data. In this work, a lightweight block cipher based on Feistel structure is employed for encryption. The use of Feistel structure provides the advantage of using the same algorithm for both encryption and decryption process. The proposed scheme encrypts a 64-bit block of data by using a 128-bit key. The algorithm employed for encrypting the plain text is presented below.

```
Algorithm
Step 1: Divide 64 bit $\mathbf{M_i}$ into 32 bit $\mathbf{M_L}$ and $\mathbf{M_R}$;
Step 2: Pass $\mathbf{M_i}(\mathbf{M_L} \,||\mathbf{M_R})$ in the first round;
Step 3: Increment $\mathbf{i}$ for every round;
Step 4: Concatenate $\mathbf{M_L}$and $\mathbf{M_R}$to obtain $\mathbf{Ci}$;
// Round function
Step 1: Input: 32 bit $\mathbf{M_i}$ and Output: 32 bit $\mathbf{Y_i}$
Step 2: Perform XOR operation between $\mathbf{M_i}$ and $\mathbf{K_i}$;
Step 3: Obtain two 16 bit outputs $\mathbf{X_i}$ and $\mathbf{Y_i}$;
Step 4: Produce 32 bit output $\mathbf{Y}$ by weight functions $W_1$and $W_2$;
Step 5: Employ double swap function to generate 128-bit key;

// Weight function $W_1$
Step 1: Divide 16 bits into four blocks;
Step 2: Apply S-box to produce S1;
Step 3: Perform circular shift operation to produce S2;
Step 4: Perform XOR between S1 and S2 to generate $Y_1$;
// Weight function $W_2$
Step 1: Divide 16 bits into four blocks;
Step 2: Apply S-box to produce S3;
Step 3: Perform circular shift operation to produce S4;
Step 4: Perform XOR between S3 and S4 to generate $Y_5$;
Step 5: Generate F by $\mathbf{Y_1}||\mathbf{Y_5}$;
Step 6: End;
```

The 64-bit plain text $\boldsymbol{M_i}$is divided into two blocks of 32 bits each, which are $\mathbf{M_L}$ and $\mathbf{M_R}$and this produces a 64 bit cipher text. The encryption process uses a 64 round feistel structure. Figure 4.3 shows a typical feistel structure. The input to the first round is the plain text $\mathbf{M_i}(\mathbf{M_L}\ ||\mathbf{M_R})$. The input to the $\mathbf{i+1}$ round is computed as follows.

$$L_{i+1} = R_i \tag{4.1}$$

$$R_{i+1} = L_i \oplus F(k_i, R_i) \tag{4.2}$$

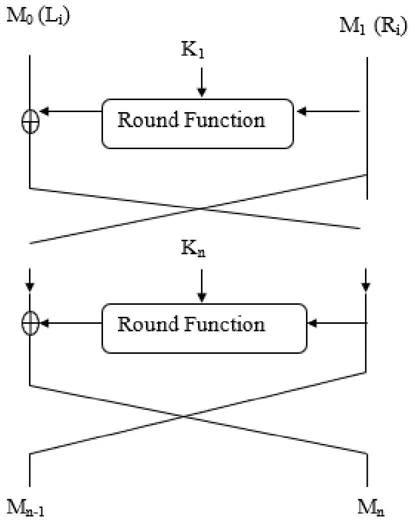

Figure 4.3 Feistel Cipher Structure

The cipher text c_i is obtained by concatenating the two strings obtained in the last round. The process of round is described below.

4.3.2.1 Round function

The round function takes 32-bit input M_i and generates a 32 bit output Y_i. Two weight functions W_1 and W_2 are used in this process. The round function is applied on the 32 bit input M_i . The process is described below. The input M_i has to undergo Ex-OR operation with the random key K_i.This function produces two 16 bit outputs X_i and Y_i. These two outputs are then processed through the weight functions W_1 and W_2 to produce the 32 bit output Y. The process of generating random keys is described below. The process of key scheduling produces the round key Rk from the secret key, k_n where n is 128. It uses a double swap function for generating the 128 bit key. Figure 4.4 illustrates the process of round function generation. The double swap function is described as follows:

$$Y_{128} \leftarrow X_{128} \tag{4.3}$$

$$Y = X[64 - 120]||X[0 - 6]||X[121 - 127]||X[7 - 63] \tag{4.4}$$

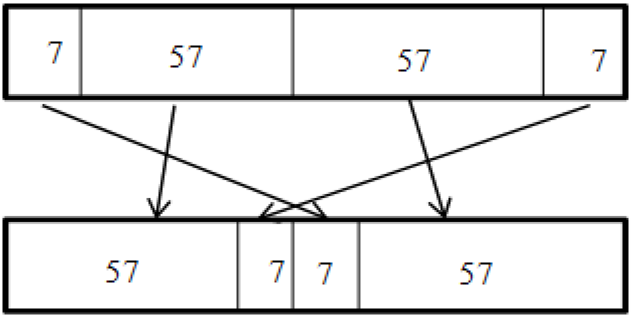

Figure 4.4 Generation of Round Function

The 128 bits are divided into four 32-bit size blocks. Each block contains 32 bits. This 32 bits can be reduced to 8 bits in each block. Finally, all the block values are concatenated to form a round key.

4.3.2.2 Weight function ($\mathbf{W_1}$)

In this W1 function, the 16-bit input is divided into four blocks consisting of 4 bits each while an S-box is applied in parallel, for producing a 16-bit output. The working of the weight function is described below.

Initially, the S-box is applied on X for production of S1. It is followed by the circular shift operation over S_1 and S_2 is performed. Both S_1 and S_2 are applied with the Ex-OR operation and W_1 is generated.

$$S_1 = \{S\ (X_1)||S\ (X_2)||S\ (X_3)||S\ (X_4)\} \qquad (4.5)$$

$$W_1 = S_1 \oplus S_2 \qquad (4.6)$$

4.3.2.3 Weight function ($\mathbf{W_2}$)

In this function, the 16-bit input is divided into four blocks consisting of 4 bits each. An S- box is applied in parallel for producing a 16-bit output. The working of the weight function is described below. Initially, the S-box is applied over Y for producing S_3, and a circular shift is applied on S_3 later for producing S_4.Finally, S_3 is Ex-OR with S_4 to produceY_5.

$$S_4 = \{S\ (Y_1)||S\ (Y_2)||S\ (Y)||S\ (Y_4)\} \qquad (4.7)$$

$$W_2 = S_3 \oplus S_4 \qquad (4.8)$$

Finally, the output of the round function F is given by $F = Y_1||Y_5$.

Table 4.1 S-Box

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

The decryption is the same as that of the encryption process, except the order of round keys. Round keys are employed in the reverse order as given by eq. 4.8.

$$L_i = R_{i+1} \oplus F(k_i, L_{i+1}), \qquad R_i = L_{i+1} \tag{4.9}$$

4.4 ATTRIBUTE BASED KEY EXCHANGE (ABKE)

By means of key exchange protocols the two users can communicate over a network, by generating a shared secret key. These protocols are necessary for prompting the users to utilize the shared key cryptography for protecting the data being transmitted over an insecure network. Thus, key exchange mechanism plays a vital role in providing secured communication. When the attributes satisfies the access structure A, the session key S_K is generated.

4.4.1 Access Structure

Let S be the access structure in the form of tree. The interior nodes of S indicate a threshold gate and the leaf node represents the attributes. The number of children of node i is represented as n_i and its threshold level is represented as $\tau_i(0<=\tau_i<=n_i)$. When the threshold gate is AND, $\tau_i = n_i$ or when it is OR gate, the output is $\tau_i = 1$. The parent of the node i is represented as paren(i), while the attribute is represented as att(i).

4.4.2 Satisfying an Access Structure

Let α be the root of the access structure S. The sub-tree of the node i is represented as S_i. Let $S_i(\alpha) = 1$, represent the set of attributes, where α satisfy the access structure. The function $S_i(\alpha)$is calculated as follows: if i is the interior node, for every child of i, $S_i(\alpha)$ is calculated. $S_i(\alpha)$ return true, only if τ_i children of i returns true. If i is the leaf node, $S_i(\alpha)$ returns 1, if att(i) $\in$ α.

4.4.3 Communication Structure

Let $c = \{c_1, c_2, \dots c_m\}$ be the set of m users. Each user is presumed to have a set of attributes. Access structure is provided to users. When a user needs to establish a session key, the attribute set S_i is checked against the access structure A. If S_i satisfies $A((S_i) \in A)$ then the protocol is executed. Thus, the user whose attribute set satisfies the access structure computes the session key. The session key is calculated by applying the hash value for the string of attributes.

4.5 EXPERIMENTAL RESULTS

The performance of the proposed MFLB model is measured and analyzed in terms of encryption time. Encryption time is defined as the time taken by the algorithm to encrypt a particular data length. The encryption time for the proposed MFLB is compared with the AES algorithm and the results are shown in Figure 4.5.

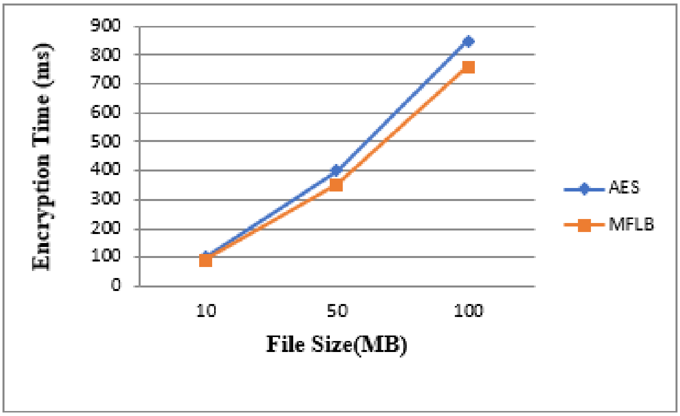

Figure 4.5 Encryption Time of Proposed MFLB Model and AES Algorithm

The results indicate the encryption time of proposed MFLB decreases with the different file size, which when compared to the AES. The encryption time of proposed MFLB algorithm achieves 12% faster than the existing AES algorithm. Therefore, for an application, which involves frequent key exchange, the use of proposed MFLB would be a preferable choice.

Chapter 4 strives to provide a lightweight security mechanism for the WBAN, because of its energy restrictions. Security is the most important need to be satisfied in the WBAN, as data tamper or deletion may reflect in the invaluable lives of humans. In order to escape from such security attacks, an effective security mechanism is the need of the hour. Though several security algorithms exist, they are not applicable to WBAN. This is because of the severe energy restriction in WBAN.

The full-fledged security mechanism consumes more energy, which drains the battery of the sensors, all at once. Thus, a lightweight security mechanism is needed for WBAN. The current chapter provides a lightweight security mechanism with its underlying roots on Feistel structure. The security mechanism of this work consists of two stages. They are key generation and encryption. The key generation relies on the ECG signal, which is time variant and thus cannot be predicted. The encryption is done by using the 32-bit key. The present work consumes lesser period of time for a successful key generation, encryption, and decryption.

4.6 SUMMARY

The current chapter proposed a modified feather lightweight block cipher model, which is based on feistel cipher structure for encryption of medical information. It is designed to provide the secure data transfer between sensor nodes to remote users. The ECG signals are exploited for the process of key generation. The fine grained access control mechanism is employed to provide the access for authorized users. The results show that the proposed MFLB provides a higher level of security to the information in WBAN storage and protects the information from eavesdropping attack, tracking attack and matching attack.

BIBLIOGRAPHY

[1]. Agrawal, D., Shrivastava, N., Buragohain, C., & Suri, S. (2004). Medians and beyond: New aggregation techniques for sensor networks. *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, 239-249.

[2]. Ali, A., & Khan, F. A. (2010). An improved EKG-based key agreement scheme for body area networks. *International Conference on Information Security and Assurance*, Springer, 76, 298-308.

[3]. Ali, A., Irum, S., Kausar, F., & Khan, F. A. (2013). A cluster-based key agreement scheme using keyed hashing for body area networks. *Multimedia Tools and Applications*, 66(2), 201-214.

[4]. Prusty, A. R. (2012). The network and security analysis for wireless sensor network: A survey. *International Journal of Computer Science and Information Technologies*, 3(3), 4028-4037.

[5]. Amin, N., Asad, M. N., & Chaudhry, S. A. (2012). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. *IEEE*

International Conference on Networking, Sensing and Control, 118-121.

[6]. Anastasi, G., Conti, M., Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3), 537-568.

[7]. Bao, S. D., Zhang, Y. T., & Shen, L. F. (2005). Physiological signal-based entity authentication for body area sensor networks and mobile healthcare systems. *Proceedings of the IEEE EMBS 27th Annual International Conference Engineering in Medicine and Biology*, 2455-2458.

[8]. Barni, M., Failla, P., Lazzeretti, R., Sadeghi, A. R., & Schneider, T. (2011). Privacy-preserving ECG classification with branching programs and neural networks. *IEEE Transactions on Information Forensics and Security*, 6(2), 452-468.

[9]. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *Proceedings of the IEEE Symposium on Security and Privacy*.

[10]. Biel, L., Pettersson, O., Philipson, L., & Wide, P. (2001). ECG analysis: A new approach in human identification. *IEEE Transactions on*

Instrumentation and Measurement, 50(3), 808-812.

[11]. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. *Mobile Networks and Applications*, 16(2), 171-193.

[12]. Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2008). Body sensor network security: An identity-based cryptography approach. *Proceedings of the ACM Conference on Wireless Network Security*, 148-153.

[13]. Fang, C., Zhang, Y., & Bae, T.-W. (2012). VLSI friendly ECG QRS complex detector for body sensor networks. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2(1), 52-59.

[14]. He, D., Chen, C., Chan, S., Bu, J., & Zhang, P. (2013). Secure and lightweight network admission and transmission protocol for body sensor networks. *IEEE Journal of Biomedical and Health Informatics*, 17(3), 664-674.

[15]. He, D., & Chan, S. (2014). A novel and lightweight system to secure wireless medical sensor networks. *IEEE Journal of Biomedical and Health Informatics*, 18(1), 316-326.

[16]. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., ... & Chee, S. (2006). HIGHT: A new block cipher suitable for low-resource devices. *Cryptographic Hardware and Embedded Systems - CHES 2006*, 8th International Workshop, 4249, 46-59.

[17]. Ethala, S., Renganathan, N. G., & Saravanan, M. S. (2013). Secret handshake issue and validate authority-based authentication system for wireless sensor network. *Journal of Computer Science*, 9(9), 1174-1180.

[18]. Banaee, H., Ahmed, M. U., & Loutfi, A. (2013). Data mining for wearable sensors in health monitoring systems. *Sensors*, 13(2), 17472-17500.

[19]. Heinzelman, W. R., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4), 660-670.

[20]. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., ... & Chee, S. (2006). HIGHT: A new block cipher suitable for low-resource devices. *Proceedings of CHES 2006*, Springer, 4249, 46-59.

[21]. Hu, J., & Bao, S. (2010). An approach to QRS complex detection based on multi-scale mathematical morphology. *Proceedings of the 3rd IEEE International Conference on Biomedical Engineering*, 725-729.

[22]. Kanjee, M. R., Divi, K., & Liu, H. (2010). A two-tiered authentication and encryption scheme in secure healthcare sensor networks. *International Conference on Information Assurance and Security*, 271-276.

[23]. Kaur, S., Farooq, O., Singhal, R., & Ahuja, B. S. (2010). Digital watermarking of ECG data for secure wireless communication. *Proceedings of the International Conference on Telecommunication and Computing Recent Trends in Information*, 140-144.

[24]. Lee, P., & Lee, D. H.-J. (2010). Secure health monitoring using medical wireless sensor networks. *Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management*, 491-494.

[25]. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and

hierarchical inner product encryption. *Advances in Cryptology*, 6110, 62-91.

[26]. Liu, J., & Kwak, K. S. (2010). Hybrid security mechanisms for wireless body area networks. *Proceedings of the 2nd International Conference on Ubiquitous and Future Networks*, IEEE Xplore Press, 98-103.

[27]. Klemm, M., Istvan, G., & Peterson, G. (2005). Novel small-size directional antenna for UWB WBAN. *IEEE Transactions on Antennas and Propagation*, 53(12), 3884-3896.

[28]. Malasri, K., & Wang, L. (2007). Design and implementation of a secure wireless mote-based medical sensor network. *Sensors*, 9(8), 6273-6297.

[29]. Mana, M., Feham, M., & Bensaber, B. A. (2011). Trust key management scheme for wireless body area networks. *International Journal of Network Security*, 12(2), 75-83.

[30]. Upmanyu, M., Namboodiri, A. M., Srinathan, K., & Jawahar, C. V. (2010). Blind authentication: A secure crypto-biometric verification protocol. *IEEE Transactions on Information Forensics and Security*, 5(2), 255-268.