International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Security and Privacy Protection of Medical Sensor Data of Patient using IOT

Priya J[1], MeeraDevi A.K.[2], Dr.Monica R Mundada[3]

[1] PG Student, Dept. of Computer Science and Engineering, RIT, Bengaluru, India
[2] Assistant Professor, Dept. of Computer Science and Engineering, RIT, Bengaluru, India
[3]Associate Professor, Dept. of Computer Science and Engineering, RIT, Bengaluru, India

---

Abstract - *Nowadays, the elderly populations is growing at a faster rate and are suffering from one disease or the other. With the help of technology and medical sensors, healthcare systems are being developed in order to constantly monitor the patient's physiological parameters such as ECG, temperature etc. These parameters are then stored in the medical data (patient information, patient medical history, test results etc). Such information can be recorded on a paper, digital file, database etc. and is collected by hospitals, clinics etc. and can be also used for research purposes. Information that is contained in the medical data relates to an individual private life especially the health data. Such data is sensitive in nature. When such sensitive medical data of a patient is sent over a wireless network, they are prone to attacks such as eavesdropping, alteration etc. Therefore security and privacy of the patient data are one of the major concern in the wireless medical sensor network. In this paper, a patient monitoring system is proposed, where a patient data is taken continuously with the help of the medical sensors (heartbeat sensors). Each of the patient data from the sensors obtained is in the encrypted form and stored in the different files. The physician can request for the key for accessing the patient data. Hence, only authorized users can view or obtain the data. Also, a graph is obtained showing the performance analysis of the two algorithms RSA and Pailier with respect to the time complexity.*

Key Words: Medical Data, Security, Privacy, Patient Monitoring System, Eavesdropping, RSA, Pailier.

1. INTRODUCTION

Wireless sensors networks, Information Technology along with Artificial Intelligence have helped us to overcome the challenges that we face every day by forming a new interdisciplinary branch in the field of biomedical engineering. The continuous increase of the elderly population is one of the major challenges that are now faced by most of the developing and developed countries According to the Population Reference Bureau[1] survey,
it is seen that in the next 20 years, 65 and above aged people population in most of the developed countries will be nearly 20% of the total population. Therefore, delivering a good quality health care to the patients along with low-cost healthcare facilities and overcoming the shortages of the nurse staff problem is one of the primary issues.

The integration of the sensing devices and the consumer electronics technology which is a useful application will help in monitoring the patient's health constantly in the healthcare area. In-home, the pervasive networks help the caregivers and residents by providing continuous health monitoring, access to the medical data, emergency communication etc. With the help of the continuous health monitoring system, detection of diseases can be found at an earlier stage of the patient. Development of wearable sensor devices is a matter of today's researchers along with making more mature and complex wireless sensors network technologies.

Wireless Sensor Networks consists of sensors (nodes) that are spatially distributed to monitor the physical environment. These sensors have capabilities such as sensing/monitoring the environment, collecting the information, processing it and then sending the processed information to its other sensors present in the network via the wireless network [2].

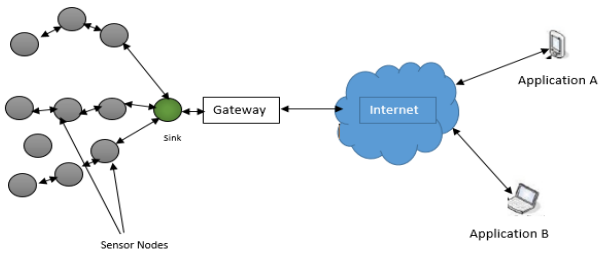

Fig -1: Wireless Sensor Network

Wireless sensor networks used in the medical field are referred to as the "wireless sensor medical networks"(WMSN's).The medical sensor nodes are placed on the body of the patient to monitor the physiological condition of the patient. Vital body parameters such as body temperature, heartbeat, paralysis etc. can be measured using the medical sensors and these parameters or information are then sent to the remote locations without any human intervention. Doctors present in the remote location can assess the patient's health condition from the data obtained from these medical sensors. These

wireless medical sensors may be portable wearable or integrated on the wireless motes [3].

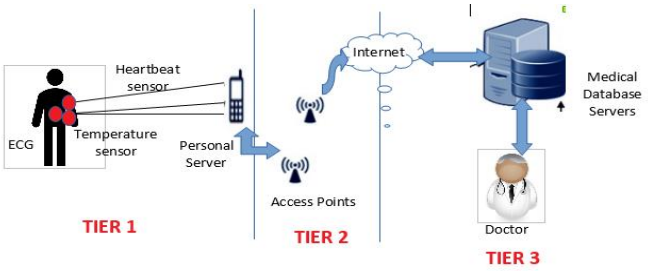

Fig -2: Wireless Sensor Medical Network

1.1 Challenges

Some of the challenges associated with the Health Care applications using the wireless sensor networks are:

- Low Power
- Limited Computation
- Material Constraints
- Robustness
- Security

Some of the threats that are harmful to the wireless medical sensors networks are:

a. Modification of data – Here the attacker can change or remove part of the information that is obtained. The altered data is then sent back to the receiver. Modifying the health data may lead to serious problems.

b. Data Breach – Data breach is a threat to the patient's data privacy where an unauthorized user gets access to the data.

c. Eavesdropping – Here the attacker uses powerful receiver antenna's and obtains the sensitive information from the channel and can misuse it. Also, a threat to the data privacy.

d. Replaying – After the eavesdropping, the information that is obtained is sent back to the sender stating for a different purpose by the attacker [4].

1.2 Health Care Applications

a. eWatch: e Watch is a form of wrist watch which contains built-in capabilities such as sensing, sending notifications, performing computations on the data etc. It can sense notion of the person, body temperature etc. and send audio or visual notifications. When the person is in a distress situation and does not respond to the query stating whether it is an emergency or not. The eWatch with its built-in network abilities could call for help. The wireless communication is via the Bluetooth and the infrared data port of the devices [5].

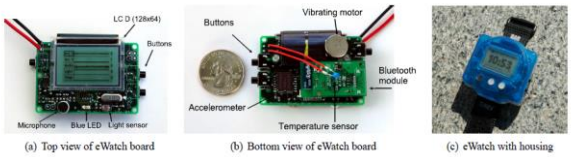

Fig -3: Overview of eWatch

b. IRevive: It is a commercial project that is based on the CodeBlue application. Here, the smartphone is synchronized with the central database server. The smartphone devices capture the body parameters in real-time and stored using a VitalDust Technology.

c. Wearable Sensor Solar Harvesting Device: This device with the help of solar energy establishes a connection from the wireless body area network to the IoT applications. Here the body parameters such as heartbeat, the temperature is measured and send to the server. The results are displayed in the web application present in the mobile device. The energy source is the solar energy obtained with the help of an output based MPPT technique. This technique is used to extract the maximum solar energy from the solar panel. The sensor nodes can be placed anywhere on the body and they operate in a full mode when solar energy is the source of power [6].

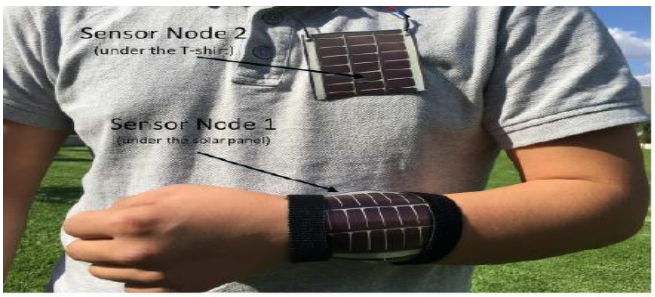

Fig -4: Wireless Sensor Solar Device

2. PROPOSED SYSTEM

The proposed System is as follows:

1. The heartbeat parameter of four patients is taken with the help of the heartbeat sensors. The sensors are connected to the Raspberry Pi and send to the server via WiFi or LAN connection.
2. The patient data obtained from the sensors is encrypted using the RSA algorithm and then send to the server. Here each patient data is sent to the single file.
3. The Admin needs to provide the username and password for access. Here the admin needs to register the details of the patient, view the

existing patient details and respond to the request of the key by the doctor.

4. The doctor needs to enter his username and password. Here the doctor can view the patient data by providing the patient ID, then requesting the key from the admin to view the data which is in the encrypted form. The doctor needs to enter the IP address of the system and the patient ID for viewing the data. The admin provides the key to the doctor.
5. Also, the two algorithms RSA and Pailier (used in the existing system) is compared in terms of the time complexity.

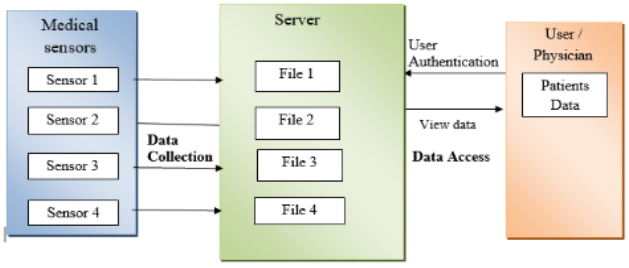

Fig -5: Block Diagram of Proposed System

3. SYSTEM DESIGN

3.1 System Architecture

The above figure represents the architecture of the patient health monitoring system. The components are:

1. Four Heart Beat Sensors.
2. Four files containing different patient data details.
3. Raspberry Pi 3 module
4. Wi-Fi Access Point

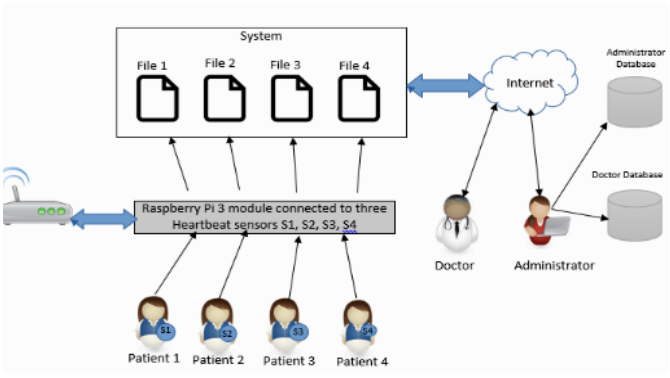

Fig -6: Architecture of the Proposed System

Heartbeat parameter of the patient is obtained from the heartbeat sensor and are sent to the different files via the Internet with the help of the Raspberry Pi 3 module. The administrator maintains the details of the patient and provides the keys for accessing the data. The doctor requests the key from the administrator and can view the original data from the system where it is present.

4. IMPLEMENTATION

4.1 Data Collection

Here four patients heartbeat rate can be checked in parallel. The patients need to place their fingers inside the heartbeat sensor. The patient data contains the following parameters:

1. Patient ID
2. Date and Time
3. Heartbeat value
4. The key

Encryption of the data is done with the help of RSA algorithm used in the Python Language. The RSA algorithm is the most widely used public key cryptography algorithm. It uses the multiplication in the modular arithmetic function to transform the message into the cipher text.

a. RSA Algorithm

The RSA consists of the three following steps:

1. Key Generation:

Step 1: First choose two large prime numbers say 'p' and 'q'.

Step 2: Compute n= p*q and the function:
φ(p -1)*(q – 1)

Step3: Choose an encryption key 'e' at random, the gcd is calculated as follows:
gcd(e, φ(n))=1, such that 1<e< φ(n).

Step 4: Now in order to find the decryption key'd', solve the following equation:
e*d = 1mod (n),where 0<d<n.

Step 5: The public key is: {e, n}, which everyone knows.

Step 6: The decryption key (private key) is: {d, n}, which is usually present with the person who decrypts the message.

2. Encryption of the message is done as follows:

- Let 'm' be the plain text message, where 0<m<n
- The public key is: {e, n}.
- The cipher text 'c' is calculated as follows:
  $c = m^e \bmod n$

3. Decryption of the message is done as follows:

- The input is the cipher text 'c'
- With the help of the decryption key that is : {d, n}
- The original message can be obtained by solving the following equation:

$$m=c^d \bmod n$$

The Security of RSA:

The hacker's ability to factorize the numbers defines the security aspect of the RSA. Depending on the length of the number, it becomes difficult to factorize, therefore better the security of RSA. When using large keys, the only advantage is that there is a computational overhead involved in the encryption or decryption process.

In this system, Result.java file shows the performance analysis based on the time taken by the two cryptosystems RSA and Pailier to process the data.

ii. Pailier Cryptosystem

Pailier Cryptosystem is a type of public key cryptography, where the keys used for encryption and decryption the message is not the same. The major feature of the Pailier cryptosystem is the homomorphic addition of two plain texts.

The Pailier cryptosystem consists of 3 steps:

1. Key Generation

Step 1: Let 'p' and 'q' be the two large prime numbers that are taken at random and independent of each other.

Step 2: Compute gcd= (p, q,(p-1)*(q-1)) =1. This will be achieved only when the two prime numbers of equal length.

Step 3: Then compute n=p*q and the Carmichael's function which is λ = lcm(p-1q-1)

Step 4: Select a generator 'g' where g belong to $Z^*_{n^2}$.

Step 5: Next calculate the modular multiplicative inverse using the following equation:

$$u = (L (g^{\lambda} \bmod n^{2))^{-1}} \bmod n.$$

where L (u) = (u-1)/n

Step 6: Therefore, the encryption key (public key) **is: (n, g)**

Step 7: The decryption key (private key) is: λ (, u)

2. Encryption of the message is done as follows:

Let 'm' be the plain text message that needs to be encrypted where m belongs to Z_n.

Randomly choose r such that r belongs to Z^*_n.
The cipher text is computed as follows: $g^m * r^n \bmod n^2$.

3. Decryption of the message is done as follows:

The cipher text c belongs to $Z^*_{n^2}$.
The original message is computed as follows:

$$m = L(c^{\lambda} \bmod n^2)\ u \bmod n$$

The Security of Pailier Cryptosystem

This cryptosystem does provide semantic security against the chosen plaintext attacks. The challenge to find out the cipher text depends on the ability of the hacker to decide on the composite residuosity. It is seen that the decisional composite residuosity assumption is intractable.

Also due to the homomorphic properties it contains, the cryptosystem is malleable. An encryption algorithm is said to be malleable if there is function that is present that can transform the cipher text to another cipher text and decrypting it can lead to the original message. Though it not a considered as an "advantage" of the Pailier cryptosystem, when this crypto system is used for securing the electronic vote, this property is important.

5. PERFORMANCE ANALYSIS

5.1 Time-Based Performance

System efficiency can be subjected to analysis in terms of the time taken by the RSA and Pailier Algorithm to process the input data (Patient data) from the sensors continuously.

Two graphs are obtained for one patient, one graph specifies the amount of time taken by the RSA algorithm to process the information and the other one by the Pailier Algorithm. Similarly for all the other patient's data is also compared with the two algorithms.

The obtained bar graph is given in Chart 1, where they show RSA algorithm is better than Pailier in the performance. Time taken by RSA algorithm to process the data is less compared to Pailier. RSA is fast and secure than Pailier Algorithm.

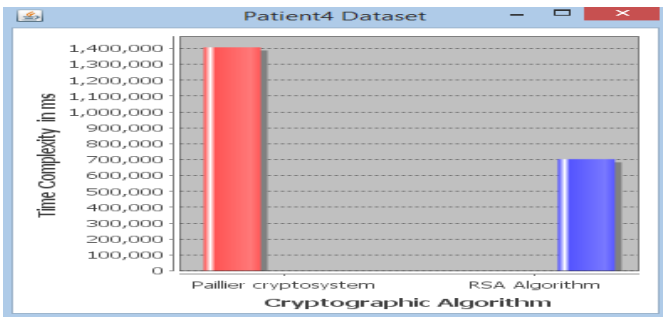

Chart -1: Graph of Pailier v/s RSA Algorithm

Here in the Patient4 data set, the readings from the patient is taken for 1 min. So RSA algorithm has taken 700,000 ms and Pailier has taken 1,400,000 ms to process the data.

6.RESULTS

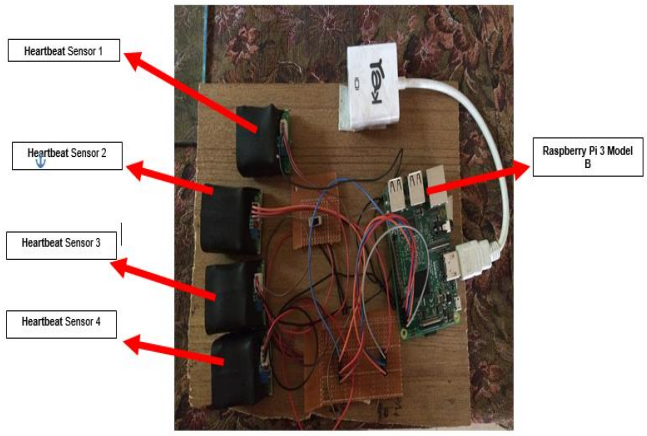

Fig -7: The Basic System Architecture

This hardware arrangement consists of the following components:

1. Four Heartbeat Sensors.
2. Raspberry Pi 3 module
3. Power Supply
4. HDMI cable to connect to the monitor for display of the data readings.

8.1 EXECUTION PROCESS

1. First connect the HDMI cable to the system from the board and then provide power supply from the board with the help of USB cable to the system.

Next open the command prompt and find out the IP address of the machine and then make sure that both the Board and the system are connected to the same network. Next the patients need to place their fingers inside the sensor. Now run the **check.py** file. Here we are checking the Heartbeat for two patients with ID: 100 and 103.

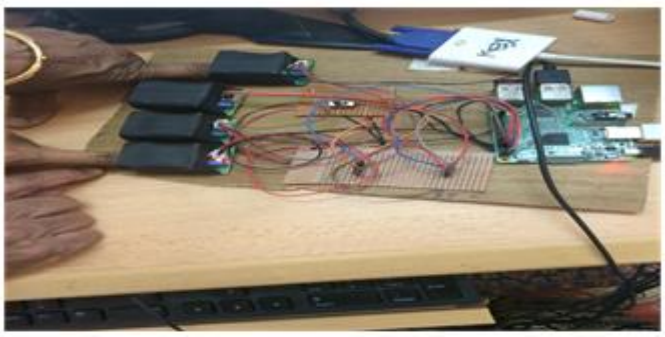

Fig -8: Heartbeat Reading of Patient 100 and 103

2.Open the Eclipse Workspace, and run the file "**Healthcare.java** "as a Java application.

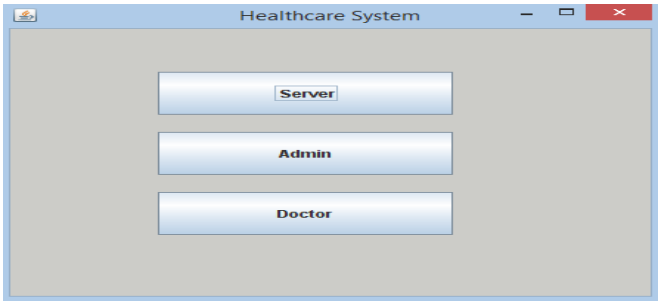

Fig -9: Heathcare. Java application

3. Now click on Server button and we see the 4 different Servers with the data stored in it.

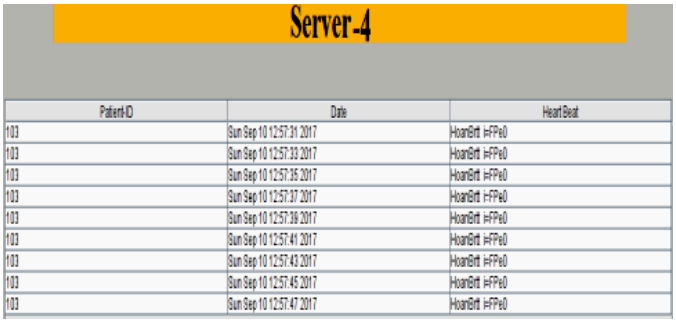

Fig-10: Patient ID -103 data in Server 4

4.The Administrator logins in using the username and password provided and gets directs to the following home page consisting of view patient data, view patients etc.

Fig-11: Administrator Homepage

5.The doctor logins in using the username and password provided and gets directs to the following home page consisting of requesting administrator for key, view server data etc.

Fig-12: Doctor Homepage

6.Now the doctor clicks on "View Server data" and enter the patient ID "103"

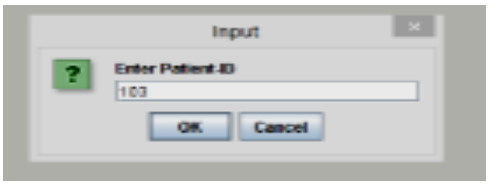

Fig-13: View Server Data Page

7. Here the encrypted data of patient ID 103 is fetched from server 4 and displayed.

Patient-ID	Date	Heart Beat
103	Sun Sep 10 12:57:31 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:33 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:35 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:37 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:39 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:41 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:43 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:45 2017	HoanBrtt i=FPe0
103	Sun Sep 10 12:57:47 2017	HoanBrtt i=FPe0

Fig-14: Patient 4 Encrypted Data

8. In order to view the original data, the doctor requests the private key from administrator by providing patient ID, selecting the priority and the IP address of the Administrator system.

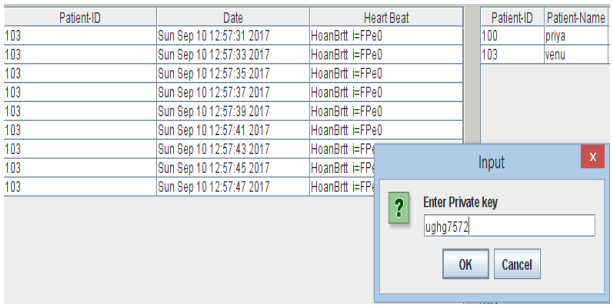

Fig-15: Input –Patient ID by Doctor

9. The Doctor clicks on "View Key", the Patient ID along with their private key is displayed.

Patient-ID	Private Key
100	fghd3281
103	ughg7572

Fig -16: View Key Page :Doctor

10. The Doctor clicks on "View Received Report", enters the patient ID and the private key. Decrypted data of Patient 4 is displayed.

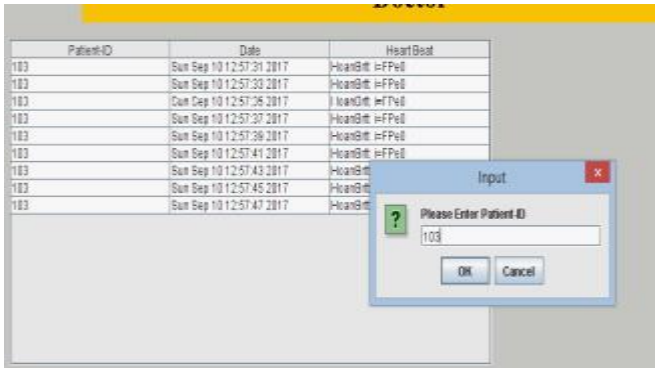

Fig -17: Input – Enter Private Key for Viewing Report

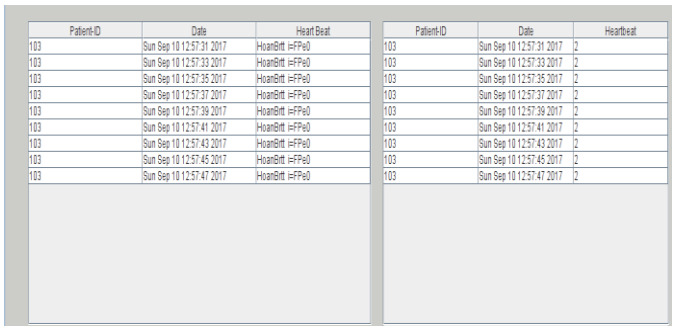

Fig -18: Patient 4 Data Displayed

9. CONCLUSION

In the highly developing era, where directly or indirectly, everything is dependent on computation and information technology, Raspberry Pi proves to be a smart, economic and efficient platform for implementing the health monitoring system. With the use of comfortable wearable sensors in global areas, the proposed healthcare system promises to improve the flexibility and scalability of healthcare applications.

To secure the communication between medical sensors and server, the data (along with the key) is send in the encrypted form using RSA algorithm. The proposed system consists of a new data collection method , where each of the data from the sensors is send to different files, which avoids the risk of keeping a the data in one single file.

For the legitimate user (physician) to access the patient data, an access control method is provided where the physician can see only the encrypted data first. Later on after providing the details of the patient, the private key will be obtained which can be used for decrypting the data. It is seen that the major challenges associated with healthcare application using wireless sensor network comprises of security and privacy issues in the medical sensor data collection, storage and queries and presented a complete solution for privacy preserving medical sensor network.

It can also be concluded that with the evolution of network integration and the management of embedded devices operating multimodal tasks, a more precise and universal healthcare service scheme can be realized.

REFERENCES

1. Kinsella K, Phillips DR,"Global aging: the challenge of success. Population Bulletin Reference", March Edition, 2011.

2. Dargie, W. and Poellabauer C. "Fundamentals of wireless sensor networks: theory and Practice." John Wiley and Sons, 2010, pp.168–183, 191–192.

3. Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem Ziaur Rahman and Kyung Sup Kwak, "A Comprehensive Survey ofWireless Body Area Networks: On PHY, MAC, and Network Layers Solutions", Journal of Medical Systems (Springer), 2010.

4. Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, -"Trust mechanisms in wireless sensor networks: attack analysis and counter measures," Journal of Network and Computer Applications, Elsevier, 2011.

5. U. Maurer, A. Rowe, A. Smailagic, and D. P. Siewiorek, "eWatch: A Wearable Sensor and Notification Platform", in international Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006), Cambridge, MA, USA, 2006.

6. Wang Yun Toh, Yen Kheng Tan, Wee Song Koh-"Autonomous Wearable Sensor Nodes With Flexible Energy Harvesting", 2014, IEEE Sensors Journal, Volume: 14, Issue: 7.