AN AUCTION BASED HEALTH MONITORING SCHEME USING GROUP MANAGEMENT TECHNIQUE IN WSN

Sharmila.G, Suriya priya.T, Saranya V.P

Sharmila.G, E.C.E Dept, Prince Shri Venkateshwara Padmavathy Engg College
Suriya Priya.T,E.C.E Dept, Prince Shri Venkateshwara Padmavathy Engg College
Saranya V.P, Assistant Professor Department of ECE, Prince Shri Venkateshwara Padmavathy Engg college

ABSTRACT

In WMSN the patient's health parameters such as heart rate, blood pressure, temperature are collected by wearable or implantable sensors which is implemented in hospitals, these PHI are stored in the database. The Adversary node can drop the messages by jamming the communication channel and modify the messages. So problem may occur. In order to overcome this problem the RSA algorithm is used. This algorithm helps to avoid the modification of patient's details. Here the public key is the encryption key and it is different from the decryption key which is kept secret and private. Health monitoring via mobile is using the application of mobile computing technologies for amending communication between doctors and patients. The RSA algorithm provides Asymmetric key encryption/decryption technique for more security purpose which has a central server that will able to read patient's incoming data from the sensors and send it to the mobile application and it will also show the other authorized doctors who are specialized to monitor the patient when authorized doctor is in offline.

Keywords:- *Health monitoring, Wireless Sensor Networks (WSN), Security, Privacy Protection, Mobile application.*

1.INTODUCTION

The convergence of Internet of Things (IOT), Wireless Body-Area Networks (WBAN) and cloud computing which has caused e-healthcare to emerge as industrial application that improves the quality of medical care. Further, evolution of e-healthcare into m-healthcare has made to gather information concerning their health status easily at anytime and everywhere. Thereafter, both electronics and mobile combination will provide both security and privacy in medical field. Even though , there is still concerning how to effectively transmit data with low sensor overhead. Due to characteristics of such limited power mobile devices and sensors, between efficiency and privacy or security should be more balanced for commercial purpose of e-/m-healthcare. Therefore, this paper helps to provide more feasible, efficient, secured and private guaranteed with improved version of mobile app which helps even more facility to patients in emergency.

1.1 Private and security

Most current e-/m-healthcare system requires doctors to participate in medical field information using Mobile app. E-/m-Healthcare still faces many challenges including information security and privacy preservation. A healthcare system (HES) framework is designed that collects medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. HES involves the GSRM (Groups of Send-Receive Model) scheme to realize key distribution and secure data transmission, the HEBM (Homomorphic Encryption Based on Matrix) scheme to ensure privacy and system able to analyze the medical data and the results automatically. Even though, it still faces more security problems due to clone node and also in privacy control who can break through due to its homomorphic encryption which is symmetric in nature. In this project, it can be avoided using RSA encryption. Encryption is the standard method for making a communication private. Anyone wanting to send a private message to another user encrypts (enciphers) the message before transmitting it. Only the intended recipient knows how to correctly decrypt (decipher) the message. Those who eavesdrops will not know how to decrypt it. As such, privacy can be ensured in electronic communication using RSA which is asymmetric cryptography.

1.2 Mobile application

In advanced technology integration which improves to small size of physical sensors, microcontroller and processor on a single chip. The wireless networking and micro-fabrication leads to create wireless sensor networks which is used for many applications. For example, healthcare monitoring, traffic monitoring etc. One of the most exciting application domains is health monitoring. The number of sensors such as physiological sensors which monitor vital signs, environmental sensors monitors like temperature, humidity, light and a location sensor can be integrated into a Wearable Wireless Body/Personal Area Network (WWBAN)]. This WWBAN is inexpensive, lightweight, and small size sensors can allow long-term, secured, in the hospital, health can be monitored with instantaneous feedback to the user about the current health status and real-time updates of the user medical records. In existing Accelerometer-based monitoring of physical activity with feedback can improve the process of physical rehabilitation. This has been improved by including automatic search for specialised doctor at the emergency time in the hospital which is the main development of this project. This provide more facility for patient who is in emergency in a secured way.

2. PROPOSED SYSTEM

We propose an advanced and secure system for wireless medical sensor networks. Each patient area network (PAN) consists of some biosensors and a controller. These biosensors collect his/her personal health information(PHI) like body temperature, blood pressure, heart bear rate, blood glucose level etc.. Sensors forward the information to the controller. The security techniques are the Rivest-Shamir-Adleman (RSA) algorithm Proxy Protected Signature Technique During each and every transmission of medical data from sensor to medical server the hash key gets updated.

2.1 BLOCK DIAGRAM

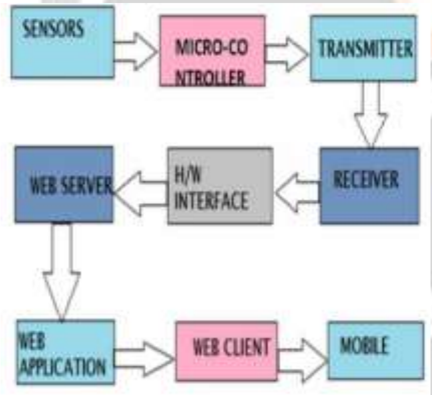

Figure 3: system block diagram.

This figure shows the detailed working of proposed system shows the wearable wireless sensor module (WWSN), in which sensors used to monitor patients health like Heart beat , blood pressure and temperature etc. Then it is connected to a microcontroller where data can be obtained will then be sent by RF transmitter and received by RF receiver connected to the serial port. This data will be transmitted to the smart phone which will have a web application that can be accessed through android like mobile device in order to provide patient’s details to the doctors or the users. If there is a emergency such as increase or decrease in heart beat or temperature then the message will automatically sent to the doctor’s mobile or user via GSM modem which will help the doctor to take the necessary steps. And it also provide more facility such as whether if authorized doctor is not available in emergency time this will show various doctors who are specialized for peculiar treatment which is our proposed in this project. The above figure show the overall structure of the proposed system. The proposed system has been divided in to three main phases of development and implementation. This can be explained in brief.

Patients Monitoring Device

This device is wearable by the patients and the sensors attached to patients body. Figure explains the sample circuit with the Heart beat and temperature sensor connected to device which transfer sensors values to central server through RF module.

Central Server Application

Web application responsible for monitoring and managing the operation of the patient's health. First part of this module will deal with patient's device and get all the reading and store it to database for further utilization. Second part of the module will be a web application which let the doctors view the patient's statistics over the mobile device

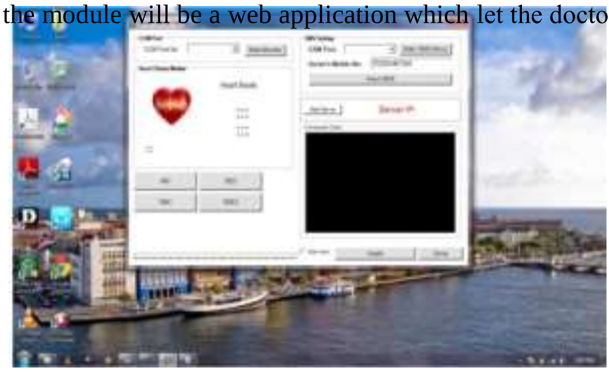

Figure 4: Server Application

Mobile application

Mobile application has been designed for simultaneous monitoring of patients connected to the sensor dev ice and used to alert for doctor in case of emergency .This shows the sample view of the GUI of mobile application which shows how doctor can monitor the patient's state and it also provide privacy features in which if admin doctor who was in online ,then this app will automatically shows other doctors who is specialized .when the patient in the emergency. So this helps to patient even when admin doctor is not available.

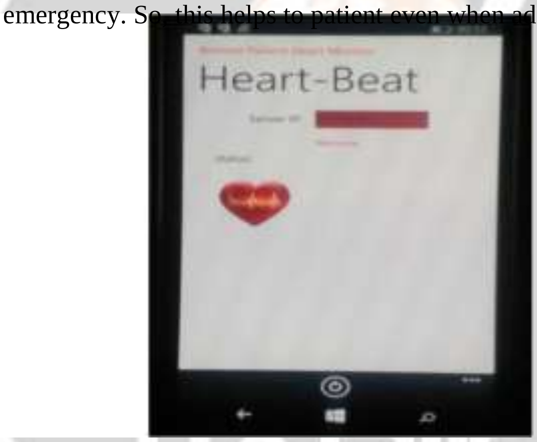

Figure 6: Mobile Application

2.2 FLOW DIAGRAM

This figure explains flow of total implementation process following,

Step 1: Using Wearable Wireless Body Area Network device (WWBSN) which monitors the patient simultaneously and collects the health information like temperature, heartbeat, blood pressure etc from the patient.

Step 2: Then this group of information are collected from the patient.

Step 3: In which, collected data are passed to central node which will distribute it to the destination in a secured way.

Step 4: From wearable device finally collected data sent via Wi-Fi in order to minimize packet delay.

Step 5: Then it is received by the server which is programmed to provide information to authorized doctor and the relative.

Step 6: server will always monitor patient data update, which will help to watch patient simultaneously only using mobile phone by both authorized doctor and relative.

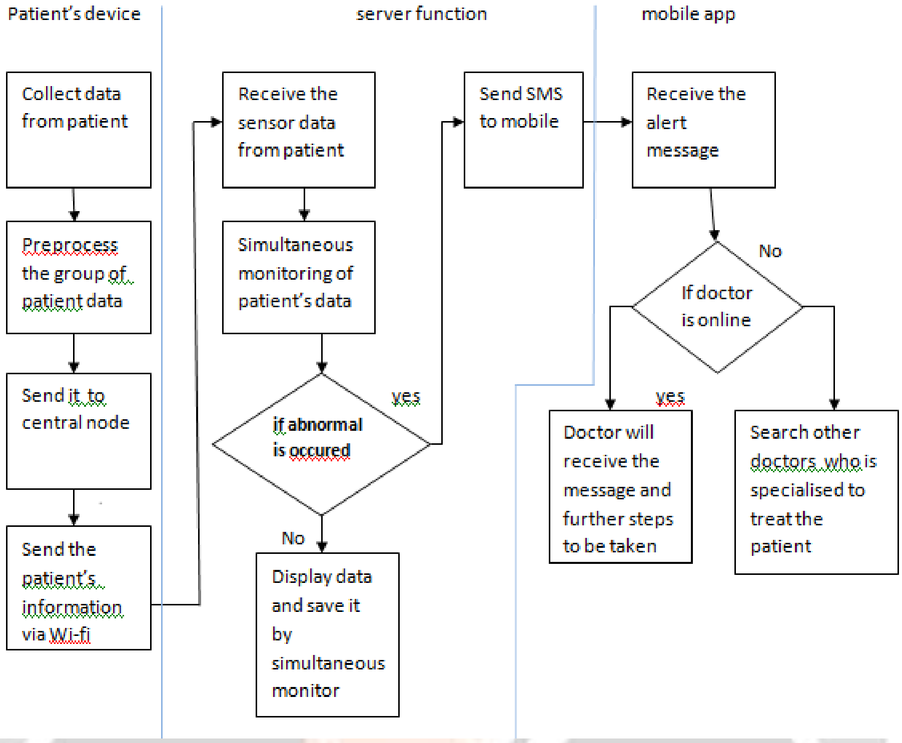
Patient's device
server function
mobile app
Collect data from patient
Preprocess the group of patient data
Send it to central node
Send the patient's information via Wi-fi
Receive the sensor data from patient
Simultaneous monitoring of patient's data
if abnormal is occured
yes
No
Display data and save it by simultaneous monitor
Send SMS to mobile
Receive the alert message
If doctor is online
No
yes
Doctor will receive the message and further steps to be taken
Search other doctors who is specialised to treat the patient

Figure 2.1: Flow diagram of total implementation process

Step 7: If any abnormal condition occur for the patient, it will alert the doctor and the relative. Else, the data will be stored in the server and again continues to monitor the patient.
Step 8: Then message send as SMS if, any abnormal has happened which used to alert the authorized doctor and relative.
Step 9: This mobile app will show whether authorized doctor is in online or not.
Step 10: If not, then it will show some other doctor specialist who are available.

The authorized doctor and user will have the secret code in order to maintain the privacy of the patient data to prevent from eaves dropping and also contain security to avoid clone node (hackers) who will misuse the patient information which can be protected using RSA algorithm.

2.3 RSA ALGORITHM

The Rivest-Shamir-Adleman (RSA) algorithm is one of the secured public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers. Using an encryption key (e,n) the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

Public-Key Cryptosystems

This is procedure to encrypt data the following steps to be done,

1. Deciphering the enciphered form of a message M yields M. That is, D(E(M)) = M
2. E and D are easy to compute.
3. Publicly revealing E does not reveal an easy way to compute D.
4. Deciphering a message M and then enciphering it results in M. That is, E(D(M)) = M

Digital Signatures

This function makes the key to act as signature in which if any editing has made in the secrete key, then it will automatically change their signature . so, it helps us to find whether the secret key been hacked or not. This will avoid security problem occurring. The signature will like as @123%, wua%$^ etc.

3. PERFORMANCE ANALYSIS

3.1 Modules

- A role-based access control scheme.

- Security and privacy scheme.
- Secure patient data transmission using RSA algorithm (Enhancement).

A role-based access control scheme

Most current e-/m-healthcare systems require doctors to participate in medical information processing, which brings two problems are low effectiveness caused by manual operations and privacy breaches due to doctors private data. A medical expert system that can automatically analyze user's private data but minimize doctors participation can address these two problems using current wearable medical devices and nodes cannot be directly linked with smart mobile terminals through 4G or Wi-Fi. Even when the mobile phone has been directly equipped with medical sensors or biometric information-sensing components, current technology limits it to collecting only one or two data items.

There are 3 different concepts are included which have been improved at each discussion as,

- Occurrence of Collision.
- Collision time delay.
- Collision co-operative.

Security and privacy scheme

To avoid collision which ensure the security of medical data transmitted in wireless sensor networks, key distribution schemes and block encryption methods are required. A key distribution scheme based on a group send-receive model (GSRM) and AES was improved. The procedure of building a group from those nodes which has the leader node will record the count of its neighbour nodes with the same GSRM-level values. To better adapt to the privacy-preserving characteristics of HES, HEBM (Homomorphic Encryption Based on Matrix) also introduced. Therefore, HEBM can effectively resist the following attacks.

- A leakage of privacy by the administrator or anyone who owns the highest authority.
- Eavesdrop attack. The attacker is unable to access substantive information.
- Chosen plaintext attack. the attacker has already obtained the entire records of a specific user who utilized medical services from HES times.

However, some problems remain unsolved; for example, the diagnosis reliability of the expert system is not perfect, and HES cannot currently monitor or analyze sudden diseases.

- Low effectiveness caused by manual operations.
- Privacy breaches due to doctors.
- Many e-/m-healthcare architectural fails in terms of feasibility of data transmission directly from WBANs to WPANs.
- And because of Internet implementation difficulty.
- Low performance and less efficiency.

Secure patient data transmission using RSA algorithm (enhancement)

- Two keys can be used to encrypt and decrypt .
- Signature can be used for transmission security.
- Maximum packet loss can be avoided.
- Token analysis for every transaction.
- All nodes in the network are randomly placed with auction which is act as router.
- Some nodes are authorized to the source nodes which make the registration for such nodes.
- Sensor indicates ,if any problem occurred for patient to their respective specialist doctors and also to authorized node.
- Adversary node creates clone node.
- Make packet loss.
- Using flooding mechanism, the common node transmit private key to all other node in order to gather node information.
- The node which do not sent request are said to be clone node and the node which has same user id which is shared to clone node are said to be adversary.
- Therefore, data can be send to destination without any modification using RSA algorithm.

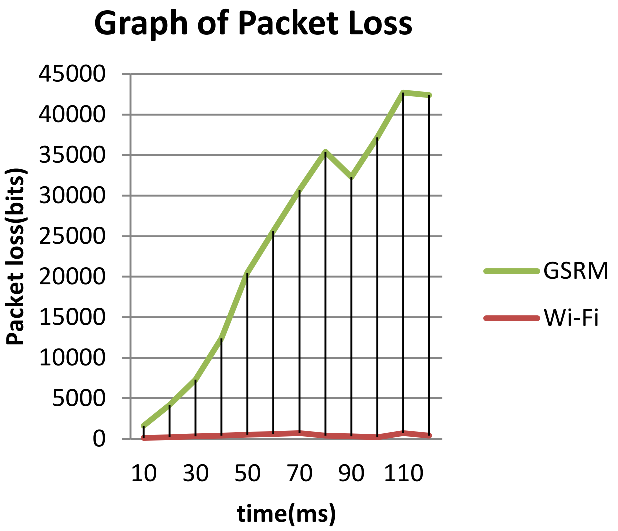

Fig 3.1 Packet loss graph

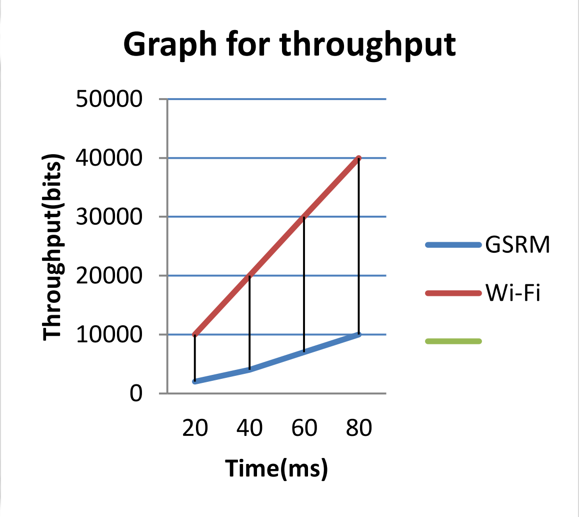

Fig 3.2 Throughput graph

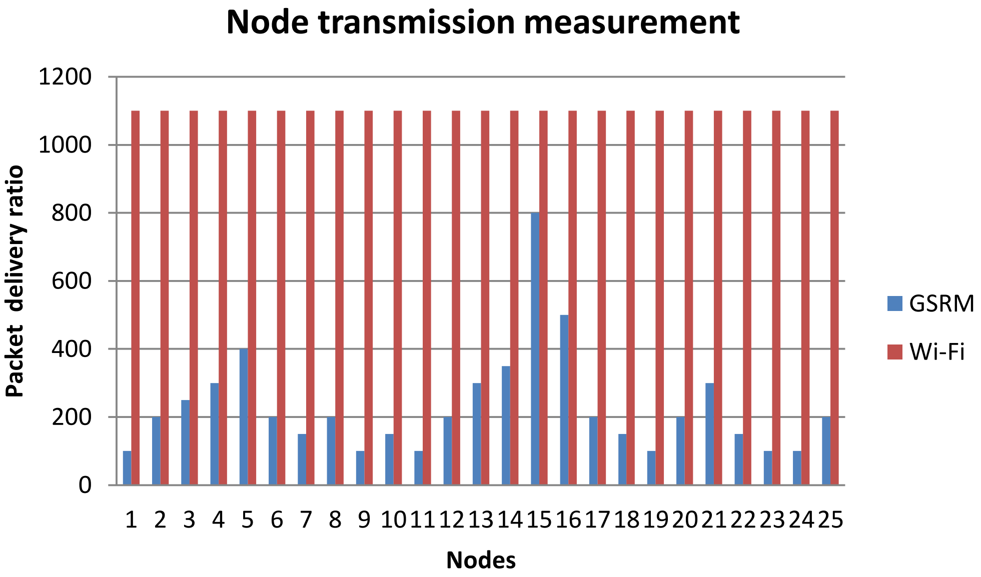

Fig 3.3 Graph of node strength

4. CONCLUSION

This shows the improvement of security and privacy using RSA algorithm and advanced mobile application. We proposed a secure and lightweight system for wireless medical sensor network. The medical data transmission is done in a secure manner using hash chain based key updating mechanism. Fine-grained access control was achieved using proxy protected signature technique. The two security techniques such as hash-chain based key mechanism and proxy key signature technique achieves the goal i.e. secure patient medical data transmission and access control in the wireless medical sensor network. The system offers great conveniences to both patients and health care providers. This demonstrates an intelligent system for mobile health monitoring.

REFERENCE

[1] Amirbekyan and V. Estivill-Castro, “A New Efficient Privacy-Preserving Scalar Product Protocol,” in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM ’07), 2007, pp. 209-214.

[2] Bekara and M. Laurent-Maknavicius, “A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks,” in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[3] Rifat Shahriyar1, Md. Faizul Bari2, Gourab Kundu3, Sheikh Iqbal Ahamed, and Md. Mostofa Akbar Intelligent Mobile Health Monitoring System (IMHMS), International Journal of Control and AutomationVol.2, No.3, September 2009.

[4] Yanzhi Ren, Yingying Chen, Mooi Choo Chuah, and Jie Yang, "Smartphone Based User Verification Leveraging Gait Recognition For Mobile Healthcare Systems," IEEE SECON 2013.

J. J. Yang, J. Q. Li, and Y. Niu, “A hybrid solution for privacy preserving medical data sharing in the cloud environment,” Future Generation Computer Systems, vol. 2015, no. 43-44, pp. 74-86, Nov. 2015.