International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9288-9293

A Probably Secure WiFi Based Health Monitoring System through Assymetric Cryptography (RSA) Using Embedded Applications

G.Pandit Samuel[1]
Assistant Professor,

Ch.D.Naidu[2]
Sr. Assistant Professor

Suresh Chettineni[3]
Professor

[1,2,3] *Information Technology Department, Anil Neerukonda Institute of Technology and Sciences (ANITS) Bheemunipatnam, Sanghivalasa, Visakhapatnam, Andhra Pradesh 531162, India.*

Abstract

The most important thing in this world is one's life, large percentage of loss of life's are due to late action according to the patients health emergency. In this fast growing bio medical field, monitoring the health condition of a patient for acting in terms of emergency is very important. It's also required that the information reaches the concerned Doctors, nurses and important medical departments for their immediate support. As the data passes through an unsecured public channel, it is also important in maintaining confidentiality and integrity towards the data with proper authenticity.

Towards this prospective, this paper proposes a web based health monitoring system for continuous monitoring of health of a patient using biomedical sensors like temperature sensors, pulse oximeter, etc, where the data collected through the sensors are ordered through a microcontroller which is updated to the cloud web server for accessing it from any place possible through internet while providing security to the data which is updated to the web server with proper strong encryption mechanism. This project also aims to provide strong Authentication mechanism using password protection.

Keywords: Health care system, Android smart phone, web server, cryptosystems and Authenticity.

INTRODUCTION

Many primary healthcare clinics in rural areas do not have any healthcare electronic systems and continue to operate on paper based systems and patients have to keep their medical records by themselves. In certain conditions physician may not be available, in such cases patients may have to face a number of difficulties. In case of emergency it may also lead to the death of patient. In such case wearable healthcare monitoring systems will play a very important role in breath breaking situations. The patients under certain health conditions need to be monitored continuously for predicting certain changes in the body, In such cases health monitoring systems takes a major role in protecting the patient's life even in the absence of the prescribed doctor. As the nation's healthcare infrastructure continues to evolve new technologies promise to provide readily accessible health information that can help people to address personal and community health concerns. In general wearable and implantable medical sensors and portable computing devices present many opportunities to provide timely health information to physicians, public health professionals as well as consumers.

Fig 1 health care monitoring system architecture describes the functional design of the system. The paper proposes an approach with physiological health parameters such as heart rate, temperatures which are continuously monitored and send to personal or home server via Zigbee transceiver where any authenticated user can access it.

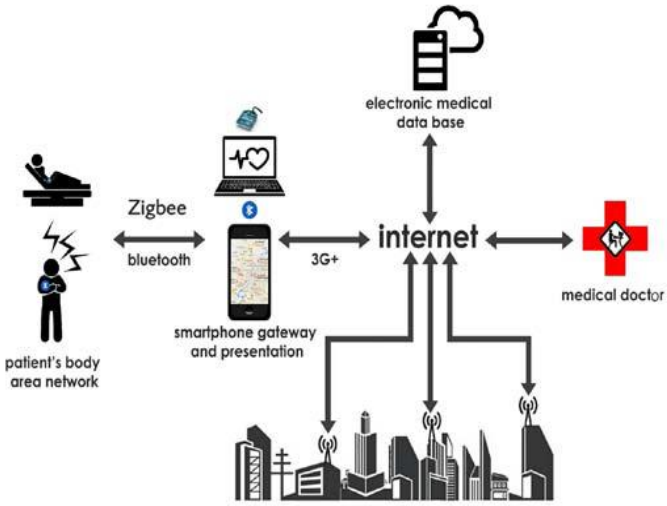

Figure 1: Health care monitoring system architecture

RELATED WORK

The approach proposed in this paper provides integrated solution to all aspects of healthcare monitoring systems such as power consumption, cost and complexity. Using it, the healthcare monitoring system with low power consumption, low cost can be design. Related work includes various techniques and work done related to healthcare monitoring systems.

In the literature, there are various works dealing with remote monitoring of patients. For example, in [9] a heterogeneous wireless access-based remote patient monitoring system is presented in which multiple wireless technologies are used to monitor continuous physiological signals in presence of patient mobility. In [10] author presents a methodological

review on the role of information technology and engineering models in transforming healthcare and explains how they can support the transformation in healthcare systems with the help of computational models. In [11] author proposed a hybrid framework for monitoring patient health status by using a sensor cloud. Benefits of using sensor cloud architecture are demonstrated for patient health-status monitoring. Christian Bachmann *et al.* [12] presented a comparative analysis of potential radios for use in health monitoring systems. The system is bulkier, much expensive, modules used are not wearable and there is no provision to minimize power consumption. In [2] author aims at developing the healthcare monitoring system for the monitoring of the patients by combining clinical observations with data from wearable sensors. Several authors addressed different issues related to cost, complexity etc but security issues and importance are not addressed. This proposed system addresses a strong encryption using Asymmetric cryptography using RSA algorithm to ensure the security of the data before storing it into the database.

HARDWARE AND SOFTWARE

In this section we discuss several hardware and software used in implementing the system

The hardware used in this proposed approach are LM35 temperature sensor, IR pair with LM324 amplifier to amplify the signal from IR pair as sensor nodes, 8051 microcontroller as sensor information receiving node, WIFI transmitter compatible with 8051 MC and receiver for transmitting data wirelessly between short distances. A cloud based Web server which acts as a web server to update the received information to be updated to the database which can be accessed by any individual with internet.

The software used in the proposed approach is phpMyAdmin database as a user friendly database, XAMPP server as front end server to serve pages according to the user requirement. The languages used to develop the web pages are HTML, CSS and java script which can be differed according to the developer. Keel, and flash magic software's are used to write embedded c programs and dump the code to the microcontrollers. This hardware and software are chosen to implement the proposed architecture with low cost, efficiency and ease of use into consideration.

DESIGN OBJECTIVES

This project helps in designing a low power healthcare monitoring system which is implemented using WIFI Technology. Following are the objective in designing a healthcare system.

1. The healthcare system has been designed using WIFI technology without using any intermediate machines to monitor but updating the data directly to the cloud with low power consumption.
2. The system will be cost effective and less complex
3. Data acquisition and transmission with low power.
4. Privacy through RSA encryption in the system for the database protection which is prone to security attacks
5. To solve the problems of the sensors of writing the complicated and cumbersome collected data program code.
6. An effective communication protocol will be proposed taking in to consideration the network partitioning with postural mobility.

PRAPOSED ARCHITECTURE

The proposed system architecture as shown in fig.2 can be explained as follows, the system can be divided into sensor nodes, a microcontroller unit and a wired and wireless communication unit.

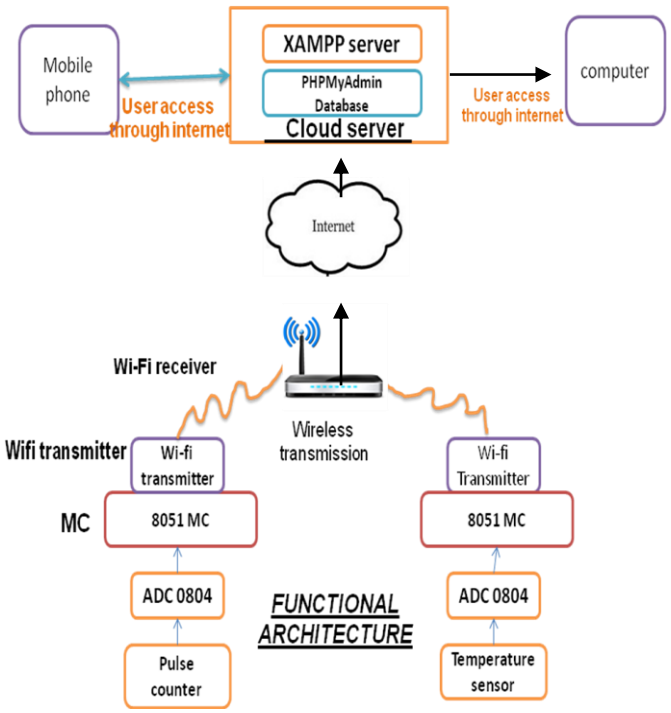

Figure 2. Functional architecture

The Fig 2 explains the constructional model of the system. There are two nodes which are connected to central cloud server. Each node is constructed using a sensor (i.e Temperature sensor) where the sensor is interfaced to a microcontroller using an Analog to digital converter (ADC). As the temperature sensor senses the temperature and transmits it in Analog, the data has to be converted into digital for the microcontroller to access it. So, an ADC0804 is used.

The 8051 microcontroller transmits the received temperature adding the primary key contents to uniquely identify the patient to the web server through internet. Here Wifi transmitter and receiver acts as an transmitting and receiving entity to connect to the internet. Use of Wifi also reduces the

use of wires. At the server PC the data is stored in a database which can be accessed by any authenticated user from anywhere else in the world with proper internet facility.

Hardware Connectivity

The hardware connectivity explains us the interfacing of different hardware components knowing their pin configurations as shown in the fallowing figures fig 3 and fig 4

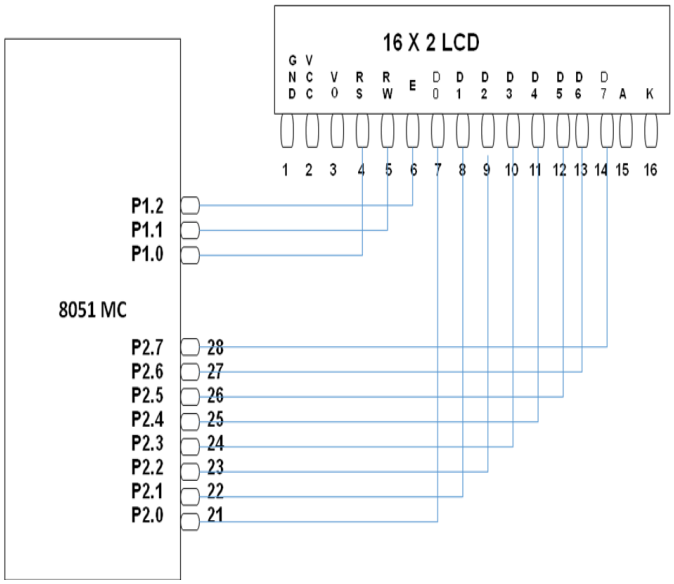

Figure 3. Interfacing 8051MC to 16x2 LCD

From fig 3 and fig 4 we can identify the hardware connectivity of the system

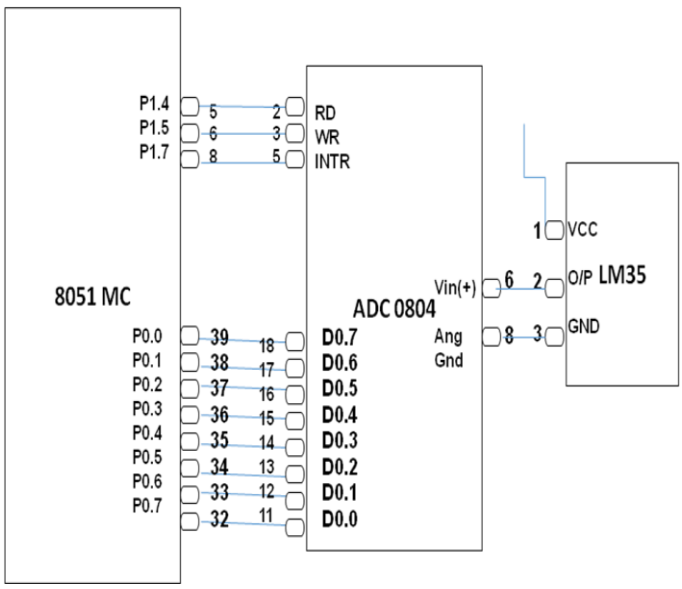

Figure 4. Interfacing of MC8051, ADC0804 and LM35

Software implementation

We use several software to implement the software part where a user can access a system using his webpage from anywhere else with internet connectivity available. The implemented webpages are shown in the fallowing figures

Figure 5. Home page

The fig 5 shows the home page where a user can interface with the system. Here we have three categories of users namely Doctors, Nurses and pharmacist, where these three users are given different privileges according to their requirement

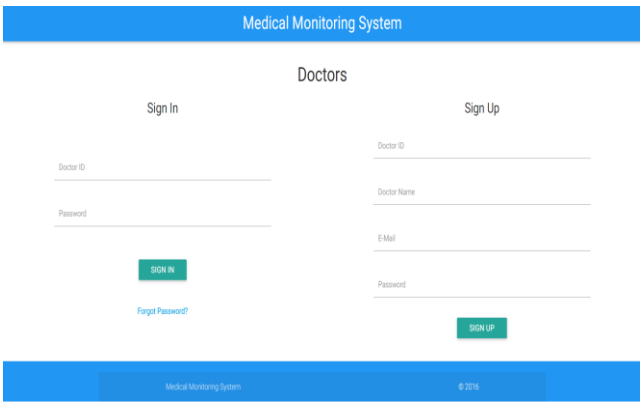

Figure 6. Doctors login page

On the home page we can find three menus such as doctor, nurse, and pharmacist. By clicking on doctor we can enter into the doctor's page as shown in fig 6. In the doctor login page we can view two sets of options if a doctor is already an registered user he can directly enter the doctor Id and his password to access his credentials but in case the doctor is not an registered user he can sign up giving his details on the right column of the page, the doctor is authenticated after verifying the credentials by the administrator.

The doctor's login details are automatically verified comparing the details of the database by maintaining the authenticity of the system. This is common for all the users.

Figure 7. Doctor View page

Entering into the doctors view page, the doctor can view the details of the patient and the information of the patient. Doctor can also update the updates at the comments portion in order for proper advice which will be updated in the database which can also be viewed by the nurses and pharmacist. This is similar for all the three members of the system.

SECURITY AND AUTHENTICITY

The proposed systems major goal is to provide security to the data which is passing through the unsecured public channel. For this cause every user of the system is authenticated using a username and a password which provides authenticity to the system.

Secondly every data travelling through the unsecured channel has to be secured for its integrity. For this cause, we use a strong cryptography algorithm to encrypt all the data passing through the public channel. We choose RSA algorithm using Asymmetric key algorithm to form a crypto system. The algorithm and steps are as follows.

Encryption Steps using RSA Crypto System at the Source

Key generation algorithm:

This is the original algorithm.

1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (phi) φ= (p-1)(q-1).
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi).
5. The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d. Other times we might write the key pair as ((N, e), d).]

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

Algorithm: Generate an RSA key pair.

INPUT: Required modulus bit length, k.

OUTPUT: An RSA key pair ((N,e), d) where N is the modulus, the product of two primes (N=pq) not exceeding k bits in length. e is the public exponent a number less than and coprime to (p-1)(q-1) and d is the private exponent such that ed=1(mod(p-1)(q-1).

1. Select a value of *e* from {3, 5, 17, 257, 65537}
2. **repeat**
3. p ← genprime(k/2)
4. **until** (p mod e) ≠ 1
5. **repeat**
6. q ← genprime(k - k/2)
7. **until** (q mod e) ≠ 1
8. N ← pq
9. L ← (p-1)(q-1)
10. d ← modinv(e, L)
11. **return** *(N, e, d)*

Encryption Steps:

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer *m*, 1 < m < n
3. Computes the cipher text $c = m^e \bmod n$.
4. Sends the cipher text *c* to B.

Decryption Steps:

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative *m*.

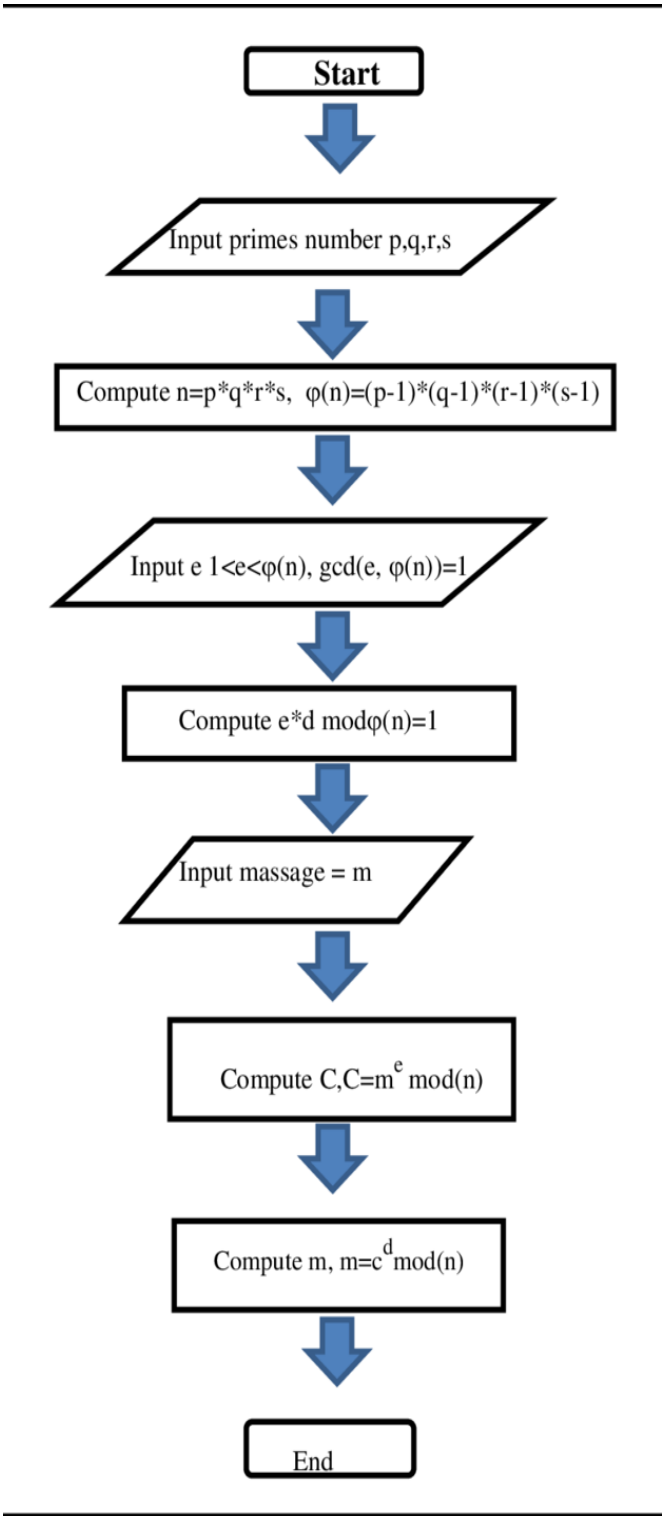

Figure 8. Flow chart for hybrid encryption

Fig 8 shows the RSA algorithm flowchart which can be studied easily.

The encryption of the data before transmitting it into the unsecured channel internet is done at the sensor node level.

The algorithm is implemented in 8051 microcontroller using embedded c coding which encrypts all the data using certain generated key and then encrypted data is travelled through internet to be stored in the web server's database. The authenticated user can access the data from the database which is decrypted using the private key using client server request.

CONCLUSION AND FUTURE SCOPE

A probably secure Wifi based health monitoring system through Asymmetric cryptography (RSA) using embedded applications has been designed and successfully implemented in this work. Since the proposed system does not add any additional nodes as intermediates, we can conclude that it is a low power and low cost system. Moreover, major part of the proposed system has been implemented using keel software. The proposed system has been designed for security of sensitive patient information using RSA cryptosystem. We can conclude that the system is probably secured one. The proposed system is designed to provide access to authenticated users like Doctors, nurses, pharmacists from anywhere using the internet. Hence we can conclude that system can be accessed from any part of the world using internet. Hence, the proposed system is easily reconfigurable and it can be connected to the Internet easily. The system is also able to store physiological data of patients for 24 hours a day and seven days a week. In future the proposed system can be extended to include more sensors that can measure more parameters like diabetes and blood pressure. The proposed system is flexible enough to include such kind of modifications.

Hence, the proposed system would probably address the secure communication between the microcontroller unit and the web server using a strong cryptosystem and also specifies the secure Authentication mechanism to identify every individual user accessing the system through internet

Future scope

The key drawback of this proposal is that there are no intermediate i.e. local servers or internetworking servers. In such cases if internet fails the details cannot be updated or collected by any individual. This issue can be addressed by installing a local server through which the data is updated to the web server.

A probably secure Wifi based health monitoring system through Asymmetric cryptography (RSA) using embedded applications is presented which allows doctor to view his patient's medical parameter remotely and dynamically in a Web page in real time and does not need to have any special requirement on his PC or mobile. All he needs is an internet access. In future we can add a set of sensors to completely monitor the health condition of a patient. We could also extend this work in developing the entire system wireless without using wires. We can also extend our study towards different security attacks on medical databases and authentication systems in evaluating the threats and securing the contents accordingly.

REFERENCES

[1] *Alexandros Pantelopoulos and Nikolaos G.Bourbakis*, "A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis", IEEE Transactions on Systems, Man and Cybernetics, Vol.40, No.1, January 2010, pp.1-12.

[2]. "Android based health care monitoring system" *by Maradugu Anil kumar, Y.Ravi sekhar* at IEEE sponsored 2nd international conference information embedded and communication systems ICIIECS'15

[3]. "Real time wireless health monitoring application using mobile devices" *by amna abdullah, asma ismael, aisha rashid, ali abou-elnour, and mohammed tarique* at International Journal of Computer Networks & Communications (IJCNC) Vol.7, No.3, May 2015

[4]. *H. Ting and W. Zhuang*, "Bluetooth-Enabled In-home Patient Monitoring System: Early Detection of Alzheimer's disease," IEEE Wireless Comm., Feb. 2010, pp. 74-79.

[5]. "ARM Based Remote Monitoring and Control System for Environmental Parameters in Greenhouse " ,by *Nagesh Kumar D.N in* IEEE transactions 2015

[6]. *Jae Hyuk Shin, Boreom Lee, and Kwang Suk Park*, "Detection of Abnormal Living Patterns for Elderly Living Alone Using Support Vector Data Description," IEEE Transactions on Information Technology in Biomedicine, Vol. 15, No. 3, May 2011, pp.438-448.

[7]. "Wearable Sensors for Human Activity Monitoring": A Review , *by Subhas Chandra Mukhopadhyay, Fellow, IEEE at* IEEE SENSORS JOURNAL, VOL. 15, NO. 3, MARCH 2015

[8]. *Juan M. Corchado, Javier Bajo, Dante I. Tapia, and Ajith Abraham*, "Using Heterogeneous Wireless Sensor Networks in a telemonitoring System for Healthcare," IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 2, March 2010, pp.234-240.

[9] *Dusit Niyato, Ekram Hossain and Sergio Camorlinga*, "Remote Patient Monitoring Service using Heterogeneous Wireless Access Networks: Architecture and Optimization," IEEE journal on selected areas in communications, vol. 27, no. 4, pp. 412-423, May 2009.

[10] *Misha Pavel, Holly Brugge Jimison, Howard D. Wactlar, Tamara L. Hayes, Will Barkis, Julia Skapik, and Jeffrey Kaye*, "The Role of Technology and Engineering Models in Transforming Healthcare," IEEE reviews in biomedical engineering, vol. 6, pp.156-177, 2013.

[11] *Mohapatra, S., Rekha, K.S.:* 'Sensor-cloud: a hybrid framework for remote patient monitoring', Int. J. Comput. Appl., 2012, 55, pp. 1–11.

[12] *Christian Bachmann, Maryam Ashouei, Valer Pop, Maja Vidojkovic, Harmke de Groot, and Bert Gyselinckx,* "Low- Power Wireless Sensor Nodes for Ubiquitous Long-Term Biomedical Signal Monitoring," IEEE Communications Magazine , pp. 20-27, January 2012.

[13]. *Reza S. Dilmaghani, Hossein Bobarshad, M. Ghavami, Sabrieh Choobkar, and Charles Wolfe*, "Wireless Sensor Networks for Monitoring Physiological Signals of Multiple Patients," IEEE Transactions on biomedical circuits and systems, vol. 5, no. 4, august 2011, pp.347- 356.

[14]. *Rong Fan, Ling-Di Ping, Jian-Qing Fu, Xue-Zeng Pan,* "The New Secure and Efficient Data Storage Approaches for Wireless Body Area Networks," IEEE 2010.

[15]. "Design and Implementation of Wireless Patient Health Monitoring System*" by Prakash H. Patil, Pratyush Singh, Swatee Biradar, Prasad Rane* at International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 6, June – 2013

[16]. *Yifeng He, Wenwu Zhu and Ling Guan*, "Optimal Resource Allocation for Pervasive Health Monitoring Systems with Body Sensor Networks", IEEE Transactions on Mobile Computing, Vol.10, No.11, November 2011, pp.1558-1575.