ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 9, September 2016

A Probably Secure Arm Based Health Monitoring System through Hybrid Cryptography Using Embedded System

Mrs. Ch.sirisha , Mrs. Navya Nidigatti

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 of at most importance. It's also important that the information reaches the concerned Doctors, nurses and important medical departments for their immediate support , As the information passes through an unsecured public channel, it is also important in maintaining confidentiality and integrity towards the data with proper authenticity.**

For this cause, this paper proposes a web based health monitoring system for continuous monitoring of health of a patient using different sensors like temperature sensors, pulse oximeter, etc, where the data collected through the sensors are ordered through a microcontroller which is updated to the 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.

Index terms- **Health care system, Android smart phone, web server, cryptosystems and Authenticity.**

I. 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 many rural areas many times the physician may not be available in such case patients have to face lots 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.

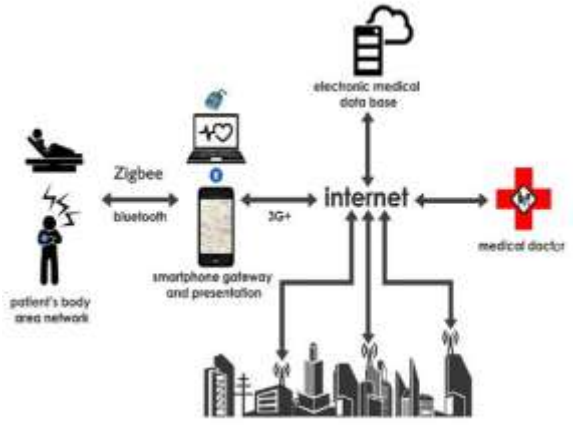

Fig 1: Health care monitoring system architecture

II. 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 including into the health monitoring systems are not addressed. This proposed system addresses a strong encryption using hybrid cryptography to ensure the security of the data before storing it into the database.

III.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 , Zigbee transmitter and receiver for transmitting data wirelessly between short distances. ARM cortex M3 board with NXP LPC1768 microcontroller is used as a base station to receive data from the two sensors, An PC which acts as a web server to update the received information to be updated to the database.

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 develop the web pages are HTML, CSS and java script. Keel, and flash magic software's are used to write embedded c programs and dump to 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.

IV.DESIGN OBJECTIVES

This project is designs a low power healthcare monitoring system is implementing system using NXP LPC1768 microcontroller. Following are the objective in designing a healthcare system.

1. The healthcare system has been designed using ARM Cortex LPC 1768 Microcontroller 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 hybrid 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.

V.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.

The Fig 2 explains the constructional model of the system. There are two nodes which are connected to the base station. 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.

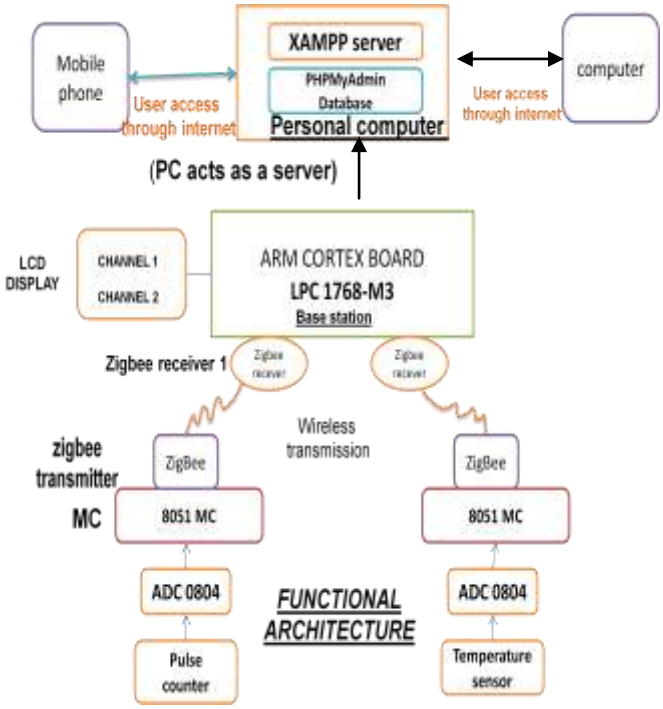

Fig 2. Functional architecture

The 8051 microcontroller transmits the received temperature to the ARM Cortex M3 base station using a zigbee transmitter. Here zigbee transmission is used to transmit data wirelessly in mesh network form without using wires. The data received at the base station is updated to a server PC using serial line. 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

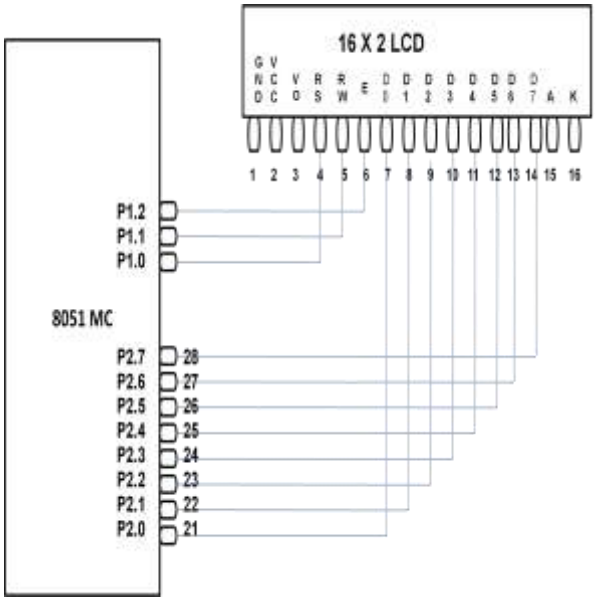

Fig 3 interfacing 8051MC to 16x2 LCD

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

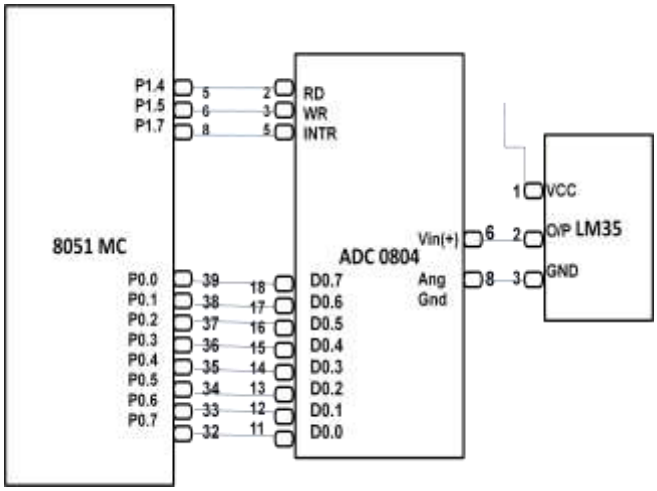

Fig 4 interfacing of MC8051, ADC0804 and LM35

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

Fig 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

Fig 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.

Fig 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.

VI .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 Hybrid encryption using both symmetric key and Asymmetric key algorithm combining to form a hybrid crypto system. In this we use a combination of two algorithms RSA and Deffie Helmen as Asymmetric and Symmetric key algorithm. The algorithm and steps are as follows.

Encryption Steps using Hybrid Crypto System at the Source

- source has destination public key(PUK)

- Inputs: Plain Data Block (PDB) Symmetric Key (SK)
- Outputs: Encrypted Data Block *(EDB)*
- Note: EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)

Encryption Steps:

1) Encrypt PDB using SK to get ED.
(Note: This can be done using any symmetric-key crypto algorithm like DES and AES)
2) Encrypt SK using destination's PUK to get ESK. (Note: This can be done using any public key algorithm like RSA)
3) Concatenate ED with its corresponding ESK to get EDB which is sent to the destination. EDB = {ESK, ED}

Decryption

Prerequisite: Destination has its Private Key (PRK)
Inputs: Encrypted Data Block (EDB)
Note: EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)
Outputs: *Plain Data Block (PDB)*

Decryption Steps:

1) Decrypt ESK using PRK to retrieve SK.
(Note: This should be done using the same public key algorithm which is used at source)
2) Use the retrieved SK as decryption key to decrypt ED to get PDB.

Hybrid crypto system using RSA and D-H

Steps of this algorithm are as

1. Choose two large prime numbers P and Q.

a. Calculate N = P x Q.

b. Select public key (i.e. encryption key) E such that it is not a factor of (p-1) and (q-1)

c. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1

Suppose R, S and G is automatic generated prime constants and put A=E and B=D

2. Now calculate following as public number $X= G^A$ mod R $Y= G^B$ mod R

3. Calculate session key with formula $KA = Y^A$ mod R $K_B = X^B$ mod R Such that $K_A = K_B = K$.

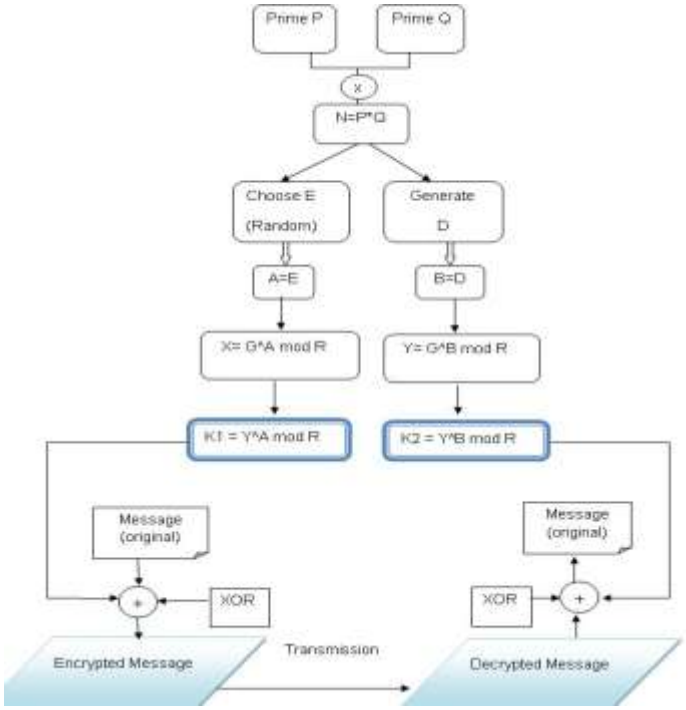

Fig 8 flow chart for hybrid encryption

Fig 8 shows the hybrid encryption flowchart which can be studied easily

VII CONCLUSION AND FUTURE SCOPE

A probably secure ARM based health monitoring system through hybrid cryptography using embedded system has been designed and successfully implemented in this work. Since the proposed system is based on ZigBee, 8051 microcontroller and ARM cortex M3 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 hybrid 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 an strong cryptosystem and also specifies the secure Authentication mechanism to identify every individual user accessing the system through internet

Future scope

A probably secure ARM based health monitoring system through hybrid cryptography using embedded system application 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

AUTHORS PROFILE:

Mrs. Ch . sirisha received her M.Tech degree from Kakatiya institute of technology and sciences (KITS) in the field of digital communication in the year 2007. She is pursuing her PHD degree from Andhra University in the filed of wireless communication. she held her positions as Assistant Professor in the MLRIT and GVPCEW. The area of interests are Embedded Systems, Digital Communication and wireless communications. She had publications under the title "Low-power, Low-Transition Test Pattern Generator in Logic BIST Schemes" in international journal of scientific & engineering research, volume 5, issue 9, september-2014 and "Performance Optimization of Dynamic and Domino logic Carry Look Ahead Adder using CNTFET in 32nm technology "in IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) in 2014 and 2015 respectively.

Mrs. Navya Nidigatti was awarded a B.Tech degree in the year 2014 from Pydah College of engineering, Visakhapatnam in the field of electronics and communication engineering and present pursuing her M.Tech degree from Gayathri vidya parishad engineering college for women. Her area of interests are in Embedded systems and embedded programming.