MODERN HEALTHCARE SYSTEM USING BODY SENSOR NETWORK WITH AES ALGORITHM

Kishan Kumar Chaurasiya, N.Kiran Sai, SK.Reshma
Department of Electronics and communication
SRM University, Chennai
Email:kishankumar0455@gmail.com

Ms. A.Ramya
Asst.Prof(O.G)
Department of Electronics and Communication
SRM University, Chennai

ABSTRACT--Due to the heavy equipment and the need of doctor to be present at the hospital the manual and periodic inspection of patient's health will be difficult.The patient cannot leave the premises of the hospital and the doctor. To overcome this inconvenience we can use Body Sensor Network (BSN) and Internet of Things (IOT) technology for real-time monitoring, patient information management, and healthcare management of patient even in open environment and even in the absence of doctor. In this modern health care environment, by using the IOT technology brings convenience of physicians and patients. However, development of this new technology in healthcare applications without considering security makes patient privacy defenseless. The Security hazards such as: Data Privacy, Data Integrity, Data Freshness, Authentication, Anonymity should be considered in the IOT. In this paper, the security issues can oppressed by using 128- bits Advanced Encryption Standard (AES) algorithm. The automatically updated data from the BSN can be seen on the website. Besides, when there is any abnormalities in data the web server sends immediate alert to the person/ family members/ emergency room through beep.

Key words: IOT, RFID Module, AES Encryption

I.INTRODUCTION

In the present day the manual and periodic inspection of patient is done. For this process the patient and Doctor should be present in the hospital which might interrupt their convenience and By using Internet of Things (IOT) technology real-time monitoring of patient is done even in the absence of doctor so by observing [1] BSN using IOT is used. it is highly necessary to give precautions aimed to prevent Netizen from creating fake accounts to do criminal offence. One of the means is to use authentication code where it contains activation message. This authentication code is generated through activation message combined with timestamp values which would further be used on One-time Password. Then, it would be encrypted using Advanced Encryption Standard cryptographic algorithm, the generated authentication code can only be used once within a limited time [2]. However, development of this new technology in healthcare applications without considering security makes patient privacy defenseless.The Security requirements such as: Data Privacy, Data Integrity, Data Freshness, Authentication, Anonymity should be considered in the IOT [3]. Radio frequency identification (RFID) offers tantalizing benefits for supply chain management, inventory control, and many other applications. Only recently, however, has the convergence of lower cost and increased capabilities made businesses take a hard look at what RFID can do for them it can be used as ID card for patient[4][5]it can be connected to computer for direct communication with IOT[6]. Wireless medical sensor networks, also called e-Healthcare systems, provide mobility to the patients for making life easier and comfortable. However, a secure mobility support is highly desirable to a patient while he/she is moving. Healthcare applications, and propose a secure session-key scheme for addressing security issue [7]. The proposed mechanism, only simple cryptographic operations (i.e. one-way hash function, XOR operation) are used in RFID tag [8].The Motivation Behind this paper is very well discussed in **Section II. Section III** describes the problems with the present day systems .The proposed Methodology for solving the problems is described in **Section IV.** Simulation analysis for the system is very well depicted in the **Section V**.

II.PROBLEM DEFINITION

In general, the manual and periodic inspection of patient is done. For this process the patient and Doctor should be present in the hospital which might interrupt their convenience.

In the modern health care environment, By using Internet of Things (IOT) technology real-time monitoring of patient is done even in the absence of doctor. However, development of this new technology in healthcare applications without considering security makes patient privacy defenseless.

The Security requirements such as: Data Privacy, Data Integrity, Data Freshness, Authentication, Anonymity should be considered in the IOT.

III.PROPOSED METHODOLOGY

This system consists of NODE MCU (ESP 8266) which does all the function according to the interfaced program. RFID readers are present with each patient to get the detail about them. After scanning it the complete data of patient is shown so required sensor are attached to them. IOT is use to send the information of the patient to the monitoring section at the same time it is transmitted to the server.

In the BSN network Temperature sensor and Blood Pressure sensors are used on the patient's body In general, security is a concept similar to safety of the system as a whole. Now, the communication in sensor network applications (like BSN) in healthcare are mostly wireless in nature. This may result in various security threats to these systems. These are the security issues cloud pose serious problems to the wireless sensor devices.

For security reason Wi-Fi and web page has login id and password. So know these they can only connect.

While transmitting the data the encryption is done by ESP 8266 so now one can hack it and decryption is done by the monitoring section.

RFID is used for identifying the person so directly they can scan and get the information

In this Project, several bio-sensors are placed on patient's body. These sensors are also known as BSN (Body Sensor Network) which are wearable tiny sensors. The advancement of BSN in healthcare applications have made patient monitoring more feasible. These sensors collect the physiological parameters of the patient body and transmit it wirelessly to the coordinator called Local Processing Unit (LPU) for further analysis.

The data collected from these sensors is sent to a Local Processing Unit (LPU). In this system the Wi-Fi module is representing LPU. From this Wi-Fi module the data is sent to the BSN- Care server. When the BSN-Care server receives data of a patient from Wi-Fi module analyses the data. Based on the degree of abnormalities of data, the web-server will interact with the family members of the person, local physician, or even emergency unit.

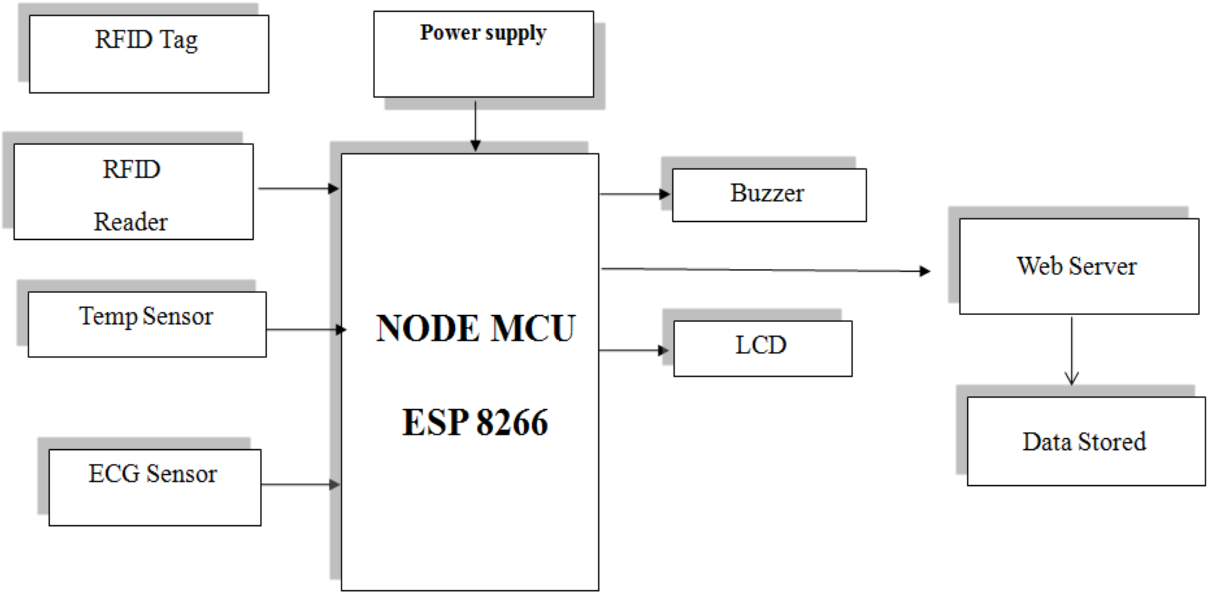


Fig. 1.Block diagram for processed methodology

Updated engineering standards / specifications of the design project

Description	**Engineering Standards / Specifications**
ESP8266	802.11 b/g/n
DS18B20	-55°C to +125°C (-67°F to +257°F)
EM18	6 to 10 cm.
PIR Sensor	• Range 10m • Angle of ± 15 degrees

EXAMPLE OF ACTION TABLE USING BP DATA

BSN BP	Data Action	Response
BP 120 Null	No Action	Null
BP > 130	Inform Family Members	FR:T/F
BP > 160 and	Inform Local Physician	FR:F PR:T/F
BP >160, FR:F and PR:F Inform Emergency ER:T/F	FR:F and PR:F Inform Emergency	ER:T/F

FR: Family Response; PR: Physician Response; ER: Emergency Response; T: True; F: False; BP: Blood Pressure

In IOT the Wi-Fi module and sensors are embedded with technology which is capable of exchanging data. In the healthcare area, IOT involves many kinds of cheap sensors (wearable, implanted, and environmental) that enable elderly people to enjoy medical healthcare anywhere, any time. In this system the health condition will be automatically updated to the internet through IOT for analysis continuously.

To fulfil some security requirements Radio-frequency identification (RFID) is used as it can store sensitive data, wireless communication with other objects, and identify and track objects automatically. This RFID is used to differentiate between the individual patients. Each patient is given a RFID tag which has unique RFID number.

A webpage is designed in which the patient's data will be collected from the sensors and then stores it securely on the cloud, where it can be accessed by those on the patient's care team in URL

The Wi-Fi module IP Address is 192.168.4.1 is used as an intranet. When we connect the internet to this Wi-Fi module the data is transmitted.

When we transmit the data through IOT many security measurements should be considered. As people sometimes feel uncomfortable knowing that their highly personal data is being stored and accessed. Patient's record system is encrypted with highly secured AES algorithm.

The following steps are taken to modify the AES algorithm and to design webpage for secured transmission of data thorough internet.

ESP 8266 Module:

The ESP8266 Wi-Fi Module is integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor.

This module has a powerful enough on-board processing and storage capability that allows it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development up-front and minimal loading during runtime

.

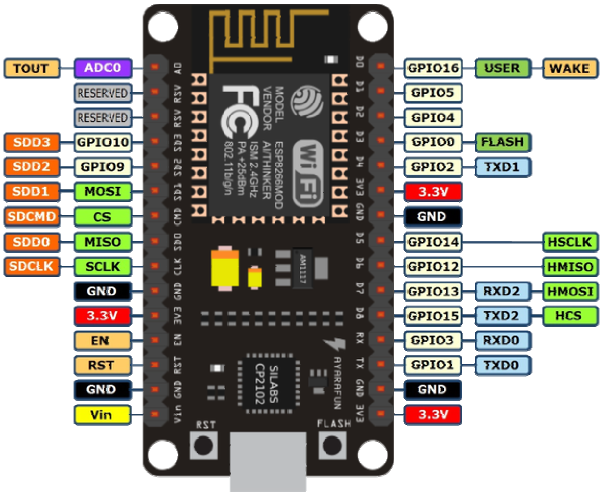


Fig. 2 block diagram for ESP8266

Features:

- 802.11 b/g/n
- Integrated TCP/IP protocol stack
- Integrated TR switch, LNA, power amplifier and matching network
- Power down leakage current of <10uA
- 1MB Flash Memory
- Integrated low power 32-bit CPU could be used as application processor
- Wake up and transmit packets in < 2ms
- Standby power consumption of < 1.0mW (DTIM3)

DS 1820:

DS18B20 is wire digital temperature sensor . Reports degrees C with 9 to 12-bit precision, -55C to 125C (+/-0.5C). Each sensor has a unique 64-Bit Serial number into it allows for a huge number of sensors to be used on one data bus.

Each DS18S20 has a unique 64-bit serial code, which allows multiple DS18S20 to function on the same 1-Wire bus.

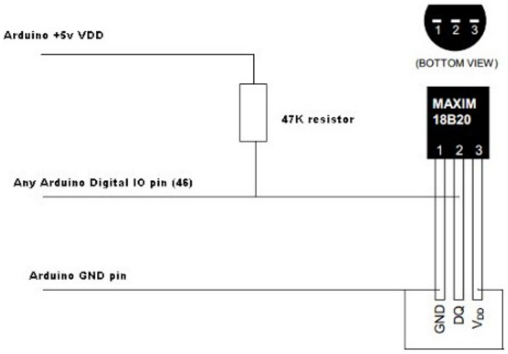


Fig. 3 circuit diagram for DSP18S20

Key Features

- Measures Temperatures from -55°C to +125°C (-67°F to +257°F)
- ±0.5°C Accuracy
- 9-Bit Resolution
- No External Components Required

RFID Tag and Reader

RFID (radio frequency identification) systems use data strings stored inside RFID tags) to uniquely identify people or objects when they are scanned by an RFID reader.
Key Features

- Reading Distance: 6-10 cm
- Frequency: 125kHz
- Current Rating: 35mA (Max)
- Operating Voltage: 4.6V - 5.4VDC

Pulse Sensor:

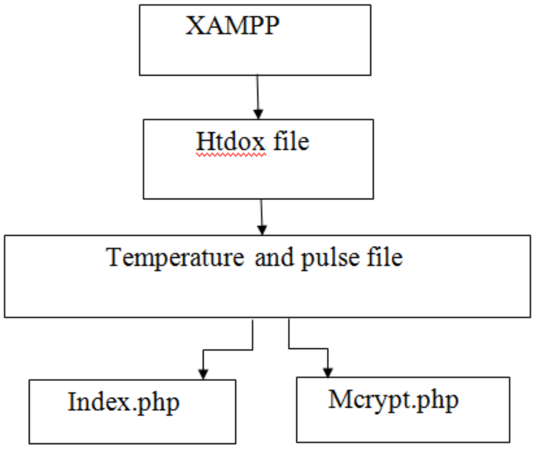
Electrocardiography (ECG or EKG) is the process of recording the electrical activity of the heart over a period of time using electrodes placed on the skin.
ECG sensors directly use electrical signals produced by heart activity. PPG uses electrical signals derived from light reflected due to changes in blood flow during heart activity.

IV. AES ENCRYPTION:

The AES algorithm is a symmetric-key algorithm. In this project 128-bits AES algorithm is used. This encryption is done at Wi-Fi module and at webpage where data is converted to cipher text form. At webpage decryption is also done and the data is shown in the plain text form. AES uses 10 rounds for In 128-bits. In each round 4 transformations are performed. The encryption key used in this project is

ENCRYPTION KEY: 0123456789abcdef

In decryption the same set of reverse rounds and the same encryption key are applied to transform cipher text into the original plain text.



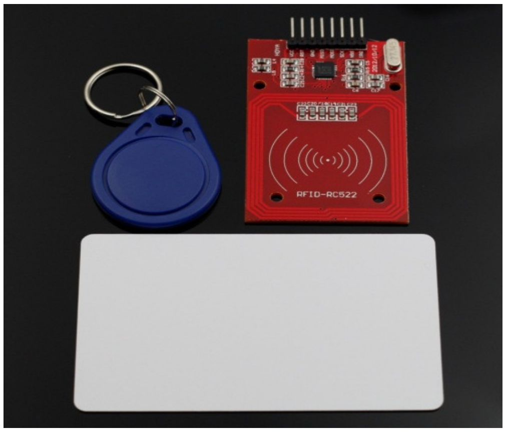


Fig. 4 block diagram for RFID Tag & Reader

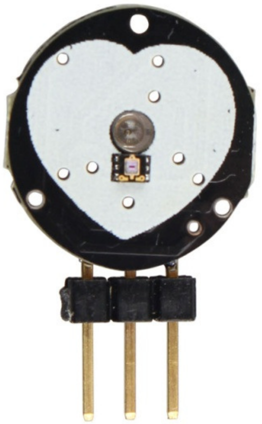


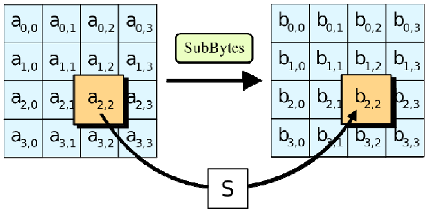
Fig. 5 diagram for Pulse Sensor

Figure 4 Block diagram for Flow diagram of AES Encryption code

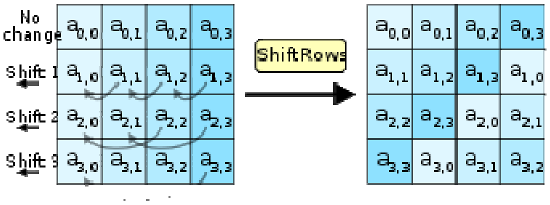
Rounds:

The 4 transformations are used in each round and in last round only 3 transformations expect MixColumns are used.

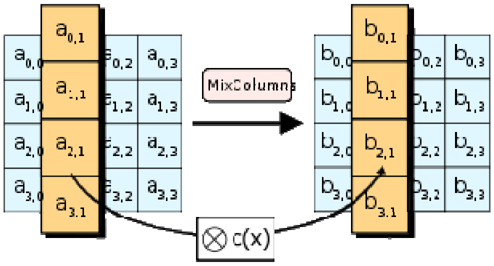
1. SubBytes - a non-linear substitution step where each byte is replaced with another.


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

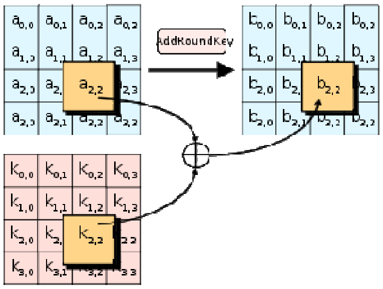
2. ShiftRows – The rows of the state are shifted cyclically a certain number of steps. N row is shifted left circular N-1 bytes.


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

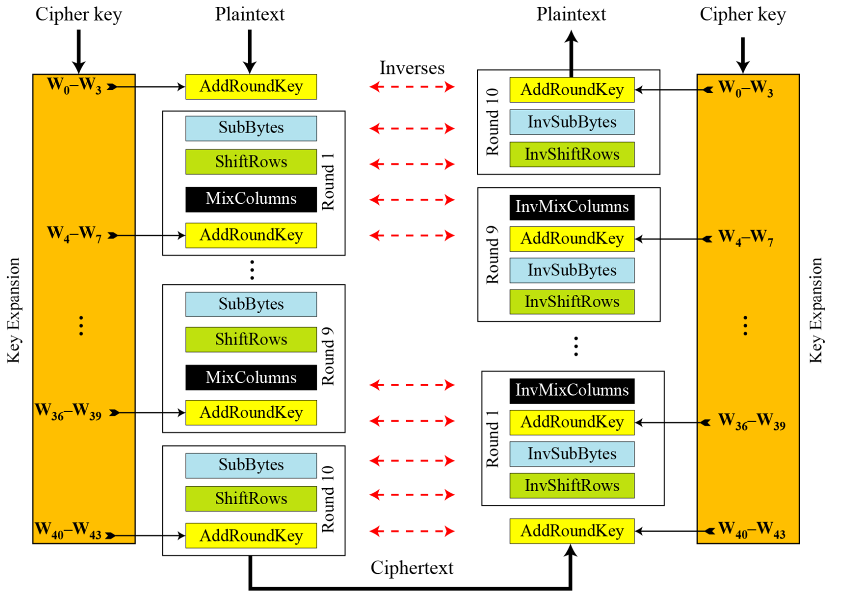
3. MixColumns - The columns of the state, combining the four bytes in each column.


MixColumns
⊗c(x)
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

4. AddRoundKey - each byte of the state is combined with a block of the round key using bitwise xor operation.


AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

<u>The overall structure for 128-bits AES algorithm</u> :



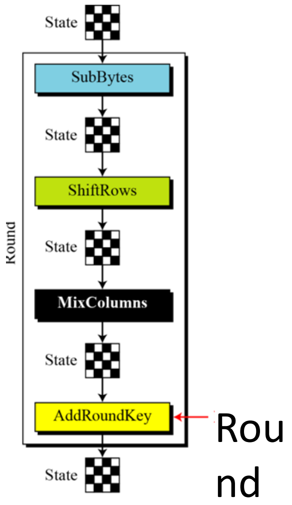


Fig. 6 block diagram for AGS Encryption.

XAMPP :

XAMPP stands for Cross-Platform (X), Apache (A), MySQL (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for to create a local web server. This file can be downloaded from the internet.

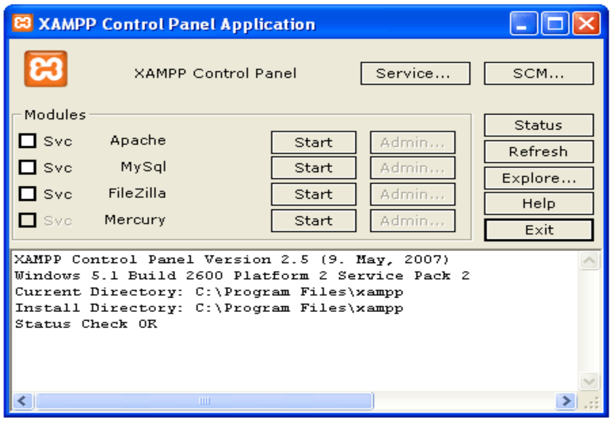
The location of installed XAMPP is (**C:\Program Files\xampp**) and double click on XAMPP Control Panel (**xampp-control.exe**). This will bring you following screen. Click on **Start** buttons next to Apache and MySQL for starting them

Htdox file: Under XAMPP root directory there is a folder called htdox. That's where the web site related documents are stored.

Temperature and pulse file: This file is created in htdox where the encryption code related to website and Wi-Fi module. In this two files are created.

V.CONCLUSION

This advantageous to many existing systems for its security advancement


XAMPP Control Panel Application
XAMPP Control Panel
Service...
SCM...
Modules
Status
Refresh
Explore...
Help
Exit
□ Svc Apache Start Admin...
□ Svc MySql Start Admin...
□ Svc FileZilla Start Admin...
□ Svc Mercury Start Admin...

```
XAMPP Control Panel Version 2.5 (9. May, 2007)
Windows 5.1 Build 2600 Platform 2 Service Pack 2
Current Directory: C:\Program Files\xampp
Install Directory: C:\Program Files\xampp
Status Check OK
```

Fig. 7 control panel for XAMPP Softwa

Index.php: The code for designing the website has been written using c and cpp programming language.

Mcrypt.php: The encryption and decryption code for webpage and the Wi-Fi module is written using Java programming language

. The RFID technology makes it easy to differentiate among patients.WiFi module helps to connect to the server wirelessly and transmits the data. The webpage is used to access the patient's data to authorised people by providing user ID and password. Thus, there is no doubt in saying that this system will help to reduce the burden to patient and doctor by using BSN technology and secure transmission of data through AES encryption method.

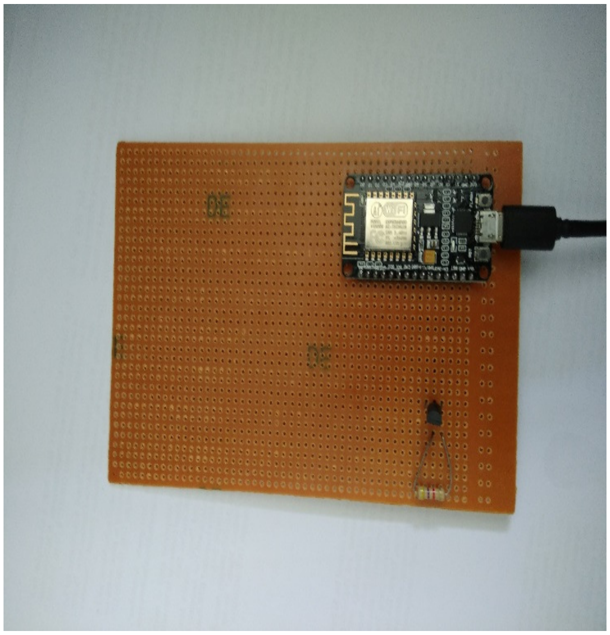
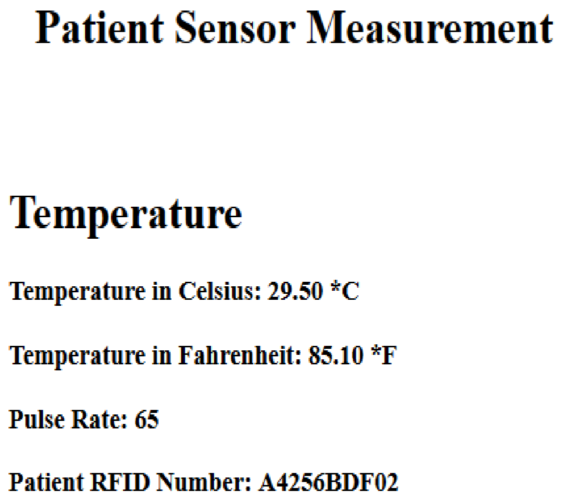


Fig. 8 circuit diagram for Normal Room Temperature.



Patient Sensor Measurement

Temperature

Temperature in Celsius: 29.50 *C

Temperature in Fahrenheit: 85.10 *F

Pulse Rate: 65

Patient RFID Number: A4256BDF02

Fig. 8.1 Temperature Reading.

The different temperature experiment is shown below in first case normal temperature of person is shown and in second temperature is increased.

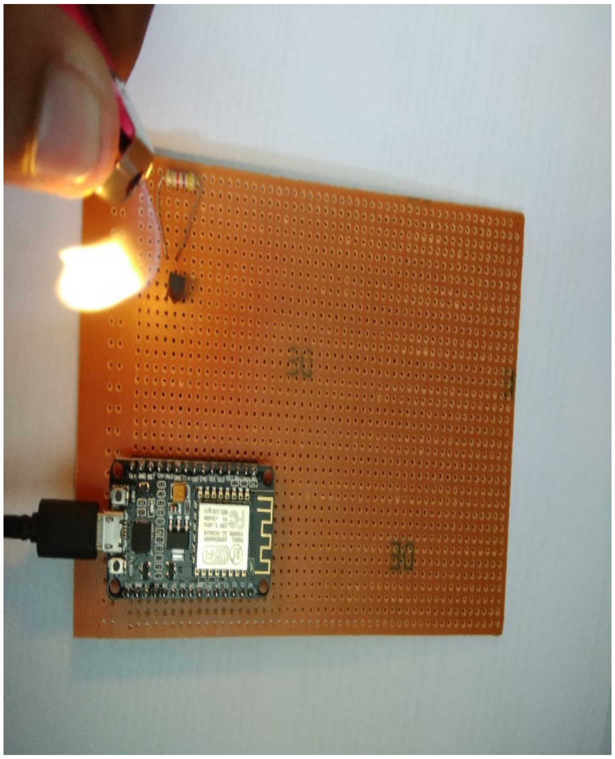
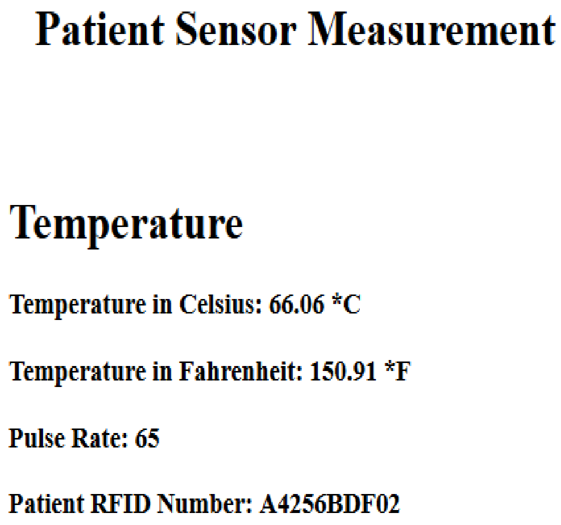


Fig. 9 circuit diagram At High Temperature



Patient Sensor Measurement

Temperature

Temperature in Celsius: 66.06 *C

Temperature in Fahrenheit: 150.91 *F

Pulse Rate: 65

Patient RFID Number: A4256BDF02

Figure9.1 Reading At High Temperature

VI.REFERENCES

[1]. P. Gope, T. Hwang, “BSN-Care: A Secure IOT-based Modern Healthcare System Using Body Sensor Network”. IEEE Sensors Journal 2015 DOI 10.1109/JSEN.2015.2502401.

[2]. SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, Iman Muhamad Ramadhan, 978-1-5090-1721-8/16 ,2016 IEEE.

[3]. Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256bit Encryption in Cloud,

4]. Debiao He and Sherali Zeadally , “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography.” IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, FEBRUARY 2015

[5]. R. Weinstein, “RFID: A technical overview and its application to the enterprise,” IEEE IT Prof., vol. 7, no. 3, pp. 27–33, May/Jun. 2005

[6]. P. Gope, T. Hwang, “A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System,” Computers & Security (Elsevier Journal), Vol. 55, pp. 271–280, 2015.

[7]. P. Kumar and H. Lee,“Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey.” Sensors (Basel, Switzerland) 12.1 (2012): pp. 55–91.