IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

Design of a Multi-Sensor IoMT Based Secured and Alert Health Monitoring System

Surabhi Joshi[1], Sunil Joshi[2]

Department of Electronics and Communication, CTAE, Udaipur, India[1,2]

Abstract: A reliable health monitoring system essentially requires real time and continuous monitoring of critical health parameters of the patient and a prognostic approach to generate and send an alert during medical emergency. Day by Day, the change in lifestyle increases, changes in environment which causes arising in the health problem, and require a daily or time to time check up to ensure about the health. As our senior citizen don't able to go hospital regularly for their regular check up. So our main to design such a module which is useful for them and overcome this issue plus making patient's data secure so that no one can steal crucial or sensitive data of patient's health. Here we have designed a prototype of a multi sensor IoMT (Internet of Medical Things) based secured Health Monitoring System in which we worked on two algorithm (compression and encryption (cryptography) technique) and four alert categories (SMS, Voice Call, VoIP and Email) based on biomedical embedded system and Internet of Things. Cloud computing is used for to store data so that any time doctor can reach to report of a patient. This system is an improved version of existing systems and can be useful for patients on move or in intensive care unit.

Keywords: Alert system, Biomedical embedded system, Compression, Cloud computing, Data protection, Encryption, Health Monitoring System, IoMT, SMS.

I. INTRODUCTION

The monitoring of health parameters for person suffering from chronic disease or for patients under intensive care unit is very important in order to deal with medical emergencies. However, the timing of information sent to doctor or nursing staff plays an important role. Further, the security of data is a major concern in such type of system because it carries sensitive and crucial medical database. The transfer of information over an internet channels carrying crucial data pertaining to patient's health may be corrupted on account of multiple types of security threats. Therefore, a robust and secured system is essential with efficient and adequate encryption technique. Challenges for data protection includes: physical security, secure routing, data transparency, security of handling Iot data etc. Sensor based wearable electronics hardware should be preferred for ease of operation in patient's in move or work place or in intensive care unit. An alert mechanism based on prognostic approach is highly desirable and embedded software is developed in order to send alert message to medical authorities. The primary health parameters considered in proposed technique are ECG, body temperature, blood pressure, Galvanic skin response etc.

Internet of Things (IoT) enables real time data gain, data transfer, device connectivity , to control end user application. With the quick development of web innovation and communication technology, our every day schedules are progressively focused on virtual world [1].The term IoMT (Internet of Medical Things), basically used in the healthcare application which consists of connected devices that sense vital data of human physiological parameter in real time. IoT is most promising or better way in healthcare applications since it causes patients to deal with their very own illness and get help in most crisis case by means of portable devices [2]. It is foreseen that the demand of personal healthcare aid increasing rapidly. The provision of IoT in health monitoring system using cell phones is referred as M-HEALTH which consists of sensing of data, analyzing of data, storing of data through various sources like devices, biomedical sensors or medical specialty acquisition systems. But most of these system and applications are not intended to deal with the security and privacy attacks and it builds a ton of security and protection issues in the IoT systems, for example, access control, authentication etc.

In this paper, we have worked on biomedical embedded system and IoT technology. We have focused on real time analysis of physiological parameter of human using 3 sensors named as Body temperature, Galvanic Skin Response and 3 lead ECG sensor. We have also worked on Compression and Cryptography technique is used to make the network path secure and efficient. We have worked on alert system for our crucial patient data using SMS, Voice call, VoIP and Email. So that if one alert miss then we have 3-4 alternate option also. On the basis of result of compression of data, Compression ratio is calculated.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

II. EMBEDDED SECTION

In hardware architecture it includes Tiva CC3200 micro controller, DS18B20 temperature sensor, Galvanic skin response sensor, 3 lead ECG AD8232 sensor. CC3200 is a high performance ARM CORTEX M4 microcontroller [3] having built-in WiFi connectivity thus it is mainly developed for Internet of Things i.e IoT. Figure 1 describes the block diagram of CC3200 launchpad. This controller can work on a multiple power modes viz. Hibernate, sleep, deep sleep, low power deep sleep etc to reduce power consumption. 32-Channel Direct Memory Access (µDMA), 4-Channel 12-Bit Analog-to-Digital Converters, Advanced Low-Power Modes, Clock Source –40.0-MHz Crystal with Internal Oscillator, Wi-Fi and Internet Protocols in ROM etc are the specification of CC3200. Body temperature is easy to observe and it can depict various health issue. Here we have used Ds18b20, is a digital temperature sensor with one wired configuration and having a range of -55 to +125 °C with accuracy +/-0.5 °C.Galvanic Skin Response is used to measure skin conductivity with the help of resistance of a body. As the sweating increases, resistance decreases thus conductivity increases as per inverse property. Here we have used the model number 101020052/01 for our work. It is having two probes to measure signals. Strong emotion activate sympathetic nervous system, cause more sweating. Thus it is used in medical world to find out emotion of patient such as fear, frightened, sock etc with the help of sweating formula. ECG is termed as ElectroCardiacGram Sensor. Most widely used ECG monitor sensor module is based on AD8232 analog IC. It has a ability to measure the electrical activity of a heart. Here we are using this sensor to extract ECG features with 3 lead probes.

Fig. 2: DS18B20 Temperature Sensor and GSR sensor 101020052/01

Fig. 3: AD8232 with probes

Energia IDE is used to develop application code. It is an open source IDE (Integrated Development Environment) based on wiring and arduino framework. It is supported on Mac OS, Windows, Linux. This platform was started in 2012 by Texas Instrumentation. TI offers a CC32xx, CC13xx, MSP430 etc launchpad to use with Energia IDE. Here we have used this to create and upload code to CC3200 launchpad. Matlab stands for matrix laboratory. It is powerful software, allows plotting of function, implementation of algorithm, matrix manipulation, GUI etc. Here we have used this for analysis of our sensor's data and for connecting to Thingspeak cloud. Thingspeak is an internet of thing platform used to collect and store and data. It allows analysis and visualization of data in MATLAB. It has many

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 9, September 2019

features in which we have used it as storage of our data, MATLAB analysis and for the generation of alert system. Alert mechanism is interlinked with IFTTT which uses various services of IFTTT.

III. ALGORITHM SECTION

A. Huffman Compression:

As using the IoT technologies, we have limited storage capacity to store or save patient's data. Storage capacity is also increasing day by day but instead of this, we also make sure that large amount of subject's data can be store in minimum place. Compression of the data is best option for this. It can be lossy or lossless compression of data. In medical field, lossless compression technique should be considered because medical data is very sensitive, minor change can cause many problem. Huffman compression coding [4] is also known as Huffman encoding and having a quality of lossless compression. It is used for data compression. Huffman is worked on the prefix code and binary tree rules. Character is generally stored in 8 bit in the series of "0" and "1" and this is called fixed length encoding. In Huffman, here we have used variable length encoding depending upon the frequency of character i.e how many times that character appears. Thus we are storing the character on that length only which are needed for thus size of bits is reduced.

Performance parameter for compression:

1. **Compression Ratio:** It is a ratio between the compressed file and original size file.

$$\mathbf{CR}= \frac{size\ of\ a\ compressed\ file}{size\ of\ a\ original\ file} \qquad \mathbf{(1)}$$

B. RSA Cryptography:

The protection of captured health information from different sensors furthermore from unlawful access is critical. Accordingly, stringent approaches and specialized safety efforts ought to be presented to impart patient's information with approved users and organization. Challenges for data protection includes: physical security, secure routing, data transparency, security of handling Iot big data etc. One of effective and most used algorithm is RSA (Rivest Shamir Adleman). RSA is one of the best cryptographic algorithms [5] in present use that ensures secure communication over networks because of its long key generation manner.

Algorithm for RSA is as follows:

Key generation:

- Compute two prime number i.e p and q where p!=q.
- Calculate modulus n i.e n= p*q.
- Calculate phi φ where $\varphi = (p-1)(q-1)$
- Calculate exponent e where e!= factor of n and satisfy equation **1 < e <** φ (n)

Encryption and decryption algorithm

- Obtain public key (n, e) and represent the plaintext message as a positive integer m.
- Compute the cipher text c = m^e(mod n).
- Using private key (n, d) to compute m = cd(mod n).
- Extract the plaintext from the integer representative m.

C. Alert System:

Alert system is used when emergency occur in patient's health data. Here with the help of features of Thingspeak app i.e react and ThingsHTTP and IFTTT (If This Then That), we generate alert system in four ways are as follows:-

1. Alert Through SMS
2. Alert Through Voice Call
3. Alert Through VoIP(Voice over Internet Protocol)
4. Alert Through Email.
5. Alert Through Google Assistant

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 9, September 2019

IV. METHODOLOGY

To carry out the proposed plan of research work following methodological steps is adopted. Following steps to follow:

1. As per initial process of this work the embedded section is to be implementing. This will have three sensors: ECG, GSR and Temperature.
2. Interfacing the sensors with the controller CC3200 by the use of analog to digital converter. Application code is developed in Energia IDE.
3. The sensor ECG will be processed on a combined single channel and along with that the other two sensors Temperature and Galvanic Skin Response sensor will be calibrated according to desired units.
4. At last connect to the IFTTT with the help of Webhooks and other services like SMS, VoIP, Voice call, Email and Google Assistant. If any abnormalities occur it will send alert to respective person.

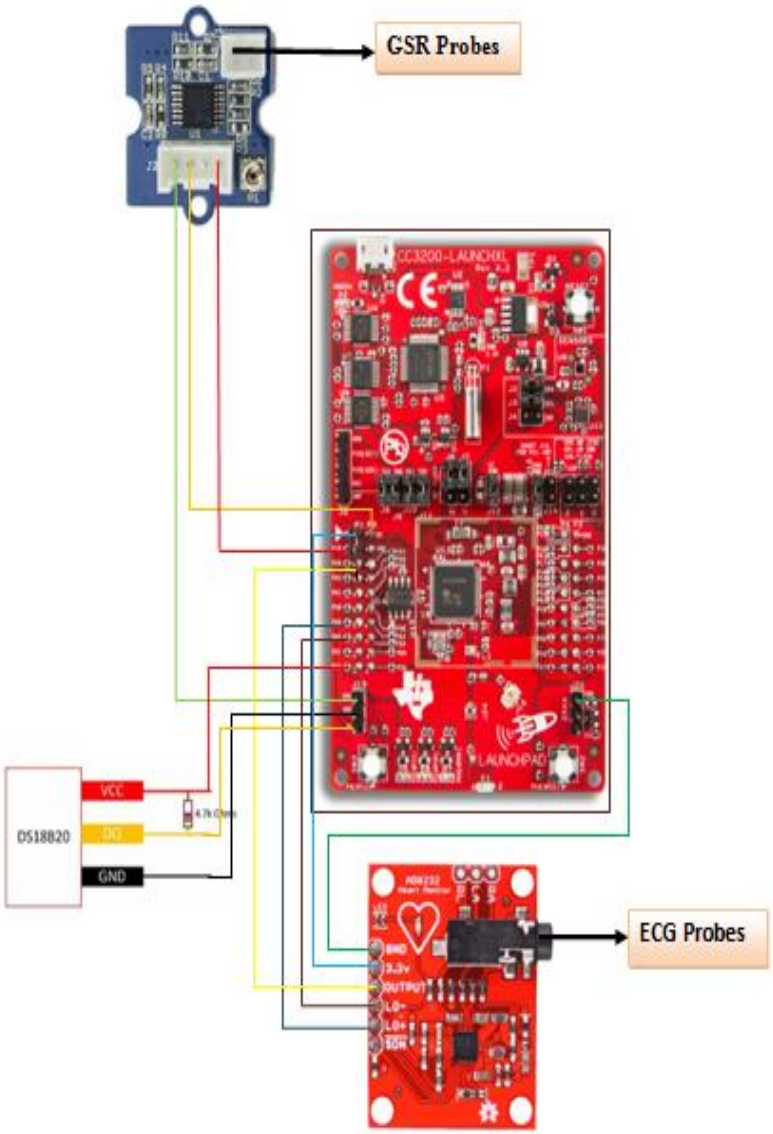

Fig. 4: Circuit Diagram

5. Now, transmit the data serially from the hardware module to the MATLAB interface by data transmission module.
6. Further process is to process the sensor's data signal in the MATLAB where an graphical user interface is created.
7. The GUI will have the monitoring system in which the received signal will be shown along with that the feature extraction approach for the PQRST features of the ECG signal of a defined signal packet will be calculated.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 9, September 2019

8. After the PQRST extraction, the threshold will be defined for all the 3 modules that are temperature, ECG values and the GSR. On behalf of the defined threshold the decision will be given on individual parameter.
9. After getting decision of the received signal further process is the signal security and IoT module.
10. The extracted feature PQRST of ECG signal, temperature and the GSR values will be compressed and secured using hybrid model of the Huffman compression and the RSA cryptography model.
11. Encrypted data will be sent over Cloud with the help of Wi-Fi.
12. We use ThingSpeak as our cloud for storage and analysis of our sensor data. Thingspeak targets for IoT applications where we can collect data and visualize our data in the form of graphs.
13. Alert system is generated with the use of react and ThingHTTP app of thingspeak.

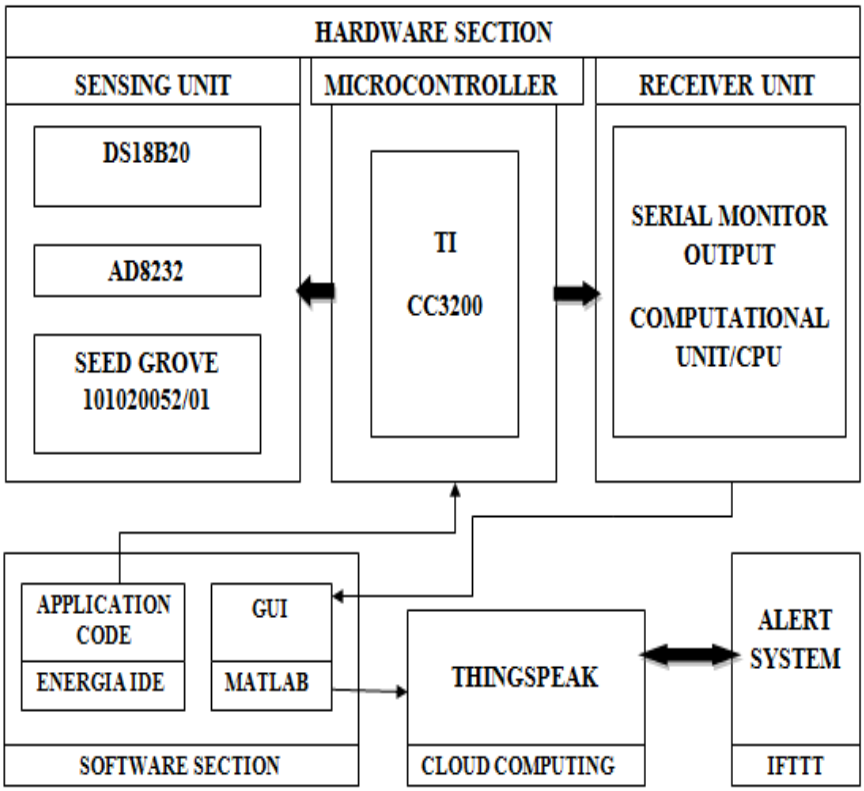

Fig. 5: System Model

The whole process can be repeated for the next packet of signal if desired. Circuit diagram and System model is figured out in fig. no. 4 and 5 respectively. The Sytem model consists of major three section i.e. Hardware section, Software section and Cloud section. Sensing unit and reciever unit are the part of hardware section in which microcontroller acts as an bridge between the two. Sensing unit consists Body temperature sensor, ECG sensor and Galvanic skin response sensor. Receiver unit as shown in fig. 5 consists of computational unit viz. output screen where results are shown via sensing unit. The software section consists of Model Application code, Graphical User Interface. The application code is flashed on CC3200 with the help of USB gateway module. Sensors get activated when power is supplied starts receiving data. The device is also connected to Wi-Fi and this complete arrangement helps to display data to GUI as well as real time data on Thingspeak cloud. Cloud section consists of thingspeak cloud which is interlinked with alert mechanism process.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 9, September 2019

A. Flow Chart

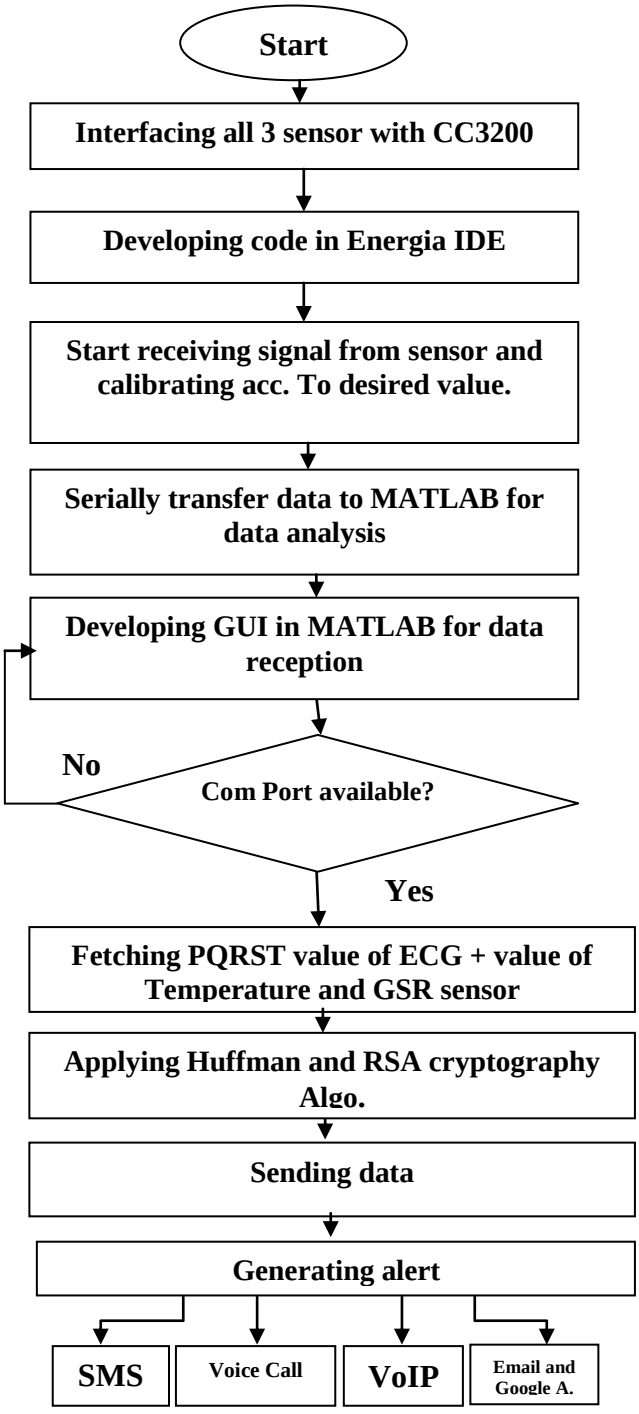

Fig. 6: Flow Chart

V. RESULT AND DISCUSSION

We have worked on 3 physiological sensor, Huffman Compression algorithm, RSA cryptography, Comparative analysis of Huffman with other technique, interfacing of cloud, generating alert through cloud and IFTTT. Results of all this are sequentially as follows:-

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

A. MATLAB real time GUI:

Output of all sensors can be seen on MATLAB GUI. In fig. 7, body temperature, GSR, ECG are shown in Graph 1, 2 and 3 respectively. Body temperature are drawn between No. of samples and ℃ . GSR readings are drawn between No. of samples and micro-Siemens (Conductivity) and ECG readings are drawn between No.of samples and mV. All the signals are stored for further analysis. The results showed that the system can also realize the acquisition, transmission and monitoring of a plurality of temperature, GSR and ECG signals. The captured data is processed to satisfy the medical requirement level. Body temperature is easy to observe and it can depict various health issue. Based on human age, the normal temperature of a body are as follows:

- Kids = 36.6°C to 37.2°C
- Adults = 36.1°C to 37.2°C.
- Above age 65 = 36.2°C

Excess of temperature causes fever (caused by virus) & deficiency of body temperature cause fits (Body shivering). There is a mechanism called hypothalamus in brain which regulates the temperature properly.

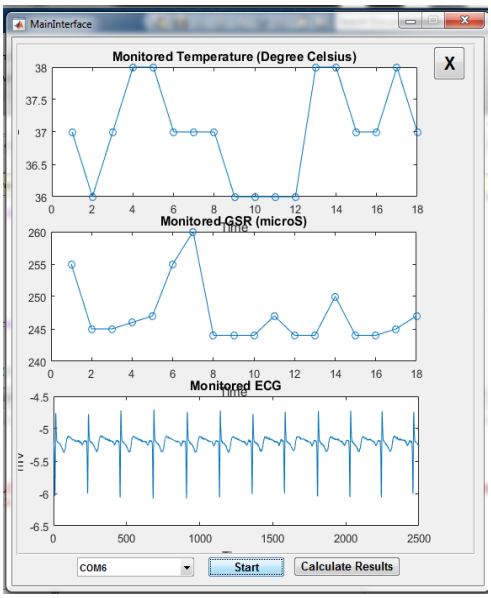

Figure 7: MATLAB GUI

B. Algorithm on MIT-BIH database of ECG for PQRST value Extraction:

Now Plotting of ECG from MITBIH Database of ECG and finding its PQRST value of ECG. The noise may disturb the readings of ECG signal. The noise may deviate the actual graph of ECG to an undesired level. So we take a one of the record from MITBIH database of ECG and apply the algorithm for the finding of PQRST value. These results are very important for the diagnosis of Cardiac patient.

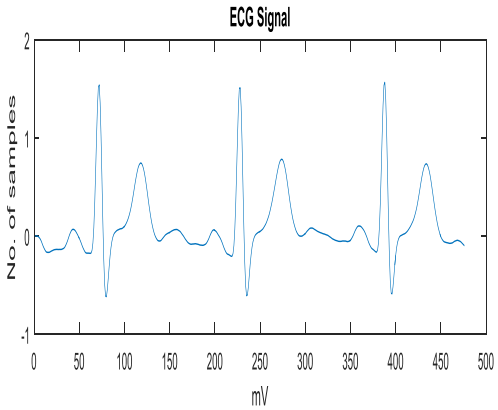

Fig. 8: Graphical Representation of MITBIH ECG Signa (Record No. 1)

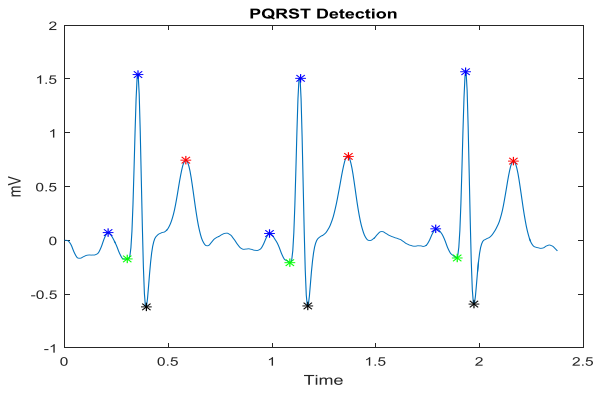

Fig. 9: PQRST value extraction

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

C. Real time encrypted and decrypted data on Thingspeak

The real time encrypted body temperature, GSR and ECG data on the cloud based on interfacing of sensors and cloud through Wi-Fi connectivity is shown in fig. 10. The monitored sensor data and its values are stored on the cloud with the date and time details. This monitoring is done using Thingspeak cloud with the help of Wi-Fi. We have applied data protection algorithm to secure network and patient sensitive data. We have got encrypted data on the cloud so no one can steal the data in the mid way and somehow if he may steal the data then he don't able to decrypt the data because algorithm is based on prime number and factorization of large number is very difficult to obtain. There is another algorithm to decrypt the data. Fig 11 shows original data after decryption (decompression also take place) in MATLAB analysis section in Thingspeak cloud.

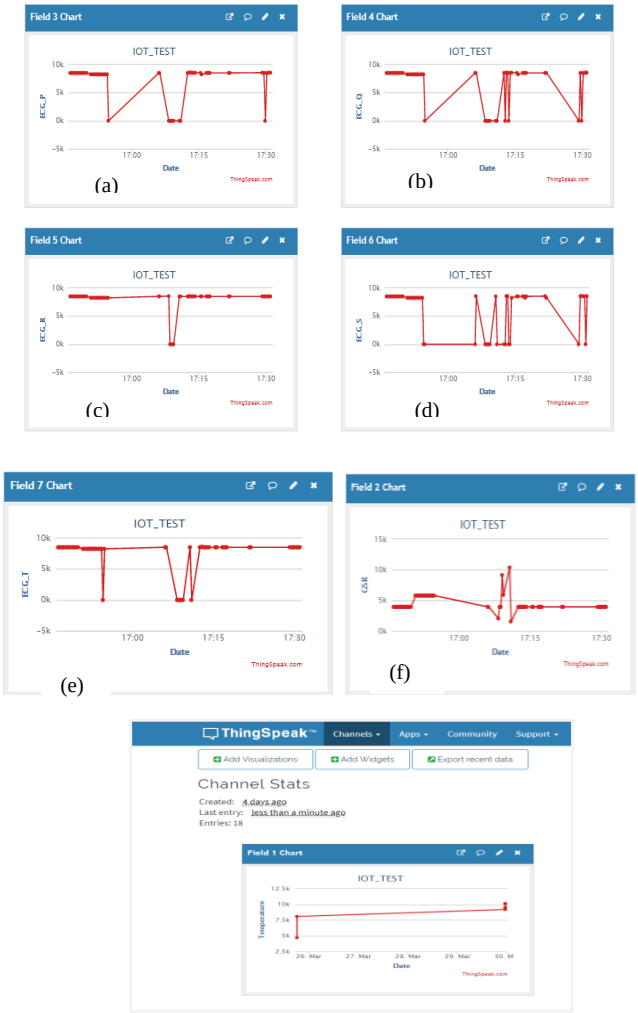

Fig. 10: (a),(b),(c),(d),(e) are PQRST encrypted value of ECG respectively. (f) is GSR and (g) is body temperature encrypted value.

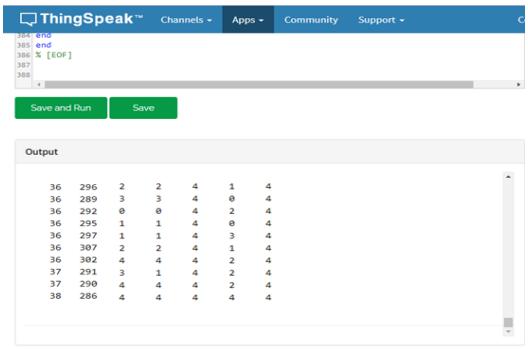

Fig. 11: Decrypted Data

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

D. Alert Generation:

As we discussed in previous section, we have created total number of 4-5 alert generation system with the use of Thingspeak cloud and IFTTT.

Sending data to doctor through cloud is very useful when patient don't able to go to hospital regularly. But Alert mechanism is also as important as cloud technology because if any abnormality is occurring it can alert doctor or relatives on that time without wasting any single second. So we have created 4-5 alert systems if any one fail then we have other alternatives also.SMS and voice call alert is main priority. Existing system suffers from lack of proper alert mechanism. So we have taken the benefit of IFTTT (If this then that) application in which we have used Webhooks technology (If This) and SMS, Gmail, Webhoopla, VoIP (Then That). Before activating the entire alert, first we have to make "React" and "ThingHTTP" condition for IFTTT activation.

ThingHTTP permits communiqué among gadgets, websites and net services without having to enforce the protocol at the device degree. React works with some specific apps to carry out actions whilst channel records meets a positive condition. React is connected to ThingHTTP. ThingHTTP can be connected to various services. A condition is defined on React section. Whenever this condition met, react calls ThingHTTP and URL specified in this section will called out and related service will be activated.

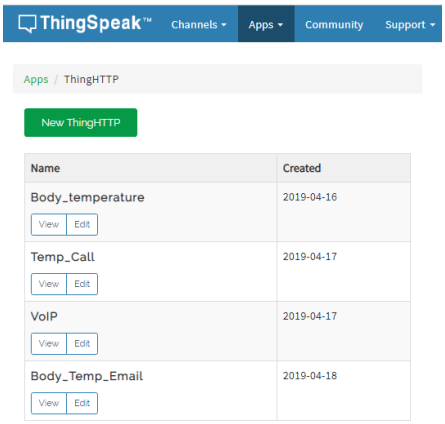

Fig. 12: Total number of four ThingHTTP Activation

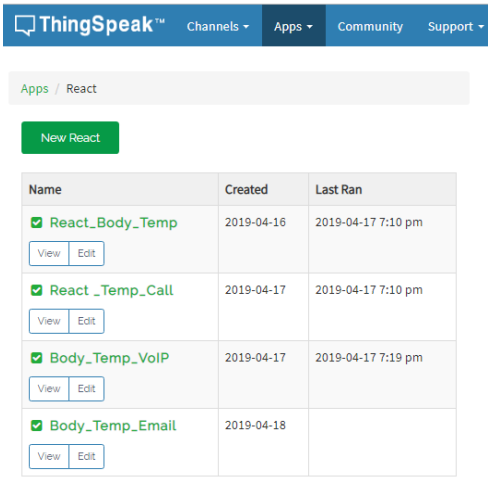

Fig. 13: Total number of four react activation

Using react and ThingHTTP app of Thingspeak Cloud, now we activates various services for alert mechanism through IFTTT. Fig. 14 shows the "If This" condition where we created events on Webhooks application. Fig. 15 shows the "Then That" condition where we activated services according to alert type.

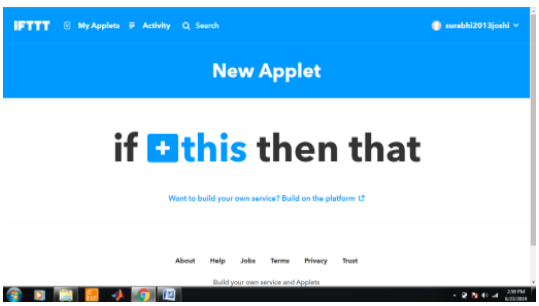

Fig. 14: IFTTT: If This condition

Fig. 15: IFTTT: Then That condition

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

1. Alert Through SMS Data:

Fig. 16: Screenshot of SMS alert

2. Alert through voice call and VoIP

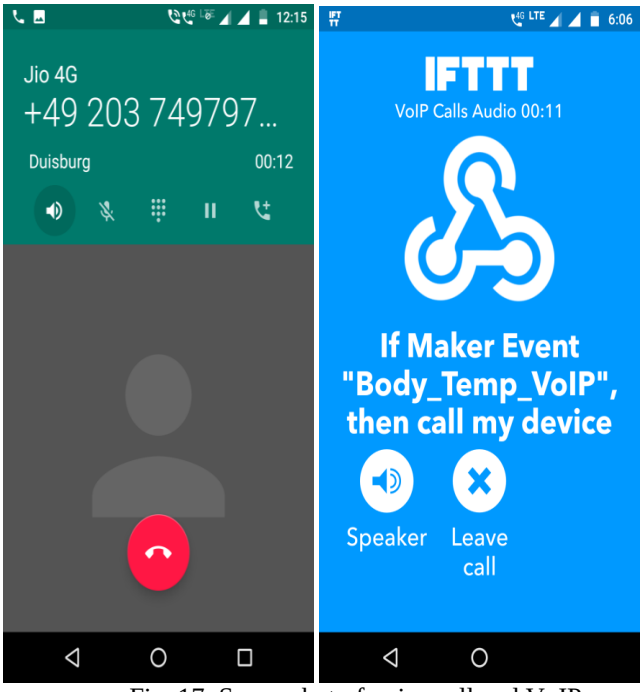

Fig. 17: Screenshot of voice call and VoIP

2. Alert through Email

Fig. 18: Screenshot of Email alert

3. Alert Through Google assistant

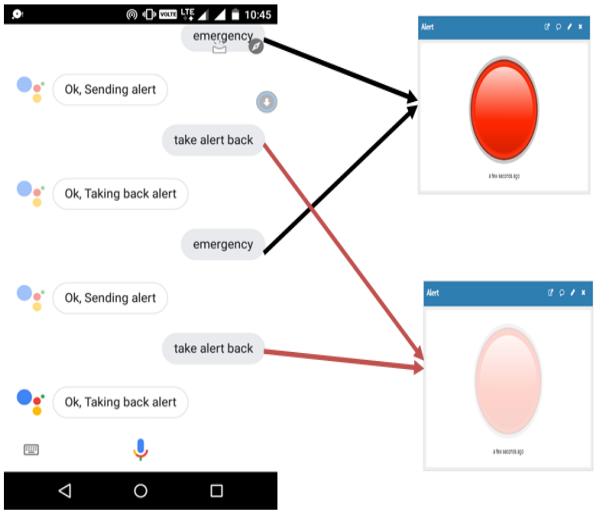

Fig. 19: Alert through Google assistant

In the case of google assistant alert, patient himself can send the alert to the doctor. Reason of emergency can be anything.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

E. Analysis of Data compression:

We took total no. of 10 samples of each sensor data to analyze performance parameter of Huffman technique. We have observed file size before compression is 270 and after compression is 141. We have to calculated compression ratio. It is a ratio between compressed file size and original size file [7].

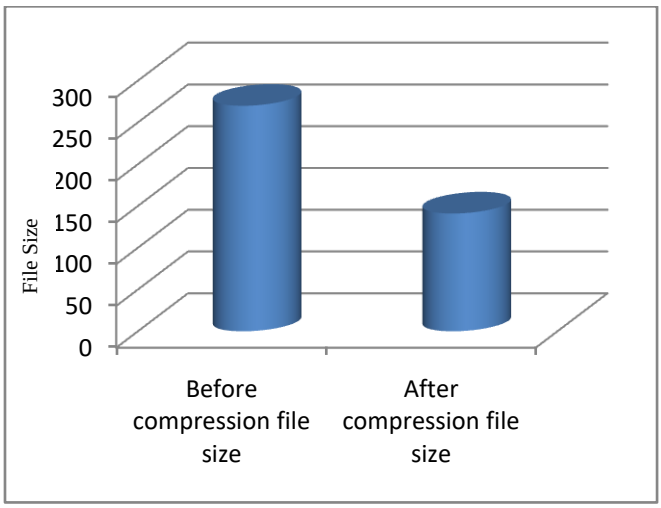

Fig. 20: Graphical representation of file size before and after compression

Calculations:

File size before applying compression algorithm = 270

File size after applying compression algorithm = 141

$$CR = 141/270$$

$$= 0.52$$

Therefore file size compression % = 0.52 * 100 = 52%

Space saving % = 100-52 = 48%

F. Real time hardware arrangement for proposed prototype work analysis:

Fig. 21 and 22 shows the real time arrangement of proposed research work.

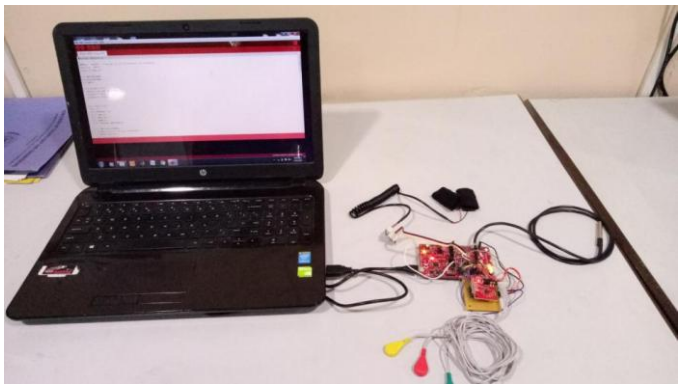

Fig. 21: Setup for flashing application code in microcontroller

DOI 10.17148/IJARCCE.2019.8920

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 9, September 2019

Fig. 22: Real time monitoring

VI. CONCLUSION

In this paper, we have worked on IoT and cloud computing. This includes all basic physiological parameter with secure data transfer in network path. When the emergency occurs, we have four alert systems; through them we can alert doctor, and relatives. If one fails then we have other alternatives to alert the doctor about the patient's condition. Following are the advantages of proposed prototype system are: Portability is given to a great extent. As this system size is quite small so it can be carried at various locations with ease. Doctors can see data remotely and analyze temperature, GSR, ECG signals of patients. This is the most important advantage of this system. The persons living in remote locations who have no access to a doctor can be helped through a greater extent through this system, as this system sends all the values and signals on the website and the doctors which are far away can get an accurate idea of condition of a person. This device is quite useful for real time monitoring. All signals are stored for further analysis.
Therefore, these multi-sensors sense the data from patients' bodies over the wireless network to the cloud environment and patients will have a high quality services by providing real-time data gathering, eliminating manual data collection, enabling the monitoring of huge numbers of patients and with the help of lossless data compression, storage capacity increased without the loss of original biomedical data and a security algorithm to ensure the safety of the patient's personal information. It is evident that designing such a system will help in early detection of abnormal conditions of cardiovascular diseases and prevention of its serious consequences.

REFERENCES

[1]. J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.
[2]. F. Andriopoulou, T. Dagiuklas, and T. Orphanoudakis, "*Integrating IoT and Fog Computing for Healthcare Service Delivery"*, Springer International Publishing, 2016.
[3]. http://www.ti.com/lit/ug/swru372b/swru372b.pdf
[4]. Shoba, D.Jasmine and Sivakumar, Dr.S. 2017. A Study on Data Compression Using Huffman Coding Algorithms. *International Journal of Computer Science Trends and Technology (IJCST)* 5: 58-63.
[5]. Nisha, Shireen and Farik, Mohammed "RSA Public Key Cryptography Algorithm – A Review". *International Journal Of Scientific & Technology Research,* Vol. 6, pp. 187-191, 2017.
[6]. J. Wissam, R. Latif, A.Toumanari, A.Elouardi, A. Hatim and O. El Bcharri " Enhancement and Compression of the Electrocardiogram Signal Using the Discrete Wavelet Transform" *IEEE*, pp. 1-6, *2017.*
[7]. Ibrahim, A., M., A. and Mustafa, M., E. 2015. Comparison between (RLE And Huffman) Algorithms for Lossless Data Compression. *International Journal Of Innovative Technology And Research* **3**: 1808 – 1812.