Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.9 Issue 1 Page No 116-129
Conference Proceedings-TMRI-2023

IoT-Based ECG Monitoring System for Health Care Applications

Sohit Agarwal[1] , Devashish Dasaya[2]
1Assitant Professor , Department of Computer Engineering & Information Technology
Suresh Gyan Vihar University , Jaipur , Rajasthan , India
2 M.Tech Scholar , Department of Computer Engineering & Information Technology
Suresh Gyan Vihar University , Jaipur , Rajasthan , India
sohit.agarwal@gmail.com
devashish.62071@mygyanvihar.com

Abstract—To better comprehend our environment, the new IoT architecture allows for the creation of tiny devices with sensing, processing, and communication capabilities. These devices may then be used to create sensors, embedded systems, and other "services." Using the power of the Internet of Things, we describe an electrocardiogram (ECG) system for the continuous monitoring of cardiovascular health through secured data transmission (IoT). Tiny sensors, embedded devices, and other "things" with sensing, processing, and communication capabilities are now feasible thanks to the current paradigm of the Internet of Things. The Internet of Things (IoT) and other connected medical technologies have allowed for remote monitoring of patients' vital signs in real time. In the event of a corona-virus pandemic, there would be a dramatic increase in the number of persons seeking medical assistance, making regular patient monitoring essential. Concerns concerning the privacy of IoT data remain significant, as evidenced by the transfer of patients' huge amounts of personal health information made by those who do not intend to share their own medical information. Because of recent developments in IoT technology, "smart objects" (things) can now have real-time Internet communication. Sensors, a consolidated processing unit, and a database platform are all useful tools for IoT healthcare applications. This paper includes an Internet of Things (IoT)-enhanced electrocardiogram (ECG) monitoring system that can either send data to a server in real time or create an ECG graph that can be seen on a Smartphone with an accompanying app. The patient's room current temperature, humidity, and his heart rate are all shown in the app. As part of this effort, we present a lightweight method for rapidly updating data at a distance.

Keywords—*Internet of Things (IoT), Health Care System, ECG monitoring system, IoT Based ECG*

I. Introduction

The old proverb "Health is Wealth" remains true now as much as it ever did. Humans have the technological prowess to launch rockets to distant planets, but they also face a number of

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

health problems that prevent them from living as long as they might otherwise. As medical technology has advanced, doctors have been able to effectively treat more symptoms. The majority of people, however, can no longer afford health regulation. It would appear that the average person cannot pay the sky-high costs associated with receiving medical treatment. Now, thanks to technological progress, people who previously could not afford cutting-edge medical treatments are able to do so. In major urban centres, those who can afford it or are covered by insurance can get quick and professional medical care. Can we do something to assist those who reside in outlying locations and, as a result, lack access to reasonably priced medical care? Putting in place technologically fueled mechanisms is the key to solving this issue. Unless it can aid the poor, technology is of little use. Scholars and academics interested in the current situation of the computer industry might draw significant inspiration from this idea. Individuals from rural areas are the focus of this article (remote places). The implementation of remote health monitoring is one practical application of this concept. This was formerly unthinkable, but that has changed. Therefore, system-wide remote monitoring is possible with the help of distributed computing technologies such as the cloud and the Internet of Things (IoT). With IoT, we can seamlessly combine our online and offline lives. The physical and digital make-ups of humans and mobile devices are drastically different. The Internet of Things allows for the smooth combination of these two infrastructures. The "Internet of Things" (IoT) refers to the worldwide system of interconnected electronic devices and infrastructures, including cellular networks, the World Wide Web, and a wide range of wearables. Cloud computing, on the other hand, makes use of a distributed network of remote computers to store and process data on-demand in a way that is easy to access, scalable, and resilient to failure. As a field dedicated to the remote monitoring of patients' health, remote monitoring relies heavily on cloud computing and the Internet of Things. Distributed programming frameworks in cloud computing make Hadoop and other data storage and management frameworks available. Based on our findings, the existing status of IoT and cloud integration in healthcare institutions is not especially helpful. A complete framework for remote health monitoring is required in cases where a primary health care centre (PHC) is accessible to a rural community. In this dissertation, we present a system for remote patient monitoring in primary care that makes use of a smart bed, the internet of things (IoT), and cloud computing. The patient's whole medical record, including vital signs, is uploaded to the cloud, where it may be accessed by the doctor and other caregivers via a mobile app after being analysed by analytics software. The next section will provide a high-level overview of the study's findings, while subsequent sections will provide more nuanced analyses.

II. Literature Review

MamoonaHumayunet. All (2020) A standardised protocol for sharing medical records in E-health settings across the Internet of Things. Many IoT devices are used in the healthcare industry for the purpose of transmitting and collecting data in real time. Unfortunately, they lack security and require specialised, lightweight security measures to be put in place due to constrained resources. In response to these issues, we devised a method that reduces the maximum possible data transmission distance while simultaneously increasing the energy necessary to send the data by using several groups of nodes and engaging in multiple rounds of node registration and key authentication. All the nodes in a cluster can use the same authentication scheme if they all register the same shared key. In this paper, we argue that ECC's level of security is insufficient for use in E-health applications and propose an alternate method. We compared our findings to those of other studies using four distinct methods of analysis (without GN, with one GN, and with two GN). Scientific rigour and a wealth of simulation data underpin our work. The results show that the

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

method of breaking up networks into many smaller networks made up of nodes can significantly enhance energy efficiency. It provides roughly 10% greater performance than the existing group node. [1]

S. Sheeba Raniet. All (2019) Following extensive investigation into the difficulties of data collection in IoT-based healthcare apps, a brand new healthcare data secure approach has been developed to protect the confidentiality of individual patients' medical histories. The data collected by the network's sensors was encrypted using a SIMON block cypher method, allowing for safer transmissions between IoT devices. The authors implemented a share generation strategy to ensure their patients' confidentiality. Using the best possible input, the CRT method creates an identical ciphertext for each message (TLBO algorithm). In light of the findings, it appears that the proposed method has a good shot at improving the privacy of cloud data and attracting more users to the cloud. What's more, it can be run in a fraction of the time required by other cypher algorithms and the model used to generate shares in the system. The best CRT provides the highest feasible level of security (between 65 and 95 percent) for a variety of blocks, significantly outperforming other methods. We hope to apply our novel data encryption techniques and hybrid optimization methodology to the design of comprehensive implementations of the algorithms that meet a variety of requirements in future studies. Many different scenarios involving attacks or threats to cloud data can benefit from this. [2]

Ashutosh Sharmaet. All (2019) To protect the privacy of all interactions between patients and healthcare professionals and to meet all user needs in a timely manner, this article introduces a healthcare CPS that is secure, SLA-compliant, and energy-efficient. Recognizing the residual energy information at the node prior to transmission enables a safe and efficient communication mechanism by recognising the required service time and adapting in AODV process methods. The proposed methodology outperforms the current state of the art in simulated environments where malicious nodes are present and where they are not. Using these metrics for SLA and energy analysis elucidates a pattern that characterises a vital component of effective communication path selection. In the absence of such dangers, however, quantitative and qualitative indicators show no deviation from their norms. Unfortunately, efficiency sometimes comes at the expense of security. [3]

Sarada Prasad Gochhayatet. All (2019) In this paper, we lay out the procedures required to implement key management across a heterogeneous network of devices using a wide range of IoT applications. For this reason, it is essential that IoT apps have solid data management skills, such as the ability to gather, store, and transport data securely. Using the benefits of mobile agents, we hope to assist local administration in protecting nodes (IoT application nodes) and ensuring that data can continue to flow from its source to its destination regardless of the user's location or the number of subnetworks they traverse. The simulations have shown that our approach is effective, therefore we should be able to complete our objectives. [4]

Mohamed Elhosenet. All (2018) The medical IoT introduces a new paradigm with the secure exchange of diagnostic information about patients via colour and grayscale photos. Using AES and RSA for encryption and 2D-DWT-1L or 2D-DWT-2L for steganography, the proposed model was effective. There were both colour and black and white illustrations, and the letter sizes varied throughout the test. It was evaluated using six statistical indicators of performance (PSNR, MSE, BER, SSIM, SC, and correlation). The proposed model outperforms state-of-the-art methods in concealing patients' personal information while transmitting a cover image with high imperceptibility, capacity, and low deterioration of the received stego-image. [5]

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

SohailSaifet. All (2018) The cloud made it possible to create and deploy a system for safe wireless body area network (WBAN) communication within the medical industry. Any network that relies on the authentication of patients' and doctors' biosignals will be difficult for unauthorised users to access. Each individual sends out a biosignal that is entirely their own. Protection against hacking is one area where AES encryption technology excels, making wireless networks much more secure. Data is more protected, authenticated, trustworthy, up-to-date, and accessible when these methods are merged, all owing to the cloud server. [6]

Hai Taoet. All (2018) Authors created a new approach to data collection that we call "Secure Data" to put customers' minds at ease regarding the security of their information when using IoT-based healthcare apps. In this paper, we present the KATAN secret cypher method, develop an FPGA implementation of it, and optimise it for use in practise. The KATAN encryption relies on private cypher exchange and repair to maintain its security. Analysis shows that the Secure Data system saves money in every category: processing, energy, and security. Implementing the algorithms and evaluating their success in averting attacks and threats will be the following steps. [7]

Munish Bhatiaet. All (2017) To that end, this essay delves deeply into one potential future application of the Internet of Things: health monitoring during exercise. By including many different aspects of health, the suggested model may provide a fast evaluation of the vulnerability of a given health condition to damage. The model's multi-tiered architecture was developed to simultaneously execute a set of predefined procedures for optimal performance. First, we use IoT to monitor the health of various exercise components. With these variables stored securely in the cloud, we can now conduct in-depth analyses. The BBN classifier model ranks attributes using a vulnerability scoring system. Temporal mining allows for real-time data segmentation, which prepares the way for the derivation of probabilistic metrics like PSoV for use in quality assessment. We utilise a median-weighted evaluation of the data values to estimate the potential danger to health. This data can be used to train an artificial neural network (ANN) prediction model that can reliably predict PSoV levels. An individual needs to first observe, then acquire knowledge, and only then make a prediction. Over the course of two weeks, five people have been monitored while they engage in a variety of physical activities to gauge the device's efficacy. Statistical analyses have shown that the proposed method has a high rate of efficiency and accuracy, suggesting it will be useful in the medical field. [8]

Mohamed Elhosenyet. All (2017) Security is of vital importance in a WSN because of its limited resources and potentially hostile environments. Energy consumption in networks can be decreased using the proposed cluster-based paradigm, extending their useful lifespans. There has been a lot of discussion and debate on the topic of how best to protect data clusters in wireless sensor networks. Most routing protocols, when implemented with a rigid clustering structure, expose networks to numerous risks. WSNs have seen the development of a number of secure clustered routing techniques (WSNs). Then, an efficient solution for protecting a dynamic cluster network was presented. It also exemplifies a four-step process for creating a safe clustering mechanism for WSNs. Implementing a secure cluster requires selecting a trustworthy cluster leader, constructing a trustworthy cluster, gathering trustworthy data from trustworthy cluster nodes, and securely routing trustworthy data to a trustworthy base station. Only when all of our requirements, which include the four stages of safe clustering, have been met can we say that a method for establishing secure clustering is complete. [9]

Haiping Huanget. All (2017) This study proposes a new paradigm for e-/m-healthcare

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

systems, which the authors call "HES," to overcome these problems. HES features can be broken down into three broad groups: We first address the problem of ad hoc communications between users' mobile terminals and embedded (wearable) medical devices (nodes) by employing low-cost and easily deployed wireless sensor networks as the relay infrastructure for GSRM-based secure transmission of medical data from WBANs to WPANs; second, we employ privacy-preserving strategies like HEBM to achieve satisfactory performance. With the aid of an expert system, users' loved ones can have access to their medical information whenever they need them, and the presence of a doctor or administrator at routine checkups can be substantially minimised. HES stands to benefit substantially from the trend toward using data to guide healthcare decisions. For instance, HES's expert system has low diagnostic accuracy and it cannot yet monitor or analyse rare diseases. [10]

Felix Bushing et. All (2015) Information pertaining to one's health and degree of physical activity are examples of particularly delicate information. It has been argued that such a complicated method is unnecessary for such data. In any case, if we can attain unrivalled high security at a reasonable price, we think it's a good plan of action. Secure transmission of sensitive information via wireless networks is made possible with the use of one-time passwords (OTPs). The approach proposed, constructed, and tested here allows for persistent and secure monitoring of sensitive data by periodically recharging WBAN node OTPs. Modern computers can store a huge number of regenerated OTPs and guarantee data transport for lengthy periods of time, albeit this does depend on the data rate being generated. DTN promises that its data stream will always be reliable and error-free. When you connect an external storage device to your computer, it won't affect the amount of RAM you need or the number of read/write cycles your machine requires. The maximum allowed size of data transfers via the transport protocol has also not altered. Data supplied securely, openly, without tampering, efficiently, and dependably may all be accomplished with OTPs. [11]

Soufiene Ben Othmanet. All (2014) New medical wireless sensor networks have made it possible to remotely monitor patients. These authors looked into the security issues that arise during the development of wireless sensor networks, which add a new dimension to healthcare applications. The problem of wirelessly conveying sensor data is the focus of our work in the area of medical wireless networks. Testing has proven that the author's method is robust enough for general use. We hope to have began enrolling hospitalised patients in our study as of the time of this writing. The operating room and intensive care units are located here. The authors are planning a new workshop to test the stated prototype. Participants will act as patients for the length of the programme. There needs to be tweaks to the protocol. Extra work needs to be spent into formalising and verifying the security features. [12]

Parthaet. All (2014) The Internet of Things is a relatively new economic game-changer with the potential to significantly impact industries as varied as logistics, environmental monitoring, retail, and agriculture. We have a moral obligation to assist with the care of the sick and aged, and Internet of Things devices are making this task easier and more accessible (IoT). The purpose of creating PAMIoT was to allow for the monitoring of people's physical activity to extend beyond clinical environments and into people's daily lives. Maintaining a healthy human population is challenging, but this method can help. PAMIoT's hardware platform and maintenance costs are kept cheap and sustainable by using low-energy communication technologies. PAMIoT excels in less constrained settings because to its straightforward design. However, PAMIoT is not useful for monitoring critical conditions. The security risks associated

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

with using PAMIoT to a network of devices need more study. [13]

Pardeep Kumar et. All (2012) There is a heightened need for secrecy and trustworthiness in healthcare sensor networks. The success of any wireless application depends on a well-planned security infrastructure. The challenges we've faced creating a healthcare monitoring system based on medical sensors point to the importance of users' confidence in a technology's safety. If used improperly, it could be fatal to the patient. There are many challenges associated with implementing wireless medical sensor networks; we believe that this research will encourage future scholars to create better security protocols for such systems. [14]

III.Methodology

3.1 Proposed Model Communication Method

Figure: 3.1 Proposed Model Communication Method

Our proposed method completely mechanises this procedure. The ESP8266 microcontroller in the node MCU gathers information from various sensors, such as those used to track environmental conditions and human health. The DHT11 Sensor is a combined temperature and humidity reader. Use of a capacitive humidity sensor and a thermistor-based temperature sensor allow for precise environmental monitoring. It has three pins labelled "Data (I/O) - Digital serial Data Output," "Ground," and "Power." **Microcontroller:** The ESP8266 is utilised as the microcontroller within the node. An environment for developing IoT apps in the open-source, free-to-use Lua language. The ESP8266 is used as the Wi-Fi SOC, and it already has the necessary firmware installed to connect to the Thing Speak cloud and make the data gleaned from it available via mobile app. The "Power" pins kick off a series of many designs. The Micro-USB Node MCU features a USB port, a 3.3V power input pin, a ground pin, and an external power input pin labelled Vin. Furthermore, this button can be used to reboot the microcontroller (control pins EN, RST). Finally, Analog pin A0 is used by the pulse sensor to measure Analog voltage.

A microcontroller constantly gathers data from sensors, which it subsequently sends to the cloud and other mobile apps. The collected information will be uploaded to the Thing Speak cloud through the Node MCU microcontroller, which features built-in WIFI. The information is accessible via a Mobile App for those with Android and iOS smartphones.

3.2 Connection Block Diagram

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

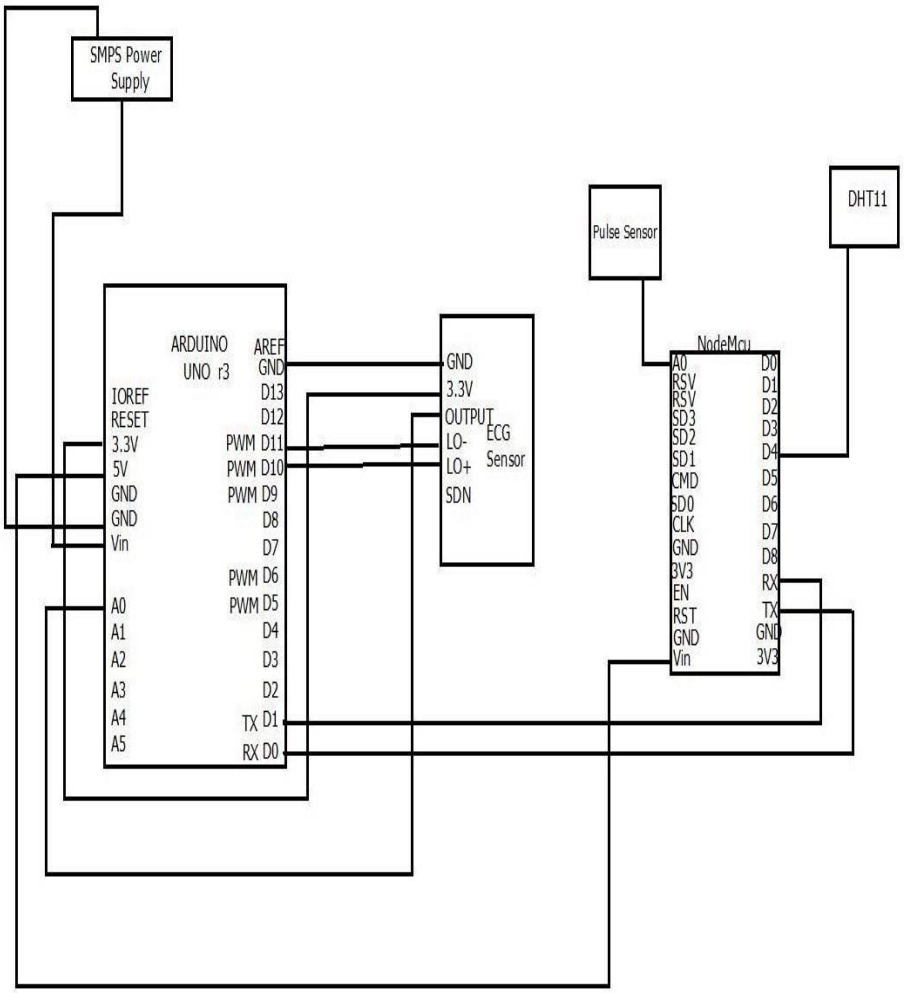

Figure: 3.2 Main Connection Diagram

The figure above is a connection schematic for the planned work, including the sensors that will be used and their respective connections. While the electrocardiogram (ECG) sensor is connected to the Arduino, the temperature and humidity sensor (a DHT11) and the pulse rate sensor (an HC-SR04) are both connected to the nodemcu. Data from the dht11 was connected to the nodemcu board's analogue input, and the pulse rate sensor's output was connected to GPIO port 4. The Arduino ECG shield allows for the simple connection of an electrocardiogram (ECG) sensor. With the Lo- and Lo+ pins of the ECG sensor attached to the analogue input pin on the Arduino board, the system can read heart rhythms. Disconnecting the IN electrode triggers dc leads off detection mode and causes the LO to rise; reconnecting the IN electrode brings about the opposite effect. In the initial step of a comparator, the logic one (LO+) is a significant output. When the +IN electrode is disconnected (high) or connected (low), the dc leads off detecting mode is engaged (low). All of the boards and sensors call for a 5V regulated supply, thus we opted for a 5V SMPS (Switch Mode Power Supply).

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

3.3 ECG Algorithm Flow Chart

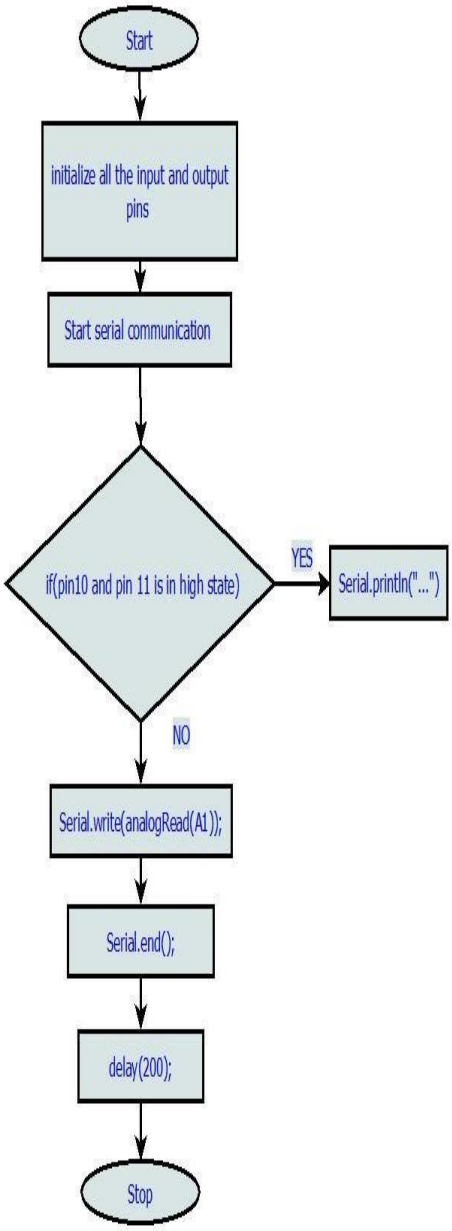

Figure: 3.3 ECG Code Flow Chart

The above diagram depicts the ECG algorithm for processed ECG data; this programme is uploaded into the Arduino board since our ECG sensor is directly connected to the Arduino board; after capture readings, the data is processed in the Arduino board and then transferred to the nodemcu via serial communication so that it can be updated on the thingspeak web server. Pins 10 and 11 are used as inputs, so they are set to input mode at the outset of the algorithm. From there, serial communication is initiated at a baud rate of

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

9600; if pins 10 and 11 are found to be high, a message is printed to the serial monitor; otherwise, the received reading is transferred to the nodemcu using serial communication.

3.4 NodeMcuCode Flow Chart

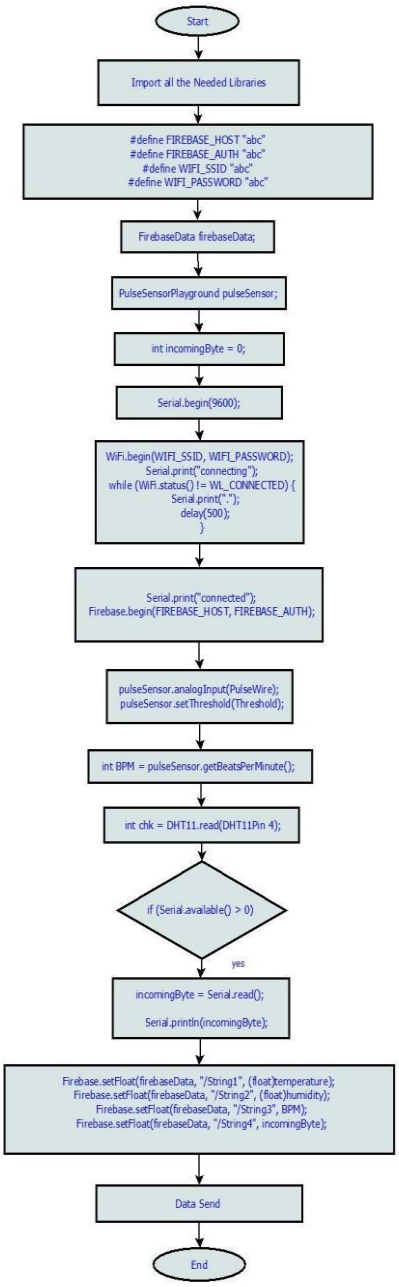

Figure: 3.4 NodeMcu (Esp8266) Code Flow Chart

Here we can see how the nodemcu application collects sensor data, processes it, and finally uploads the results to the appropriate locations on the firebase server and the thingspeak web server in the accompanying flowchart.

First, the algorithm is run; next, the firebase, wifi, thingspeak, dht11, and pulse sensor libraries are initialized; and last, the firebase host, key, and URL are displayed. At last, the nodemcu's saved wifi SSID and password are shown for use in establishing a secure connection between the router and the device. After initializing firebase data, the following step is to set up the API key, number, and URL for a Thingspeak channel. Once the timing has begun, we will begin taking pulse readings through the pulse wire connected to analogue pin 0 with the maximum ignore value set to 550. One the byte has been received, it is treated as a 0. Data read from the serial port is saved in this Arduino variable. After entering the required information, the nodemcuwifi will begin scanning for networks that match the SSID and password. The cycle starts over every 500 ms and continues until the nodemcu is offline. The serial print port on the nodemcu must be connected to the device's local IP address over WiFi so that firebase and thigspeak may communicate with each other. In this case, Nodemcu's analogue pin 0 will be used to read the information from the pulses. The analysis of heart rate requires the determination of beats per minute. The nodemcu's digital pin 4 is where the output from the dht11 sensor may be read for information on the current temperature and humidity levels. Then, we'll test if there's any new information by looking at the serial RX pin on the nodemcu. If so, then the nodemcu has received data from the arduino through its TX pin. Data is written to the incoming byte variable if all conditions are met. After this is complete, the nodemcu sends the processed data as a byte variable to the firebase server, which then converts the data into strings S1 through S4 according to the data type (temperature, humidity, pulse data, and electrocardiogram). The ECG data uploaded to the thingspeak server can be used to create a

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

graph. Finally, we'll check that the graph was updated correctly by using the condition (x==1000). Serial print channel update is complete when this algorithm returns, and the loop continues until power is restored to the nodemcu.

3.5 Firebase to Android Application Communication Flow Chart

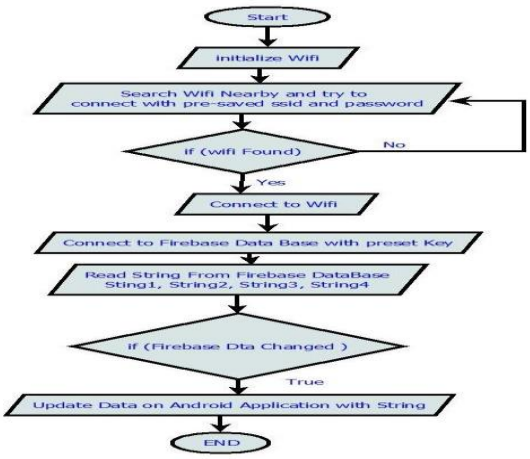

Figure: 3.5 Firebase to Device Communication Flow Chart

Firebase provides everything you need to build and manage a website, including hosting, authentication, storage, and more. This project makes use of a hosting service and a real-time database. Instead of managing a server and coordinating deployment and networking, you can use Firebase's hosting service. It's free (but severely limited), straightforward, and convenient. Google's Firebase is a platform for making mobile and web applications. As can be seen in the accompanying picture, once the first line of code is performed, all input/output devices are activated and a WiFi connection is made. The figure also shows the remaining processes that take place during a conversation between an Android app and the Firebase server. When online, the system connects to Firebase and reads sensor readings from there. Whenever you make a modification to a string in Firebase, like when new information is added, the corresponding strings in your mobile app will also be updated.

IV. Results

4.1 Serial Results

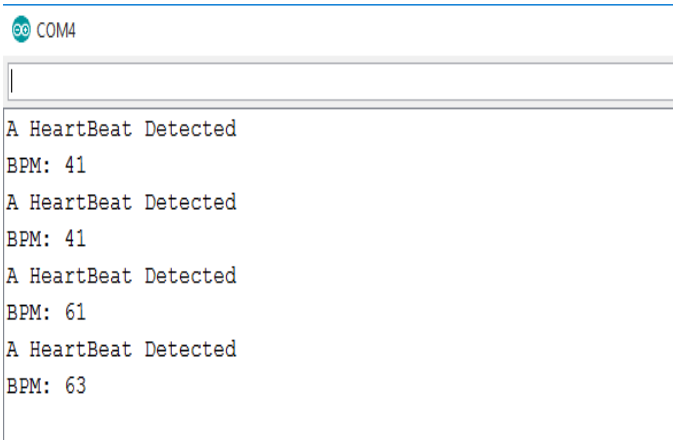

Figure:4.1 Heartbeat Detection

In this above figure we can see pulse sensor data read by nodemcu and print on serial monitor of the arduino IDE.

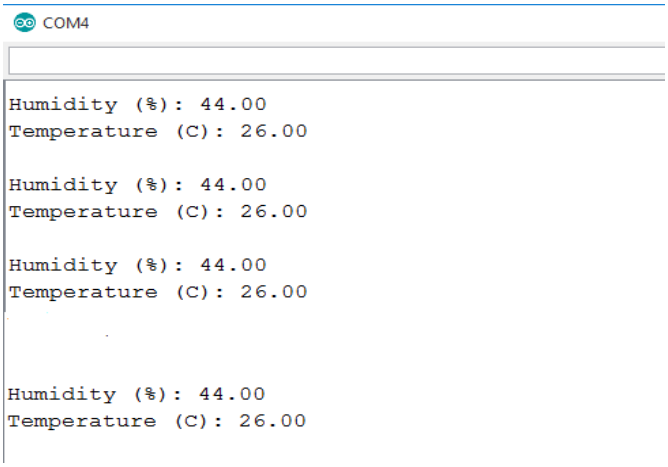

Figure: 4.2 Temperature and Humidity Detection

In this above figure we can see temperature and Humidity data sensor data read by nodemcu and print on serial monitor of the arduino IDE.

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

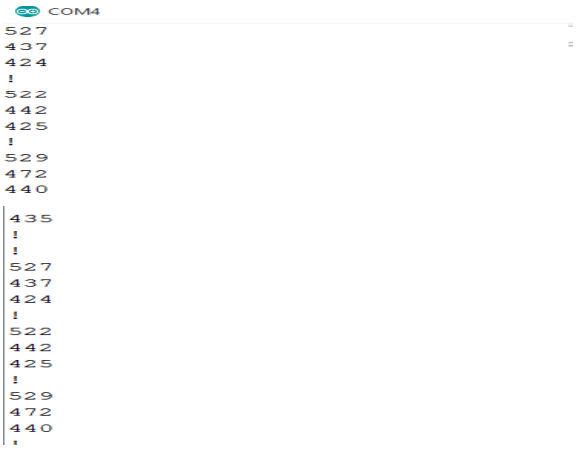

Figure: 4.3 ECG Readings

In this above figure we can see ECG sensor data read by nodemcu and print on serial monitor of the arduino IDE.

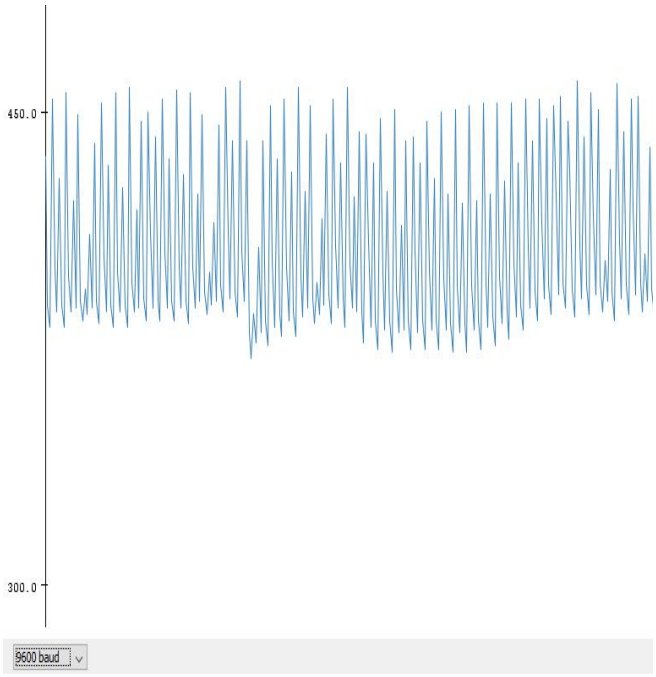

Figure: 4.4 ECG Graph

In this above figure we can see ECG Graph on serial monitor of the arduino IDE.

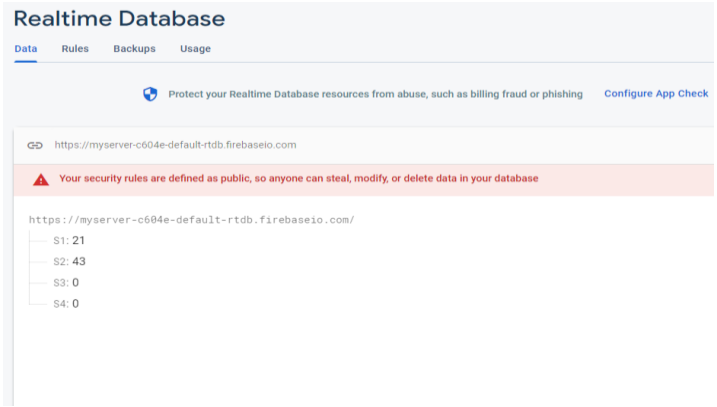

Figure: 4.5 Real-time FireBaseDataBase

In the above figure we can see our real time firebase database for store data in S1,S2,S3,S4 string in real time and this data is used for communication between nodemcu and android application.

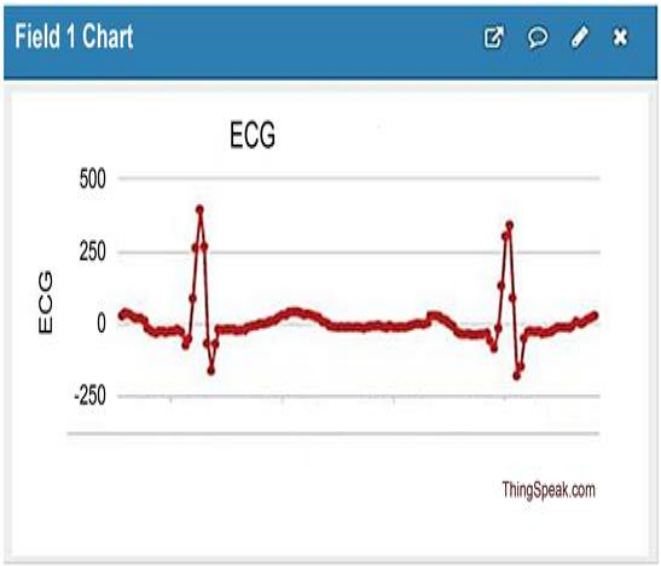

Figure: 4.6 ECG Graph On Thing Speak Server

In the above figure we can see graph plot of ECG data on the thingspeak website.

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

4.2 Android Application Results

Figure: 4.7 Temperature and Humidity on Android Application

In the above figure we can see temperature and humidity on the our developed android application, this data is captured from our firebase database.

Figure: 4.8 Beats Per Minute On android Application

In the above figure we can see heat beat reading in real time in the form of beats per minute on the our developed android application, this data is captured from our firebase database.

Figure: 4.9 ECG Graph On Android Application

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

In the above figure we can see ECG graph in real time on the our developed android application, this data is captured from our thingspeak web server.

V. CONCLUSION

Given the recent worldwide population explosion and the increasing need for health insurance, the rising expense of providing basic medical treatment has emerged as one of the most serious challenges for both individuals and governments. However, a new report from the World Health Organization emphasises the gravity of problems caused by an ageing population. More frequent checks on the health of the elderly are needed, as they will serve as a more public test of current medical structures. Careful planning is required for the diagnosis of human diseases to be quick, accurate, and inexpensive. Detection, processing, and communication capabilities may now be built into the blueprint for sensors, embedded devices, and other "things" thanks to the expanding Internet of Things (IoT) infrastructure. An Internet of Things (IoT)-enabled electrocardiogram (ECG) monitoring system has been created so that a patient's heart health can be monitored continuously. This study introduces an innovative approach to ECG quality assessment using the Internet of Things, which may one day be used to monitor cardiac health. Sensors, a centralized processing unit, and a database platform are all useful tools for Internet of Things healthcare applications. The electrocardiogram (ECG) monitoring system described in this thesis takes advantage of IoT technology to either upload real-time data to a server or generate an ECG graph viewable on a smartphone. The android application developed in this proposed work displays the patient's current temperature, humidity, and heart rate also ECG graph plot in real time. We provide a lightweight way for remotely updating data quickly with long distance.

VI. Future scope

Other non-invasive health markers include blood pressure, glucose levels, and respiration rate. Machine learning technology may prove to be an essential part of any healthcare monitoring system due to its potential to increase the rapidity and precision of medical diagnostics. In addition, other tactics can be integrated into this initiative in the event of an emergency, such as when the patient's body produces an irregular signal. Firstly, a SIM800L GSM Module will be integrated into the system, allowing for phone calls and SMS messaging to be made and received from the project to locations such as hospitals, homes, and emergency medical care hubs. NodeMCU has the ability to send urgent emails to specific addresses automatically. Second, in the case of a VF, a DC defibrillator can be worn by the patient and attached to the body in order to automatically give DC shocks (Ventricular Fibrillation). Finally, if the SPO2% falls below 90%, an automatic ventilation system can be introduced to the system to replenish oxygen levels.

VII. REFERENCES

[1] MamoonaHumayun, NZ Jhanjhi, Malak Z Alamri “IoT-based Secure and Energy Efficient scheme for E-health applications” Science and Technology2020.

[2] S. Sheeba Rani &Jafar A. Alzubi& S. K. Lakshmanaprabu& Deepak Gupta &RamachandranManikandan “Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers”Springer2019.

[3] Ashutosh Sharma, GeetanjaliRathee, Rajiv Kumar, HemrajSaini, VijayakumarVaradarajan, Yunyoung Nam and Naveen Chilamkurti “A Secure, Energy- and SLA-Efficient (SESE) E-Healthcare Framework for Quickest Data Transmission Using Cyber-Physical System”MDPI2019.

[4] Sarada Prasad Gochhayat, ChhaganLal, Lokesh Sharma, D. P. Sharma, Deepak Gupta,

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur

Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com

Jose Antonio Marmolejo Saucedo, UtkuKose "Reliable and secure data transfer in IoT networks"Springer2019.
[5] Mohamed Elhosen, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed farouk "Secure Medical Data Transmission Model for IoT-based Healthcare Systems" IEEE2018.
[6] SohailSaif, Rajni Gupta and SuparnaBiswas "Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring"Springer2018.
[7] Hai Tao, MdZakirulAlamBhuiyan, Ahmed N. Abdalla, Mohammad Mehedi Hassan, JasniMohamadZain, and ThaierHayajneh "Secured Data Collection with Hardware-based Ciphers for IoT-based Healthcare"IEEE2018.
[8] Munish Bhatia, Sandeep K. Sood "A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective" Elsevier2017.
[9] "Secure Data Transmission in WSN" Springer2017.
[10] Haiping Huang, Member, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System"2017.
[11] Felix Büsching and Lars Wolf "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink"IEEE2015.
[12] Soufiene Ben Othman, Abdullah Ali Bahattab, AbdelbassetTrad, Habib Youssef "Secure Data Transmission Protocol for Medical Wireless Sensor Networks"IEEE2014.
[13] Partha P. Ray "Internet of Things based Physical Activity Monitoring (PAMIoT)"IEEE2014.
[14] Pardeep Kumar and Hoon-Jae Lee "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks" Sensors2012.
[15] HONGGANG WANG, DONGMING PENG, HSIAO-HWA CHEN "RESOURCE-AWARE SECURE ECG HEALTHCARE MONITORING THROUGH BODY SENSOR NETWORKS"IEEE2010.
[16] ApapornBoonyarattaphan, Yan Bai, Sam Chung "A Security Framework for e-Health Service Authentication and e-Health Data Transmission"IEEE2009.
[17] H S Ng, M L Sim and C M Tan "Security issues of wireless sensor networks in healthcare applications" BT Technology2006.

Correspondence to: Sohit Agarwal, Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: Sohit.agarwal@gmail.com