Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

IoT-Based ECG Monitoring System for Health Care Applications

Sohit Agarwal [1] , Devashish Dasaya [2]
1 Assitant 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

Article Info
Page Number: 10375-10391
Publication Issue:
Vol. 71 No. 4 (2022)

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 current temperature, humidity, and 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.

Article History
Article Received: *15 September 2022*
Revised: *25 October 2022*
Accepted: *14 November 2022*
Publication: *21 December 2022*

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

I. Introduction

In modern times, the adage "Health is Wealth" is just as relevant as it was in the past. While humans can send rockets to other planets, they also suffer from a wide range of health issues. Improvements in medical technology have allowed doctors to successfully treat a broader range of conditions. However, most people are no longer in a position to afford health regulation. It appears that the average person cannot afford the exorbitant price of medical care. Those who previously could not afford cutting-edge medical treatments do now because of technological

advancements. Those who are self-sufficient or have health insurance in large cities have easy access to quality medical treatment. Is there anything we can do to help people who live in remote areas and therefore can't get access to quality, affordable healthcare? The answer to this problem can be found in the implementation of technologically driven systems. Technology has little value unless it can help the poor. This concept is a great source of motivation for scholars and researchers studying the state of the computer industry today. This discussion centres on those who reside in rural locations (remote places). One application of this idea is the establishment of remote health monitoring. Until recently, this was inconceivable. As a result, distributed computing technologies like cloud computing and the Internet of Things can be used to enable system-wide remote monitoring (IoT). Thanks to IoT, we no longer have to choose between the online and offline worlds. Humans and mobile gadgets are fundamentally different in their physical and digital compositions. These two systems can be seamlessly integrated with the help of the Internet of Things. The term "Internet of Things" (IoT) is used to describe a vast network of interconnected electronic devices and infrastructures, such as mobile networks, the Internet, and a variety of wearables. As an alternative, cloud computing utilises a dispersed network of remote servers to store and process data on-demand in a highly accessible, scalable, and fault-tolerant manner. The use of cloud computing and the Internet of Things are indispensable in the field of remote health monitoring. Hadoop and other data storage and management frameworks are made available via the use of distributed programming frameworks in cloud computing. Our research demonstrates that the current state of IoT and cloud integration in hospitals and other healthcare facilities is not particularly useful. In situations when a primary health care centre (PHC) is accessible to a rural population, a comprehensive framework for remote health monitoring is needed. This dissertation proposes a method for PHC remote patient monitoring using a smart bed, IoT, and cloud computing. All of the patient's data, including vitals, is stored in the cloud, where it is then analysed by analytics and made accessible to the doctor and other parties via a mobile app. Following this, a brief synopsis of the study's findings will be presented, with succeeding chapters delving deeper into the results.

II. Literature Review

Mamoona Humayun et. All (2020) A standardised method of transmitting patient data across the Internet of Things in E-health contexts within hospitals. Internet of Things devices are widely employed in the healthcare business for real-time data collection and transmission. These are, unfortunately, insecure and call for the implementation of specialised, lightweight security measures due to limitations in available resources. To address these concerns, we developed a strategy that makes use of many groups of nodes and involves multiple rounds of node registration and key authentication to shorten the distance data can travel while simultaneously increasing the amount of energy required to transmit the data. When nodes in a cluster register the same shared key, they can utilise it for all of their authentication needs. We claim that the level of security offered by ECC is not sufficient for usage in E-health applications and give an alternative approach. In four separate approaches, we analysed our data, and then compared it to that of other studies (without GN, with one GN, and with two

GN). Our work is supported by rigorous mathematical models and copious amounts of simulation data. Results demonstrate that a significant improvement in energy efficiency can be achieved by adopting the strategy of dividing networks into numerous smaller networks composed of nodes. In comparison to the current group node, it offers around 10% better performance. [1]

S. Sheeba Rani et. All (2019) Research into the challenges of data gathering in IoT-based healthcare apps has led to the development of a novel healthcare data secure method that ensures the privacy and security of patient records. Using a SIMON block cypher algorithm on the information gathered by the network's sensors allowed for more secure communication between devices in the Internet of Things. To safeguard their patients' privacy, the authors used a share generation method. The CRT technique uses the optimal user input to generate a copy of each ciphertext (TLBO algorithm). Based on the results, it seems that the proposed technique has a good shot at increasing the quality of cloud data privacy while also increasing the number of cloud users. On top of all that, its execution time is far lower than that of other cypher algorithms and the model utilised to create shares in the system. The optimal CRT outperforms all other approaches by a large margin, providing the best possible level of security (between 65 and 95 percent) for a number of blocks. In subsequent research, we plan to use our unique data encryption methods and hybrid optimization methodology to the development of thorough implementations of the algorithms across a range of criteria. This can be used for many different cloud data security purposes in the event of an attack or danger. [2]

Ashutosh Sharma et. All (2019) This paper presents a healthcare CPS that is secure, SLA-compliant, and energy-efficient to ensure the confidentiality of all communications between patients and healthcare providers and the timely fulfilment of all user demands. By identifying the required service time and adjusting in AODV process methods, a secure and efficient communication mechanism is given by recognising the residual energy information at the node prior to transmission. Experiments measuring the proposed framework's performance in a simulated setting show that it outperforms the status quo with and without the introduction of malicious nodes. Analyzing SLA and energy findings using these variables reveals a pattern that defines a crucial part of efficient path selection in communication. When no such threats are present, however, both quantitative and qualitative measurements perform as expected. However, security is compromised in the name of efficiency. Data size will be reduced to make efficient use of network resources, and future research will focus on applying the proposed approach to other security assaults such byzantine, jellyfish, and worm hole attacks. [3]

Sarada Prasad Gochhayat et. All (2019) In this paper, we outline the steps necessary to implement key management across a heterogeneous network of devices running various Internet of Things applications. Therefore, it is critical that IoT applications have strong data management skills, such as the capacity to collect, store, and transport data safely. We want to employ mobile agents' advantages to help local administration safeguard nodes (IoT application nodes) and guarantee that data can continue to flow from its source to its destination even if a user moves between different subnetworks. Our method seems to be working in the simulations, so we should be able to reach our goals. [4]

Mohamed Elhosen et. All (2018) Secure transmission of diagnostic information about patients via colour and grayscale images is presented as a new paradigm within the medical IoT. The proposed model utilized AES and RSA encryption alongside 2D-DWT-1L or 2D-DWT-2L

steganography. The test used both colour and black and white images with varying font sizes. Six statistical markers of success were used to evaluate the outcomes (PSNR, MSE, BER, SSIM, SC, and correlation). When it comes to concealing personally identifiable information about patients while simultaneously transmitting a cover image with high imperceptibility, capacity, and low deterioration of the received stego-image, the suggested model surpasses state-of-the-art techniques. [5]

Sohail Saif et. All (2018) The cloud enabled the development and implementation of a programme for secure WBAN communication in healthcare. It will be challenging for unauthorised users to access any node that depends on the authentication of patients' and doctors' biosignals. Every person has their own unique biosignal. Thanks to AES ciphering technology, wireless networks are safe against intrusion. When these procedures are combined, data is more secure, authenticated, reliable, up-to-date, and easily accessible thanks to the cloud server. [6]

Hai Tao et. All (2018) To ease customers' minds about the safety of their personal information when utilising IoT-based healthcare apps, we developed a new method of data collecting we term "Secure Data." We introduce, implement, and optimise the KATAN secret cypher algorithm on the FPGA hardware platform. Protecting the security of the KATAN encryption relies on secret cypher exchange and mending. The analysis demonstrates that the Secure Data system reduces costs across the board, including processing, energy use, and security. The next steps involve implementing the algorithms and measuring their efficacy in preventing assaults and threats using a variety of criteria. [7]

Munish Bhatia et. All (2017) In this article, we take a close look at one promising area of future Internet of Things application: health monitoring during exercise. The proposed model may quickly assess the susceptibility of a particular health state to injury by incorporating a wide variety of health-related characteristics. The model's layered structure was also designed to carry out a series of predetermined tasks in a synchronised method, maximising efficiency. As a first step, we use the Internet of Things to gather data on the state of various parts of a workout. Now that these variables have been safely uploaded to their corresponding cloud storage, in-depth analysis can be performed. Using a vulnerability scoring system, the BBN classifier model ranks properties. Segmenting data in real-time with temporal mining paves the way for the derivation of probabilistic measures like PSoV, which can be used in quality evaluation. To determine the health risk, we use the average weight associated evaluation of the data values. Accurate predictions of PSoV values can then be made using a neural network (ANN) prediction model trained with these numbers. In order to make an accurate forecast, one must first observe, then gain knowledge, and last make a prognosis. Five individuals have been tracked for two weeks while they perform a variety of exercises to determine the device's effectiveness. High efficiency and accuracy rates from statistical evaluations suggest the proposed technique has great potential in healthcare. [8]

Mohamed Elhoseny et. All (2017) Because of the WSN's limited resources and often hostile conditions, security is of the utmost significance. The proposed cluster-based paradigm has the potential to reduce network energy consumption and thereby lengthen their lifetimes. Protecting data clusters in wireless sensor networks is an area that has seen a lot of discussion and debate, with a number of different solutions proposed. When implemented with a strict clustering structure, most routing protocols leave networks open to a wide range of threats.

Several safe clustered routing strategies have been developed for WSNs (WSNs). Next, a power-efficient method was introduced for securing a dynamic cluster network. It also demonstrates a four-stage methodology for developing a secure WSN clustering approach. Selecting a trustworthy cluster leader, creating a trustworthy cluster, collecting trustworthy data from trustworthy cluster nodes, and securely routing trustworthy data to a trustworthy base station are the steps involved in implementing a safe cluster. An algorithm for creating secure clustering is not considered complete until all of the conditions we've set forth have been satisfied, including the four phases of safe clustering. [9]

Haiping Huang et. All (2017) To address these issues, the authors of this study propose a new paradigm for e-/m-healthcare systems they refer to as "HES." There are three distinct categories for HES characteristics: By using low-cost and easily deployed wireless sensor networks as the relay infrastructure for GSRM-based secure transmission of medical data from WBANs to WPANs, we first solve the issue of ad hoc communications between users' mobile terminals and embedded (wearable) medical devices (nodes); second, we apply privacy-preserving strategies like HEBM to achieve satisfactory performance. The necessity for a doctor or administrator to be present for routine physical examinations can be greatly reduced with the help of an expert system, and users' loved ones can have access to their medical records anytime they need it. Since healthcare decisions are increasingly being informed by data, HES stands to benefit greatly from this development. For instance, HES is not yet capable of monitoring or analysing unusual diseases, and its expert system has poor diagnostic accuracy. [10]

Felix Bushing et. All (2015) Indicators of health and activity levels are two types of sensitive data that need special protection. There are many who say this data doesn't require such a complex procedure. However, we believe it to be a sound strategy if we can achieve unparalleled high security at an affordable cost. The use of one-time passwords (OTPs) can help ensure the security of confidential data sent across wireless networks. By periodically recharging WBAN node OTPs, the system suggested, implemented, and tested here enables persistent and secure monitoring of sensitive data. Depending on the data rate being generated, contemporary computers can store a large number of regenerated OTPs and guarantee data transfer for long periods of time. The data stream provided by DTN is guaranteed to be uninterrupted and error-free. The quantity of RAM or the number of read/write cycles needed by the computer will not change due to the addition of an external storage device. The transport protocol's maximum payload size has not changed either. Safe, transparent, tamper-proof, resource-efficient, reliably delivered data can all be achieved with OTPs. [11]

Soufiene Ben Othman et. All (2014) Due to recent advancements in medical wireless sensor networks, remote patient monitoring is now a feasible option. Wireless sensor network advances give a new dimension to healthcare applications, and the authors investigated the security concerns that arise during implementation. We zero down on the issue of transmitting sensor data wirelessly in the field of medical wireless networks. Tests have shown that the author's approach is reliable enough for widespread implementation. As of this writing, we aim to have begun recruiting hospitalised patients for our study. This section of the hospital is equipped to perform surgeries and provide intensive care. To put the described prototype to the test, the authors are organising a new workshop. Participants will assume the roles of patients for the duration of the session. The protocol should be improved. It is essential to put extra effort into formalising and verifying the security aspects. [12]

Partha et. All (2014) Because of the profound effects it can have on sectors as diverse as logistics, environmental monitoring, retail, and agriculture, the Internet of Things has recently emerged as a game-changer in the business world. Internet of Things devices are making it simpler and more accessible for us to help with the care of the sick and elderly, an area in which we have a moral obligation to engage (IoT). PAMIoT was developed so that people's physical activity might be tracked outside of specialised settings and into their regular routines. The difficulty of keeping a healthy human population is one that this approach can unquestionably help with. Using low-energy communication technologies, PAMIoT's hardware platform and upkeep costs are kept low and sustainable. Due to its simple architecture, PAMIoT performs admirably in environments with less constraints. PAMIoT, however, is not suited for monitoring urgent situations and so would be of no use. More investigation on the security concerns that may occur from using PAMIoT to a network of devices is needed. [13]

Pardeep Kumar et. All (2012) The privacy and security of healthcare sensor networks are special considerations. Having a well-thought-out security strategy is essential to the achievement of any wireless application's goals. The difficulty we've encountered in developing a medical-sensor-based healthcare monitoring system highlights the fact that people are more likely to put their faith in a technology if they believe it to be safe. Use it incorrectly, and the patient's life could be at danger. The usage of wireless medical sensor networks presents a lot of obstacles, and we hope that this study will inspire future academics to design more effective security measures for these applications. [14]

Honggang Wang et. All (2010) For health-tracking programmes that use electrocardiograms, we presented a BSN structure and the related algorithms. It's a BSN alternative to the existing wireless cardiac monitoring systems based on sensor networks that's smaller, cheaper, and more adaptable. Thanks to our efforts, a wireless ECG sensor health monitoring system has been developed that is both effective and simple to implement. An advanced emergency detection system was also designed for use in a BSN, with signal classifications to prioritise resources, selective encryption, and intelligent resource allocation. This innovation minimises operational delays while maintaining a high standard for both power efficiency and signal quality. The proposed technology's potential medical applications extend far beyond ECG monitoring. [15]

Apaporn Boonyarattaphan et. All (2009) There are three main ways in which this work advances the field. As a first step, we offer a solid foundation for reliable and efficient e-healthcare. The author argues that until recently, little attention was paid to security analysis of SOA-based e-Health services. To accommodate the wide range of applications for e-Health services, we present two risk-adaptive authentication methods. Besides guaranteeing the security of crucial e-Health data, the proposed authentication methods also deliver first-rate care. In the third place, the authors have proven that using various encryption methods with the optimal key length is a cost-effective way to provide safe e-Health services. The proposed security architecture and associated methods are now being prototyped in an electronic medical record system. [16]

H S Ng et. All (2006) The advent of wireless sensor networks has brought about exciting new possibilities in medical research. A solid security mechanism must be in place before the system can be put into action. In order to authenticate sensor nodes with handoff in hierarchical network designs, this study proposes techniques for key management, such as efficiently

dispersing keys in extensive distributed topologies. Because of their limited resources, sensor nodes make it more difficult to implement a multi-layer security solution. Increasing the healthcare industry's use of pervasive computing for the benefit of the general population will require much more labour and effort. [17]

III. Methodology

3.1 Proposed Model Communication Method

Figure: 3.1 Proposed Model Communication Method

The process is automated with the help of our suggested solution. The node MCU's ESP8266 microcontroller collects data from a number of sensors, including those that measure temperature, humidity, and vital signs. Read both temperature and humidity with the DHT11 Temperature and Humidity Sensor. Accurate environmental monitoring is possible thanks to the use of a capacitive humidity sensor and a thermistor-based temperature sensor. Data (I/O) - Digital serial Data Output, Ground (VCC), and Power (GND) are its three pins.

Microcontroller: As the microcontroller for the node, the ESP8266 is used. A platform for creating Internet of Things applications that use the free and open-source Lua programming language. The Wi-Fi SOC it uses is the ESP8266, and it comes preloaded with firmware that communicates with the Thing Speak cloud and makes data accessible via mobile app. The "Power" pins are the first of various varieties. A USB port, a 3.3V power input pin, a ground pin, and an external power input pin labelled Vin are all included on the Micro-USB Node MCU. Second, pressing this button will reset the microcontroller (control pins EN, RST). The pulse sensor, to round things off, makes use of Analog pin A0's capacity to measure Analog voltage.

Sensor data is continuously collected by a microcontroller and then transmitted to the cloud and various mobile applications. When the data is collected, the Node MCU microcontroller with built-in WIFI will send it to the Thing Speak cloud. Users using Android and iOS devices can use the Mobile App that provides this data.

3.2 Connection Block Diagram

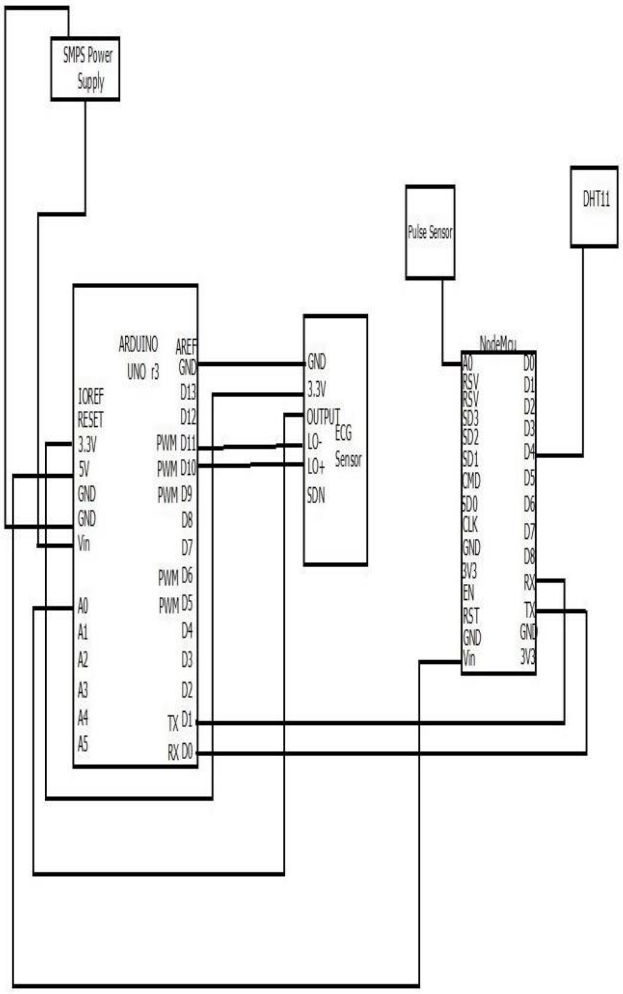

Figure: 3.2 Main Connection Diagram

The sensors that will be used in this project and their connections are shown in the image above, which is a connection diagram for the proposed work. The nodemcu is wired to a temperature and humidity sensor (a DHT11) and a pulse rate sensor (an HC-SR04), while the electrocardiogram (ECG) sensor is wired to the Arduino. In this setup, the dht11's data pin was wired to the analogue input on the nodemcu board, and the pulse rate sensor's output pin was wired to the board's fourth GPIO (General purpose input output) port. Connecting an electrocardiogram (ECG) sensor to an Arduino The analogue input pin on the Arduino board is connected to the Lo- and Lo+ pins of the ECG sensor. Once the IN electrode is unplugged, dc leads off detection mode is activated and LO rises, and the condition is reversed once the IN electrode is connected again. The logic one (LO+) in the first stage of a comparator is an important output. In the dc leads off detecting mode, LOD+ is activated when the +IN electrode is either detached (high) or connected (low). We decided on a 5V SMPS because all of the boards and sensors require a regulated 5V supply (Switch Mode Power Supply).

3.3 ECG Algorithm Flow Chart

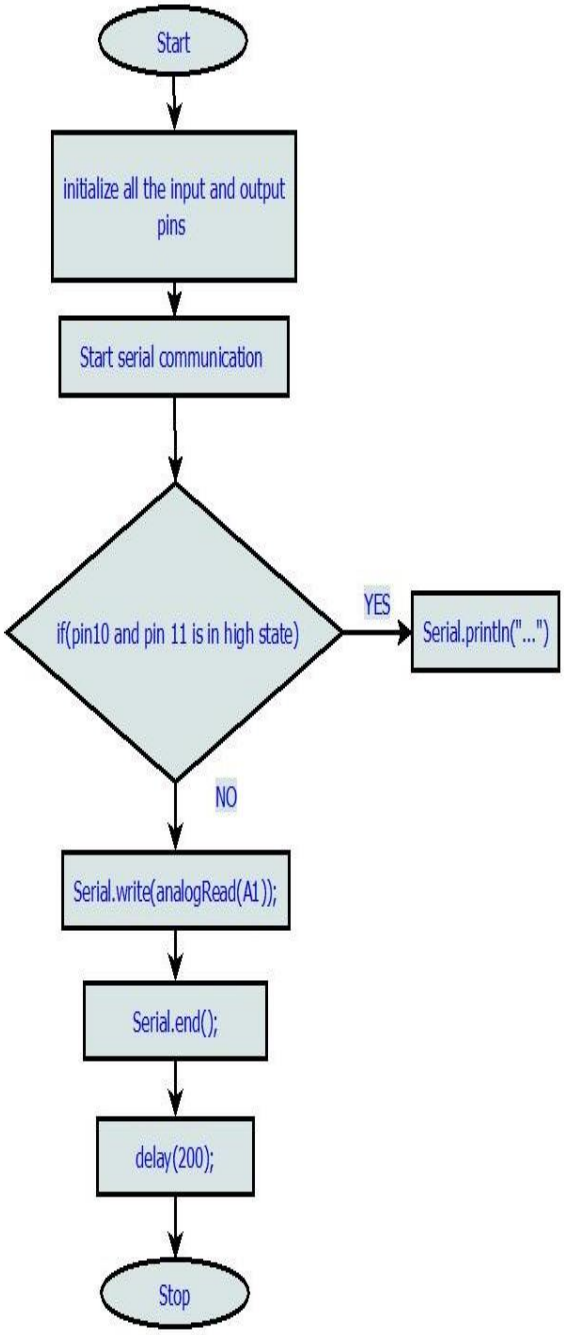

Figure: 3.3 ECG Code Flow Chart

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 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 NodeMcu Code Flow Chart

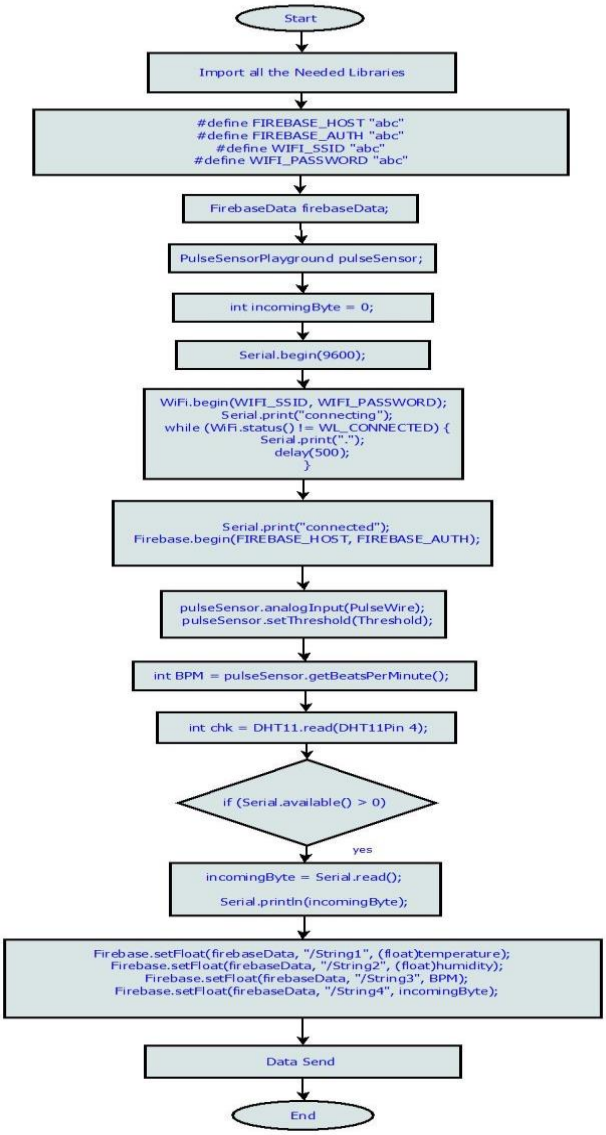

Figure: 3.4 NodeMcu (Esp8266) Code Flow Chart

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 nodemcu wifi 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 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

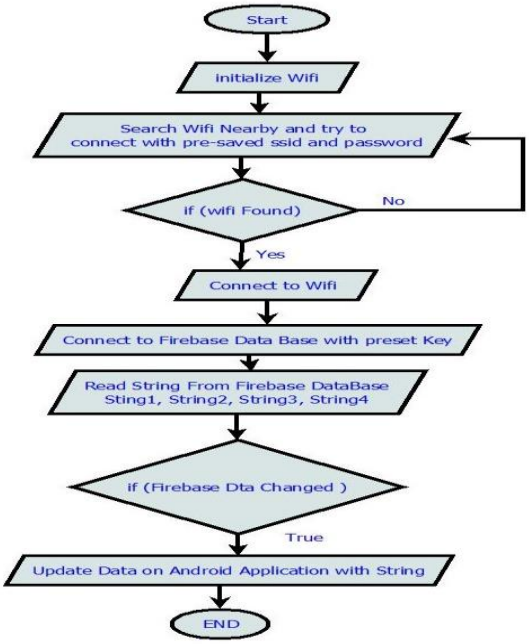

Figure: 3.5 Firebase to Device Communication Flow Chart

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

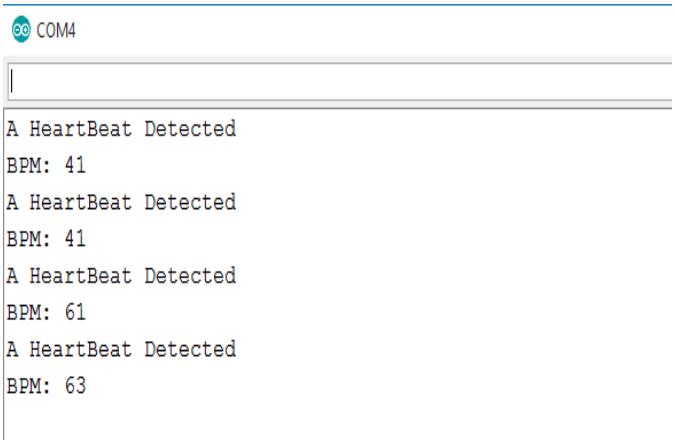

Figure: 4.1 Heartbeat Detection

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

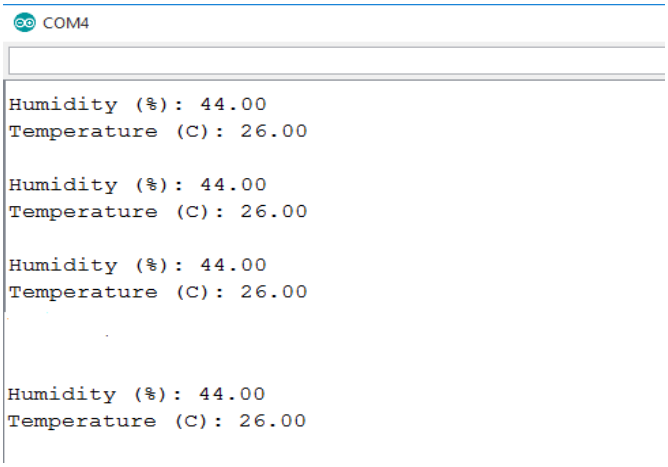

Figure: 4.2 Temperature and Humidity Detection

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.

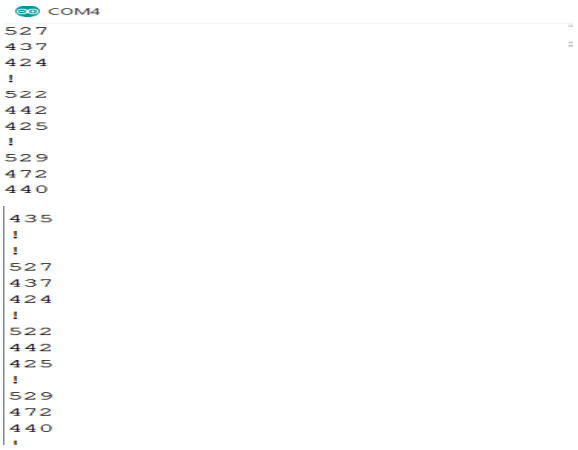

Figure: 4.3 ECG Readings

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

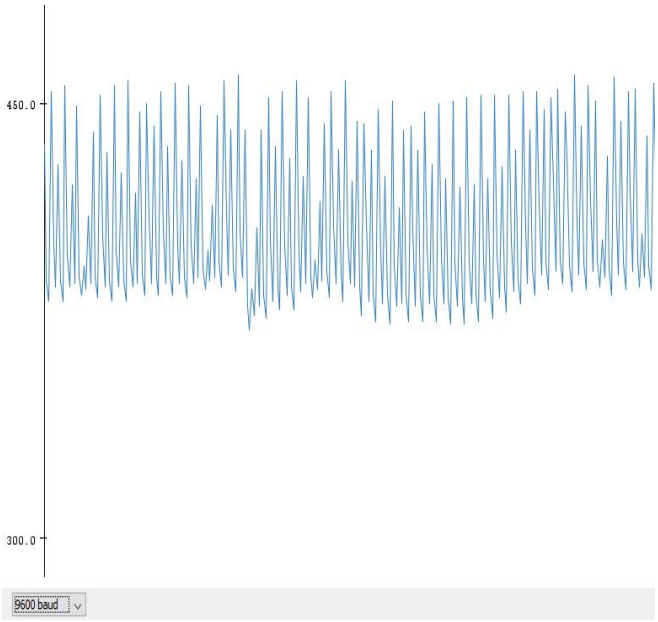

Figure: 4.4 ECG Graph

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

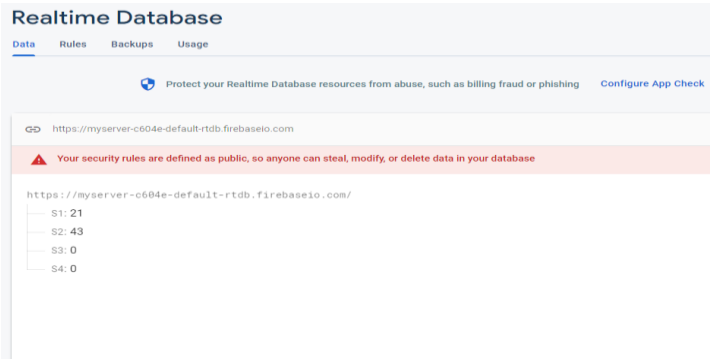

Figure: 4.5 Real-time FireBase DataBase

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.

4.2 Android Application Results

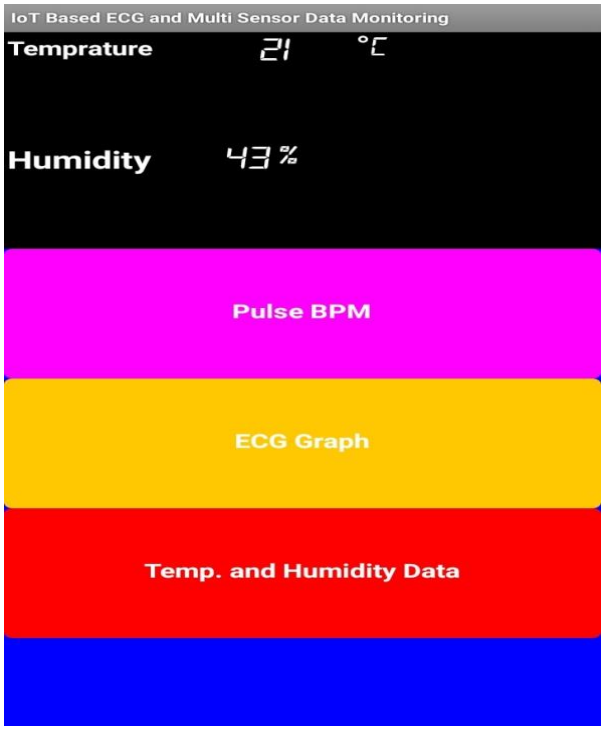

Figure: 4.7 Temperature and Humidity on Android Application

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.

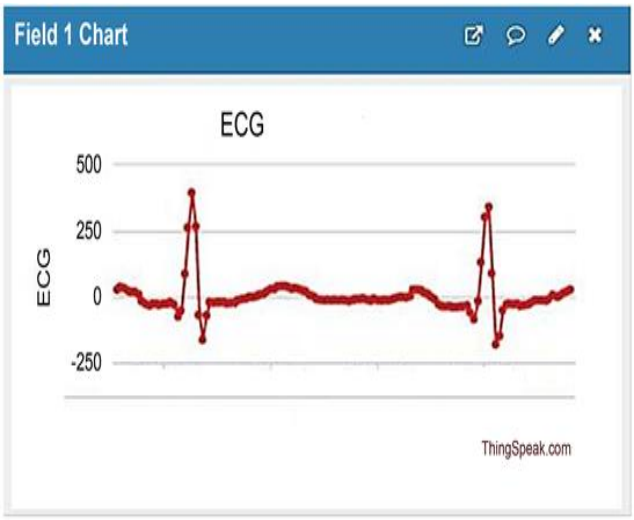

Figure: 4.9 ECG Graph On Android Application

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] Mamoona Humayun, 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 & Ramachandran Manikandan “Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers”Springer2019.

[3] Ashutosh Sharma, Geetanjali Rathee, Rajiv Kumar, Hemraj Saini, Vijayakumar Varadarajan, 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, Chhagan Lal, Lokesh Sharma, D. P. Sharma, Deepak Gupta, Jose Antonio Marmolejo Saucedo, Utku Kose "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] Sohail Saif, Rajni Gupta and Suparna Biswas "Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring"Springer2018.
[7] Hai Tao, Md Zakirul Alam Bhuiyan, Ahmed N. Abdalla, Mohammad Mehedi Hassan, Jasni Mohamad Zain, and Thaier Hayajneh "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, Abdelbasset Trad, 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] Apaporn Boonyarattaphan, 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.