ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM

A Thesis

Submitted

In Partial Fulfillment of Requirements

for the Degree of

MASTER OF TECHNOLOGY

In

Computer Science & Engineering

Submitted by:

DEEPIKA DHAWAN

Roll No : 1901622002

Under the Supervision of:

Dr. Faiyaz Ahamad

(Assistant Professor)

Department of Computer Science and Engineering

INTEGRAL UNIVERSITY, LUCKNOW, INDIA

June, 2022

CERTIFICATE

This is to certify that **Ms. Deepika Dhawan** (Roll No. 190162202) has carried out the research work presented in the thesis titled "**ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM**" submitted for partial fulfillment for the award of the **Master of Technology in Computer Science and Engineering from Integral University, Lucknow** under my supervision.

It is also certified that:

i. This thesis embodies the original work of the candidate and has not been earlier submitted elsewhere for the award of any degree/diploma/certificate.

ii. The candidate has worked under my supervision for the prescribed period.

iii. The thesis fulfills the requirements of the norms and standards prescribed by the University Grants Commission and Integral University, Lucknow, India.

iv. No published work (figure, data, table etc) has been reproduced in the dissertation without express permission of the copyright owner(s).

Therefore, I deem this work fit and recommend for submission for the award of the aforesaid degree.

Dr. Faiyaz Ahamad
Dissertation Guide
(Assistant Professor)
Department of CSE,
Integral University, Lucknow

Date:
Place: Integral University, Lucknow

DECLARATION

I hereby declare that the thesis titled **"ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM "**submitted to Computer Science and Engineering Department, Integral University, Lucknow in partial fulfillment of the requirements for the award of the Master of Technology degree, is an authentic record of the research work carried out by me under the supervision of Dr. Faiyaz Ahamad, Department of Computer Science & Engineering, Integral University, Lucknow. No part of this thesis has been presented elsewhere for any other degree or diploma earlier.

I declare that I have faithfully acknowledged and referred to the works of other researchers wherever their published works have been cited in the thesis. I further certify that I have not willfully taken other's work, para, text, data, results, tables, figures etc. reported in the journals, books, magazines, reports, dissertations, theses, etc., or available at web-sites without their permission, and have not included those in this M.Tech thesis citing as my own work.

In case , this undertaking is found incorrect, I accept that my degree may be unconditionally withdrawn.

Date:

Signature

Name : Deepika Dhawan
Roll. No: 1901622002

COPYRIGHT TRANSFER CERTIFICATE

Title of the Dissertation: **ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM**

Candidate Name: **DEEPIKA DHAWAN**

The undersigned hereby assigns to Integral University all rights under copyright that may exist in and for the above dissertation, authored by the undersigned and submitted to the University for the Award at the M.Tech degree.

The Candidate may reproduce or authorize others to reproduce material extracted verbatim from the dissertation or derivative of the dissertation for personal and/or publication purpose(s) provided that the source and the University's copyright notices are indicated.

DEEPIKA DHAWAN

RECOMMENDATION

On the basis of the declaration submitted by "**DEEPIKA DHAWAN**", a student of M.Tech CSE (Evening), successful completion of Pre presentation on 28-05-2022 and the certificate issued by the supervisor **Dr. Faiyaz Ahamad** (Assistant Professor) Computer Science and Engineering Department, Integral University, the work entitled "**ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM**", submitted to department of CSE, in partial fulfillment of the requirement for award of the degree of Master of Technology in Computer Science & Engineering, is recommended for examination.

Program Coordinator Signature
Dr. Faiyaz Ahmad
Dept. of Computer Science Engineering
Date:

HOD Signature
Mrs. Kavita Agarwal
Dept. of Computer Science Engineering
Date:

ACKNOWLEDGEMENT

I am highly grateful to the Head of Department of Computer Science and Engineering for giving me proper guidance and advice and facility for the successful completion of my dissertation.

It gives me a great pleasure to express my deep sense of gratitude and indebtedness to my guide **Dr, Faiyaz Ahmad , Assistant Professor, Department of Computer Science and Engineering,** for his valuable support and encouraging mentality throughout the project. I am highly obliged to him for providing me this opportunity to carry out the ideas and work during my project period and helping me to gain the successful completion of my Project.

I am also highly obliged to the Head of Department, **Mrs. Kavita Agarwal, Department of Computer Science and Engineering** and PG Program Coordinator **Dr. Faiyaz Ahamad, Assistant Professor, Department of Computer Science and Engineering**, for providing me all the facilities in all activities and for his support and valuable encouragement throughout my project.

My special thanks are going to all of the faculties for encouraging me constantly to work hard in this project. I pay my respect and love to my parents and all other my friends and supporting member for their help and encouragement throughout this course of project work.

TABLE OF CONTENTS

List of Tables

List of Figures

List of abbreviations

Internet of Things (IOT)

Radio Frequency Identification (RFID)

Wireless sensor Network (WSN)

ABSTRACT

One of humanity's greatest difficulties is health. In the recent decade, healthcare has gotten a lot of attention. Not just for sensory equipment, but also for communication, recording, and display equipment, technology plays a significant role in healthcare. It is critical to keep track of numerous medical markers as well as the post-operative days. As a result, the most recent trend in healthcare communication methods utilizing the Internet of Things (IoT) has been adopted. Due to its superior technology, the patient monitoring system has recently become one of the most significant advancements. At this time, a modern strategy is required. The underlying issue with the old technique is that in severe cases, health care experts must be present at the patient's location at all times to check symptoms on a frequent basis. To overcome this issue, health professionals must design a dependable patient monitoring system that allows them to monitor their patients remotely. The project is a wireless health monitoring system based on mobile devices that may deliver real-time online information on a patient's physical status. The Raspberry Pi is employed as an important element of the processing in this project, as are sensors like as temperature, pulse/heart rate, and PIR. These sensors are wired to an Arduino board, and reads the sensor readings and sends them to the Raspberry Pi through serial connection. The sensor data is now saved in a file on the Pi, which is then transferred to the cloud over the Internet. Finally, this uploaded data is retrieved through the user app. The same data is then transferred to the patient and doctor via Firebase to further improve treatment by obtaining patient information in a timely manner.

CHAPTER 1

INTRODUCTION

The Internet of Things (IoT), which uses a number of interconnected devices and networks to deliver digital solutions and monitoring systems across healthcare systems, is a game-changing technology in this field. Security is a significant concern in the creation of an IoT-based healthcare system since it deals with sensitive and secret patient information.

The internet has a significant influence on our day-to-day lives in a variety of ways. The basic idea behind this widely acknowledged technology is to link items to the Internet in a simple and effective manner. When items or devices are connected to the Internet, users may access and control them from anywhere in the world. These gadgets may also be operated with the help of computers, which allows users to configure the device [1],[4]. Under certain situations, the gadgets can conduct a series of operations. To communicate, these gadgets use sensors, microcontrollers, and transceivers. Military, business, healthcare, retail, and transportation are some of the most common uses of wireless communication networks.

These networks can be wired, cellular, or ad hoc. In society and industry, wireless sensor (WSNs), actuator networks, and vehicle networks have all attracted a lot of interest. The rising use of Internet of Things (IoT) gadgets and IoT networks in recent years has made them vulnerable to different security assaults. To provide confidentiality, authentication, access control, and integrity, among other things, effective security and privacy protocols must be deployed in IoT networks. A complete assessment of security and privacy problems in IoT. Is presented in this research. Unfortunately, the bulk of these devices and apps are not built to withstand security and

privacy attacks, resulting in a slew of security and privacy vulnerabilities in IoT networks, including confidentiality, identification, and integrity of data, access control, and secrecy [2]. Information security is a concern for both cloud consumers and cloud service providers. Because there is a risk of cloud-based attacks that compromise security features such as confidentiality, availability, and integrity. Intrusion Detection Systems (IDS) are used to improve the system's security and resilience to both internal and external threats. The basic objective of an intrusion detection system is to identify an intrusion and, if required or practicable, to take steps to eliminate it. There are primarily two approaches for detecting intrusions [3].

The perception layer's main role is to collect healthcare data from a range of devices. The network layer, which is made up of wired and wireless systems as well as middleware, processes and transmits the information gathered by the perception layer with the help of technical platforms. Transport protocols that are well-designed not only enhance transmission efficiency and lower energy consumption, but they also provide security and privacy. The application layer combines medical information resources to deliver individualised medical services and meet the demands of end users, based on the target population's current status and service need.

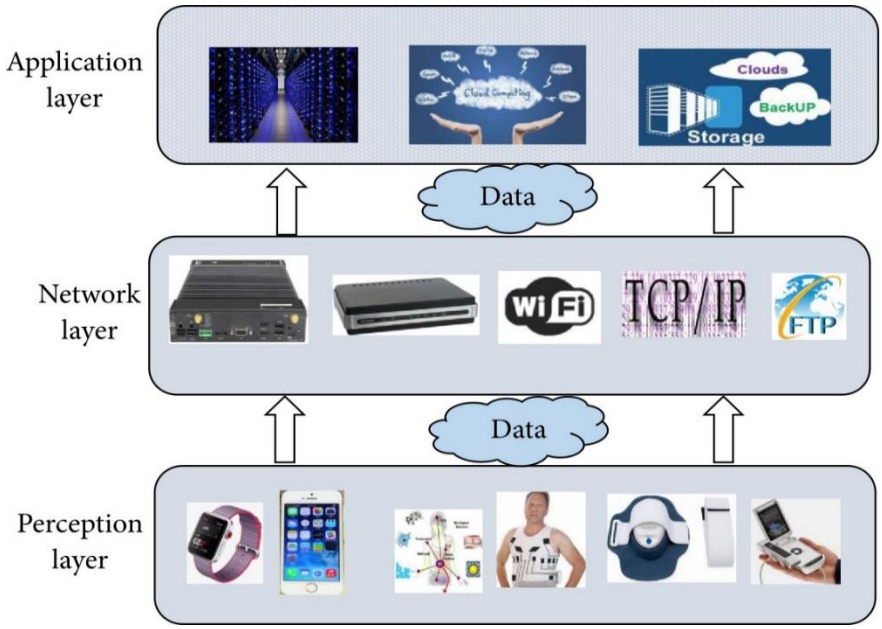


Fig 1 : Structure of Medical Internet of Things.

CHAPTER 2

BACKGROUND

Several attempts have been undertaken in the domain of IoT data processing and storage. Some existing relevant work in the area of IoT data protection in the cloud service may be summarized as follows:

Health is a fundamental capability that people require to properly sense, feel, and act, and as such, it is a key step in the development of both the individual and the environment in which they live [3]. As a result, proper ways and means must be provided to enable optimal health care based on parameter monitoring and direct provision of medical aid. Development and application of new technologies, particularly internet Online and Wireless also known as internet of Things (IoT), offer a worldwide framework for the development of health care system infrastructure [5][2]. This results in an e-health system that provides a vital set of information to all participants (patients, nursing and medical personnel, and health insurance companies) in real time, regardless of their current location. In many circumstances, real-time model parameters are not accurately recorded in clinics and hospitals, making it difficult for hospitals to monitor patients' health status on a regular basis. Constant monitoring of ICU patients is also impossible. This method is useful in dealing with problems like these. This project is intended for use in hospitals to monitor and measure different characteristics such as temperature, heart rate, and movement. The findings may be recorded and shown on a monitor using a Raspberry Pi. The result is then saved in the cloud and communicated to the user's end application over Wi-Fi. Doctors can get the findings using an app.

2.1 Objectives and Limitation of the Study

2.1.1 Objectives

IoT and cloud computing are emerging revolutionary technologies that complement each other's capabilities when integrated as flexible, scalable and efficient patient healthcare systems. The combination provides benefits including ease of implementation compared to conventional networks, enhanced information security during communication, quick access to records and energy savings over traditional modalities. IoT-cloud-based e-Health systems can significantly improve healthcare services and promote continuous systematic innovation. In IoT-cloud-based e-Health systems, underlying IoT networks enable communication between users, services and servers, with medical data stored in the cloud.

2.2 Limitation of the study

2.2.1 Priority Basis

Ambient Assisted Living (AAL): the placement of smart objects within an assisted living environment that care for and assist seniors to live more independently. AAL applications also collect, manage, and analyze patient activity to allow remote monitors to react quickly to emergencies and accurately investigate allegations of mistreatment [1,6,8,15,18]. • Internet of Health Things (IoHT): smart devices with integrated mobile and cloud

computing capabilities used in the medical field to monitor patient data in real-time. Collected data can be analyzed immediately and used to diagnose and treat patients quickly and effectively. However, such systems are still vulnerable to security attacks and privacy leaks, which many researchers have tried to identify and rectify [1,2,4,10,16,19,20]. • Wearable Devices: a distinctive sub-category of IoT devices, such as smart wristbands, watches, shoes, shirts, caps, necklaces, headbands and eyeglasses with integrated sensors and microcontrollers. Most of these devices operate on the fixed IEEE 802.11 standard frequency [5,14]. Blockchain: a system in which a record of actions is maintained across several computers linked in a peer-to-peer network. Use of blockchain technology in health systems can increase transparency between patients and doctors, ensure efficient collaboration between health organizations using smart contracts and resist failure and data fragmentation with its decentralized and distributed architecture as used in Ray et al. [21] presented blockchain technologies for IoT-based healthcare that are being heavily exploited and used in many domains. They presented consensus algorithms and platforms in IoT-based e-healthcare. They showed how their key features of the IoT and blockchain can be leveraged to support healthcare services. However, blockchains are inherently highly vulnerable to attack because of their transparency.

2.2.2 IoT-cloud-based e-Health

IoT-cloud-based e-Health system implementations are highly variable

and can be tailored to meet the needs of specific e-Health system providers. Therefore, e-Health system providers offer many different types of IoT and cloud computing services to allow functionality like continuous monitoring, preventive care, patient satisfaction tracking and AI-driven diagnosis. Each of these services constitutes a potential privacy leak that must be considered when implementing privacy protection measures within a given system. Growing awareness among end-users has made them more cautious than ever about the privacy of their medical data. For example, if a patient suffering from an embarrassing health condition had their confidential information leaked or disseminated on social media, it would be difficult to maintain their trust in the health service provider, not to mention extremely difficult for Proposed in Real-time the provider to rectify the situation such indicated in Nazir et al. [22] presented IoT for healthcare by using effects of mobile computing. They used a systematic literature review protocol and showed how mobile computing can assist IoT application in healthcare. The IoT in healthcare system can bring privacy and security in health IoT devices. Similarly, method used in Semantha et al. [23] analyzed the contemporary based on a systematic literature review to examine privacy by design frameworks in-depth targeted at the healthcare sector and identify the key limitations in the healthcare section. They propose their viable for the future research and

development direction for healthcare. Wu et al. [24] established a model based on mobile health for IoT system in social networks. The model is applied to a social network which user can used the model through APP in IoT for diagnosis and treatment. The model can modify the control variable, provide the most effective for hospitals. Khatoon et al. [25] presented a survey on application of IoT in healthcare. IoT for healthcare services can enhance the reliability and quality to the patients. The IoT in healthcare consists of sensor enabled smart devices that accurately data for analysis and actions.

2.2.3 Wireless Sensor Network (WSN):

A flexible, scalable, dynamic, cost-effective ad-hoc network of analog or digital devices and nodes that communicate using secure radio signals. They enable providers to monitor their patients in real-time. The communication of WSNs secured via hardware and software can act as an adversary to sense and challenge the individual wireless signals transmitting data to determine authenticity [2,19,22,24–26]. • Body Sensor Network (BSN): a collection of sensors connected to the body of a patient that transmits data wirelessly to system nodes for later analysis. The patient's data is collected by the sensors, then transferred to the nodes using commonly accepted routing and switching protocols such as LoWPAN, multi-hub routing and so forth. [5,14,22,25].

• Radio Frequency Identification (RFID): a low-cost system of physical

tags that continually transmit information over very low radio frequencies and the accompanying readers. RFID provides automatic identification and easy monitoring/tracking. RFID readers identify the tags, collect, process and transfer the data to designated servers. RFID tags are usually attached to the patient to collect physical health system parameters or are used in inventory systems to track medication and other miscellaneous hospital supplies and equipment. RFID has a protracted lifespan as the tags do not require power to operate as used in Fan et al. [29] presented lightweight RFID protocol for medical privacy protection in IoT. The application of RFID system to the medical system can effectively solve the problem of medical privacy. RFID can collect useful information and conduct data exchange and processing with back-end server through the reader.

• Remote Patient Monitoring (RPM): a system that utilizes flexible wireless or web-based services to monitor patients without physical contact. RPMs are used in conjunction with WSNs, BSNs and various IoT devices.

Fig 2 : Process of Data Model

CHAPTER 3

PROPOSED METHODOLOGY

3.1 Study Area Description

The project's goal is to create a dependable patient monitoring system that allows doctors to remotely check a patient's health state. The doctor regularly monitors the patient in this initiative without ever visiting the patient. Physiological characteristics such as temperature, heart rate, and mobility are sensed using a variety of sensors. These detected signals are sent to the Raspberry Pi through ADC, which converts analogue impulses to digital signals, allowing the data to be updated continually. Data is delivered to the cloud over Wi-Fi and stored, after which it is wirelessly sent to user end application. As a result, the doctor may view the patient's data while seated in his cabin.

When the patient is in a critical situation, he takes the essential steps to help them.

Firebase Database with Arduino UNO and ESP8266 Module. Storing data (such as sensor data) in a database that can be accessed from anywhere by the Internet can be very useful. Firebase makes it easy to store and retrieve data. This is a better option, which can store the data without any attack and send it from one place to another securely through WiFi. Due to which health service to the patient can be done continuously at home.

3.2 IoT-Related Standards and Guidelines

Considerations and help for designing and deploying secure IoT devices have been offered by the Cloud Security Alliance [8]. It tries to address some of the most typical problems encountered during the creation of IoT devices. A variety of tasks have been suggested that will enable a development company to begin improving the security

condition of IoT devices.

This article includes a graphical representation of the procedures required to design more secure IoT devices. Despite the complexity of IoT systems, which include devices, gateways, mobile apps, appliances, web services, datastores, analytics systems, and more, this guideline focuses primarily on "devices." Our paper, on the other hand, highlights security and privacy functionality concerns throughout the whole spectrum of IoT systems. A security framework has been presented in Industrial Internet Consortium [25] which comprises of six interacting building blocks. These building blocks are organized into three layers. The top layer includes four core security functions, which are supported by a data protection layer and a system-wide security model and policy layer. The four core security functions are: endpoint protection, communication and connectivity protection, security monitoring and analysis, and security configuration management. And then they break down each layer into related key functions and explain the responsibility for each function. This document explains and positions security or related architectures, designs, and technologies. It also identifies procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. Security characteristics, technologies, and techniques that should be applied, and methods for addressing security, have been described. However, it lacks some of the security functionalities, and in particular, it does not focus on privacy issues.

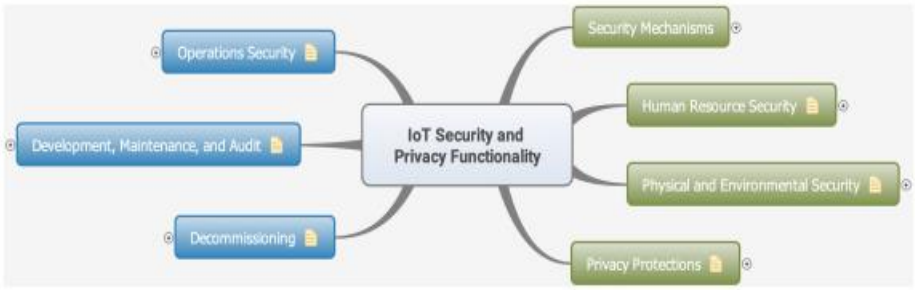


Fig 3:: IOT Security privacy and functionality framework

3.2 Work Process

- In a work presented by [27], the most relevant available solutions regarding security, privacy, and trust in IoT have been analyzed. Proposals related to security middleware, secure solutions for mobile devices, and ongoing international projects on this subject, have been discussed in their work; however, the focus is more general, addressing authentication, confidentiality and access control, while we break down security and privacy requirements in more detail, using a framework of functionalities for all the baselines.

  Main challenges and security threats in smart home networks have been analyzed by Lee et al. [17], and the fundamental requirements in order to provide secure and confidential operations in smart homes are explained from the results of their analysis. Although these requirements have been listed, they still lack practical solutions or recommendations in this matter. In [28], Suo et al. have deeply analyzed security architecture and features, and divided IoT systems

into four key levels of architecture. According to this analysis, the security requirements for each level have been summarized. Furthermore, the research status of key technologies including encryption mechanism, communication security, protection of sensor data, and cryptography algorithms, have been discussed. Roman et al. [23] have discussed threats faced by IoT, as well as security and privacy foundations based on objectives in a scenario involving a smart meter. However, they did not give any details about practical baselines and guidelines showing how to achieve these foundations.

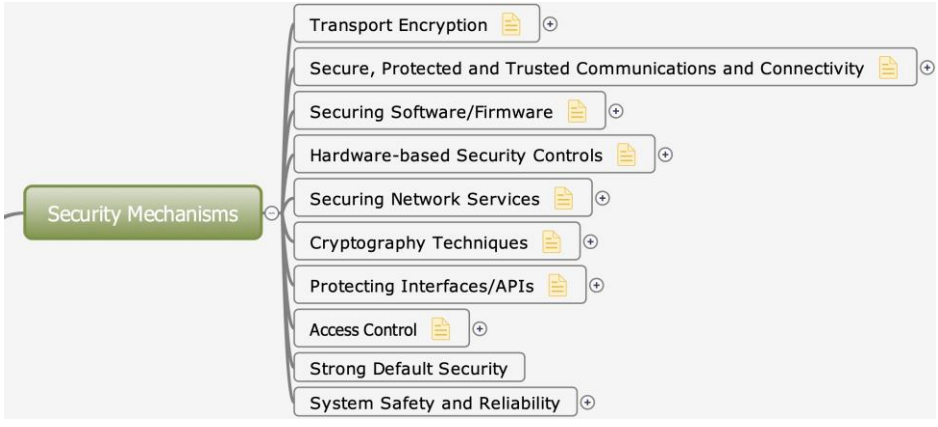


Fig 4 : Security Mechanisms

Framework Explanation

In Figure. 5.1, we present an overview of the security and privacy functionality framework, including the top-level security and privacy concepts. The functionalities are separated into two major parts, the life cycle aspects of a system and the management aspects of security and privacy. The life cycle relates to the different phases in the life of

a system, while the management of security and privacy is the ability to put supporting functionality elements in the system. We believe that awareness about where we are in the life cycle is essential, and makes it easier to apply the right functionalities and how to do the appropriate security and privacy management. We use blue color to distinguish subtopics related to the life cycle of a system from those associated with the management of security and privacy, colored in green. The coloring makes the division clear, and gives a better structure of the framework, separating the two primary concerns. In the following, we describe each part of the framework and the related subtopics. For brevity, we do not expand the whole framework and just mention some of the aspects. For more details and complete expansion of the framework refer to the long version [12]. Security mechanisms - Different security mechanisms are illustrated in Figure. 5.2. Security mechanisms are processes designed to detect, prevent or recover from a security attack in IoT devices, including:

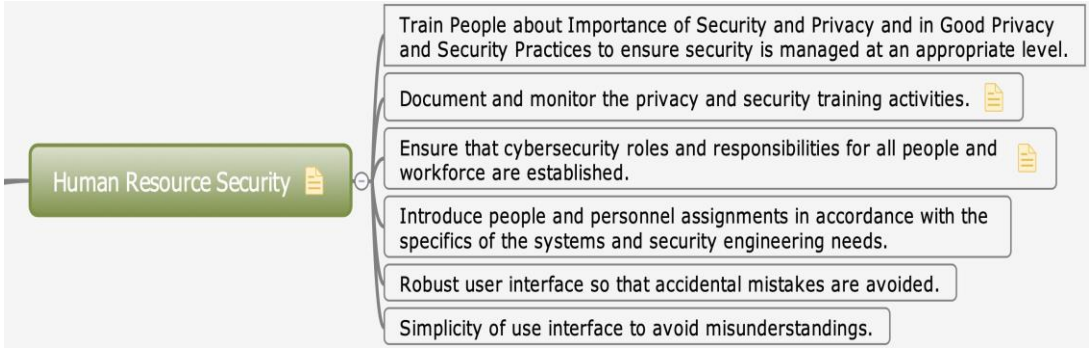


Fig 5 Human resource security

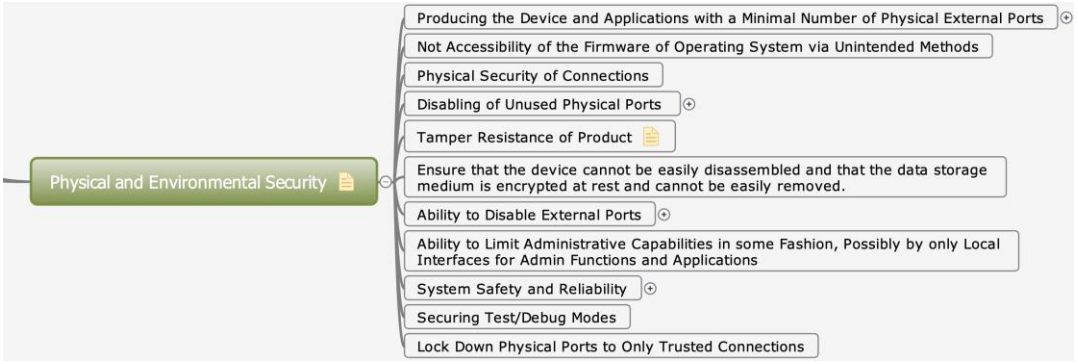


Fig 6 : Physical and environmental security

Fig 7: Privacy protection

- **Secure, protected and trusted communications and connectivity**: This includes information flow protection, standardizing security protocols (i.e., Transport Layer Security (TLS) for encryption) guaranteeing data authenticity, signing data, disabling specific ports and/or network connections for selective connectivity, etc.
- **Hardware-based security controls:** product developers should eval- uate and implement hardware protection mechanisms, including the use of Memory Protection Units (MPUs), considering a Trusted

Platform Module (TPM) into IoT Devices, securing physical inter-faces, tamper protections, etc.

- **Protecting interfaces/application programming interface (APIs):** Interface security is one of the critical tasks when it comes to developing IoT devices. IoT products interact with so many cloudservices, custom-developed smartphone apps and also peer IoT products. If APIs do not protect adequately, service providers might be exposed. APIs must protect adequately against misuse, by techniques like rate-limiting to protect against compromised IoT devices that attempts to flood the service, error handling, embedding time-stamps or counters into messaging to protect against replay attacks, certificate pinning to protect against sensitive data transmission into GET requests, etc.
- **Access control:** only authorized users should have access, applications and services and unauthorized accesses should be prevented,user accountability should be enabled to safeguard their authentication information.

Human resource security - People and contractors should understand the cybersecurity responsibilities suitable for their roles, and be trained about the importance of security and privacy. Further, to avoid misunderstanding, the user interfaces should be simple yet robust enoughto avoid accidental mistakes. See Figure. 5.3.

Physical and environmental security - The objectives of this section include prevention of unauthorized physical access, damage, and interference with IoT's

information and premises, as well as prevention of loss, damage, theft or compromise of assets and interruption to the activities and operations of IoT devices and systems. All the equipment and processing facilities should be placed in secure areas and protected from physical and environmental threats. The functional requirements ofthis matter are listed in Figure. 5.4.

Privacy protection - Personally identifiable information (PII) needs to be protected, according to the European General Data Protection Regulation (GDPR) regulations [30]. Privacy protection is also advisable to increasetrust in the internet.

Operations security - Information processing facilities should ensure correct and secure operation, including protection against attacks. Further, accountability auditing must be enabled for all events to ensure the integrity of operational systems, and prevent against exploitation of technical vulnerabilities.

Decommissioning - The product must be disposed of in a secure manner at the end-of-life period to avoid revealing crucial information to any potential attacker. As a result, no further secure devices should be added to the supply chain. An automated decommissioning approach can give a low-cost and high-guaranteed method of decommissioning.

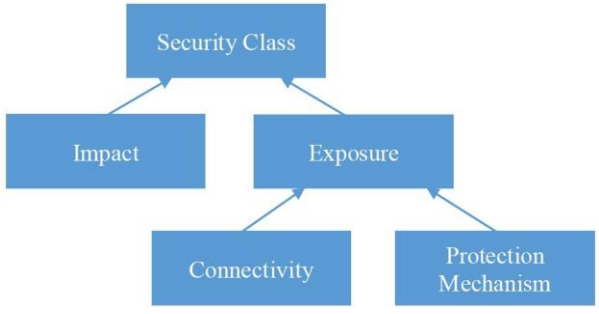


Fig 8 : Basic inputs for defining a security class

3.2.1.2 Communicate Firebase(Db) to Raspberry-pi

The Firebase Real-time Database is a cloud-hosted database. Data is stored as JSON and synchronized in real-time to every connected client. If you want to know more check out.

First things first, you need to create a new project in your console.

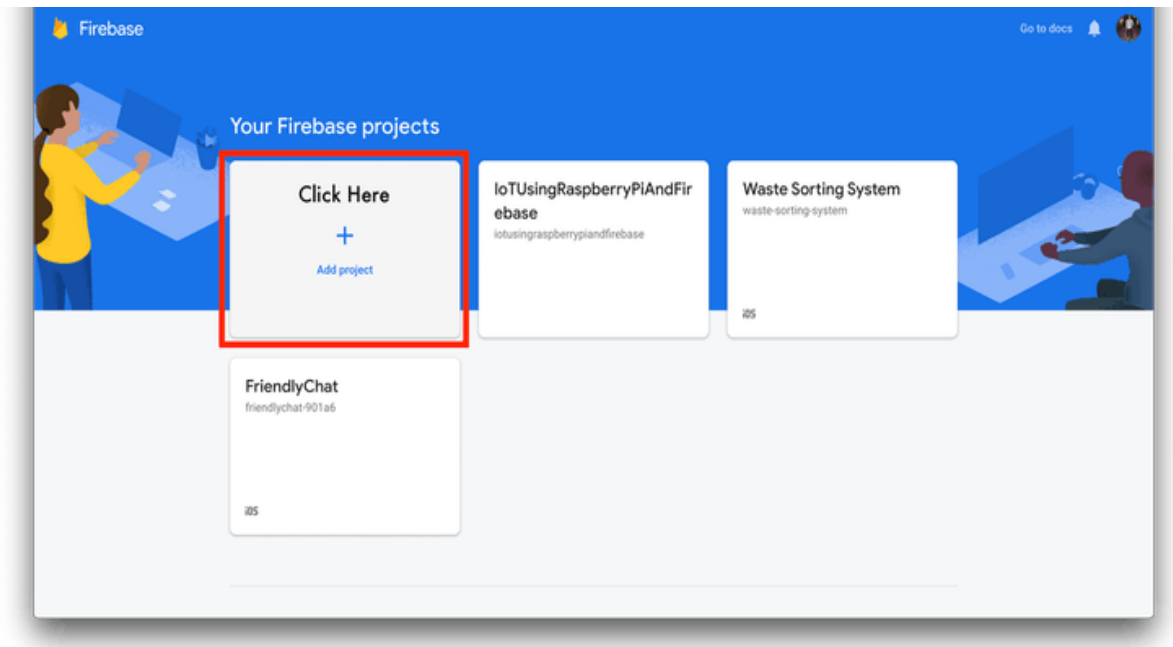


Fig 9: Create Database in Firebase

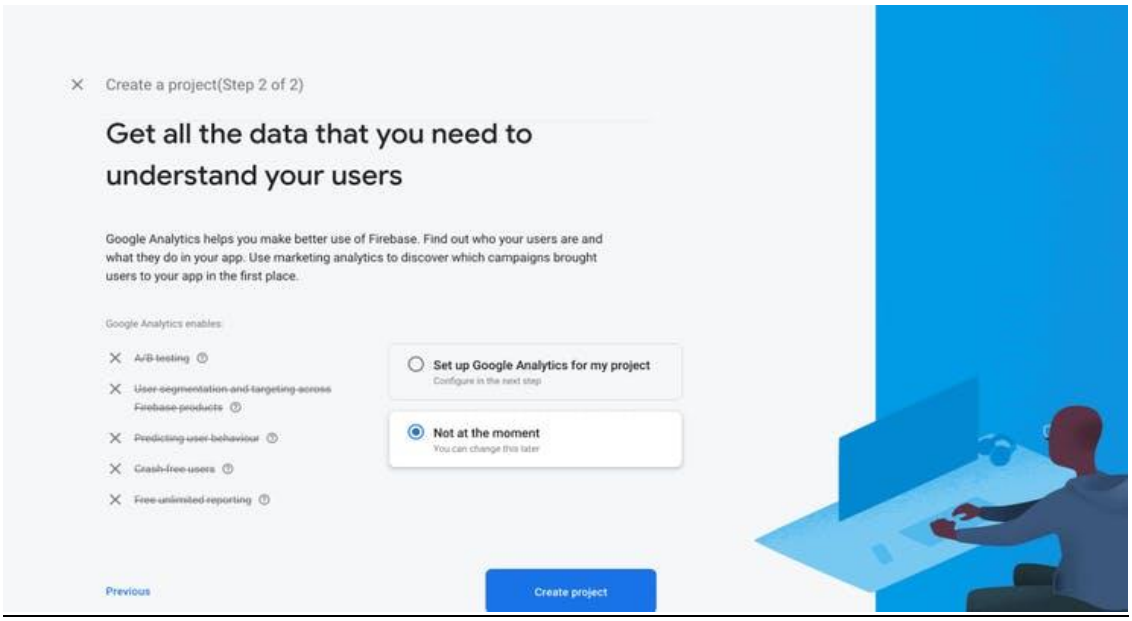


Fig 10: Permission in Firebase

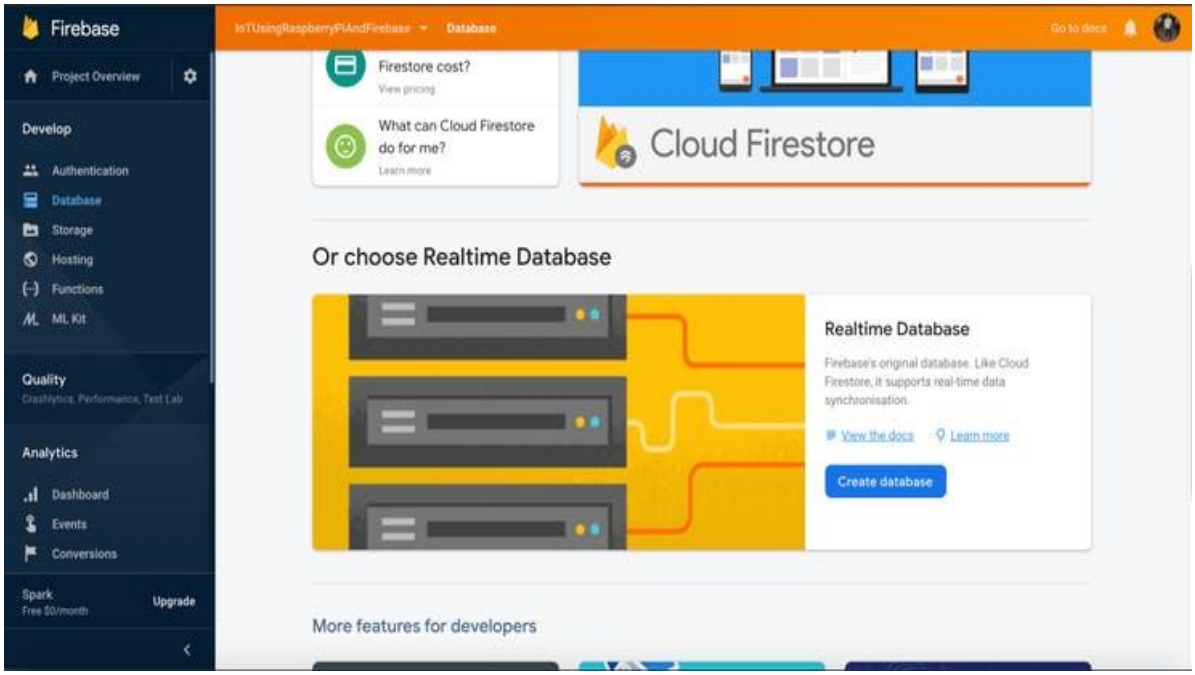


Fig 11: Access Real-time Database in Firebase

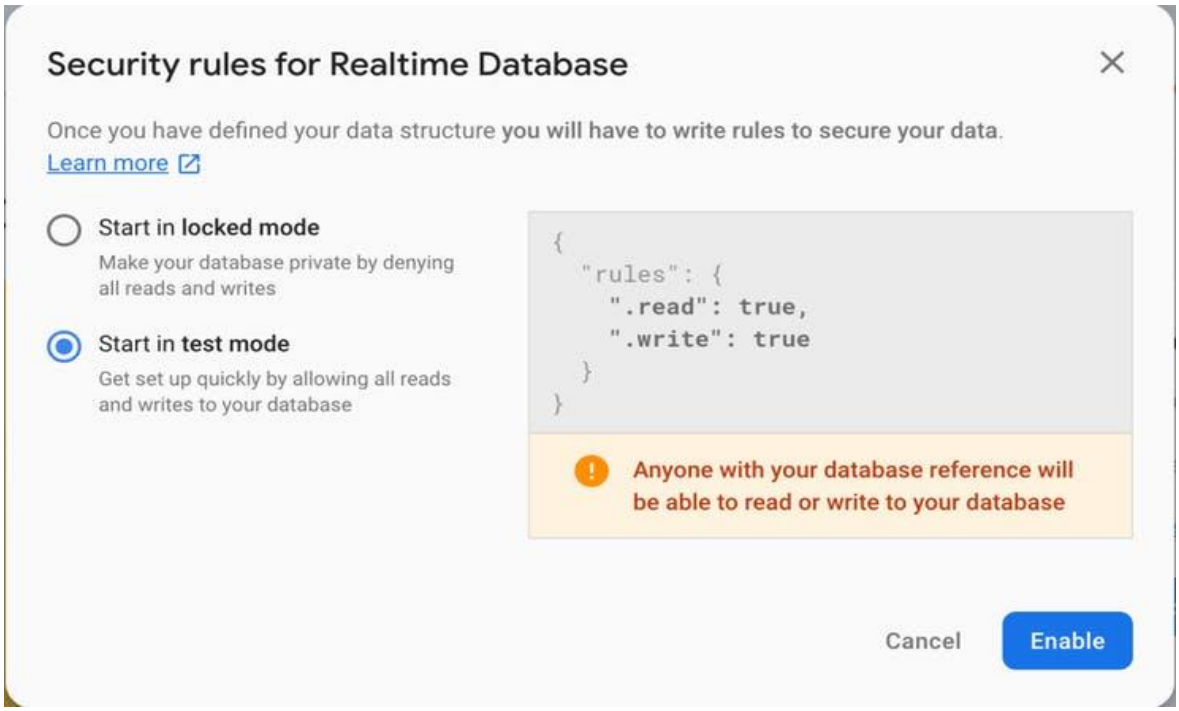


Fig 12: Security for Real-time Database in Firebase

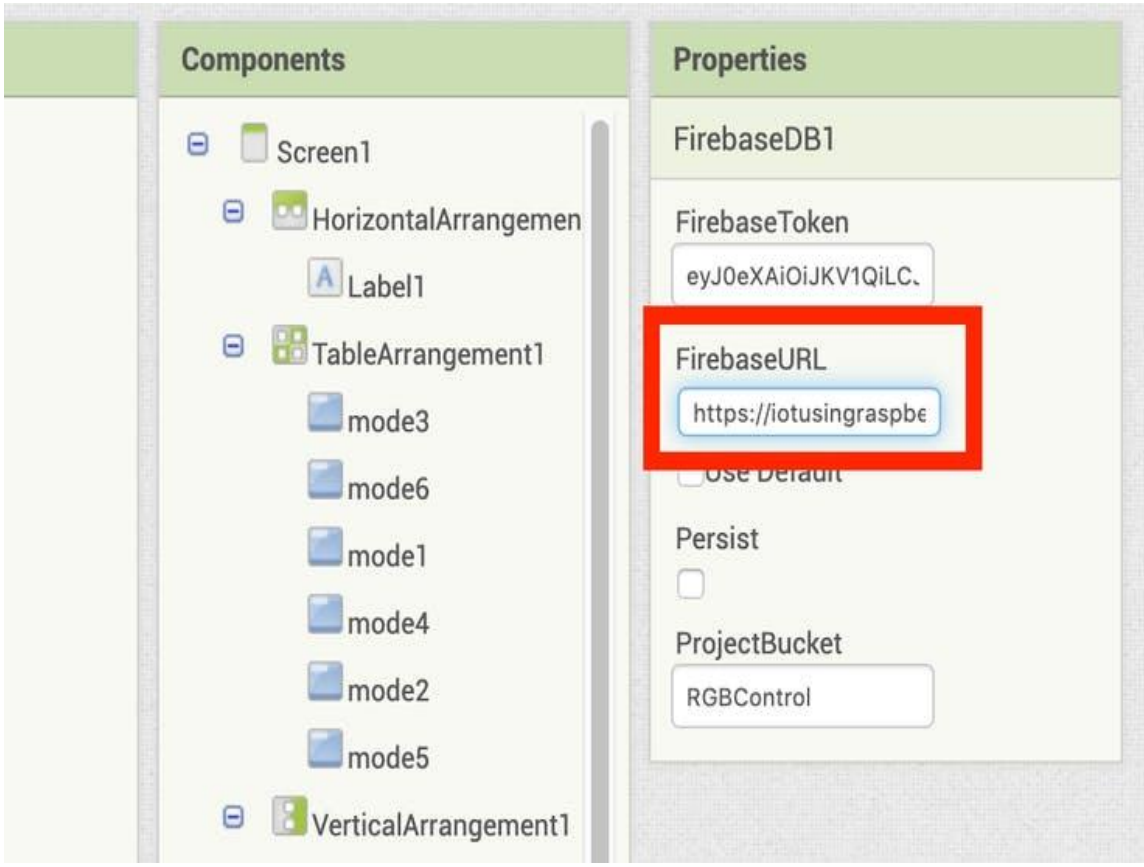


Fig 13: Real-time access data to monitor url for TMC

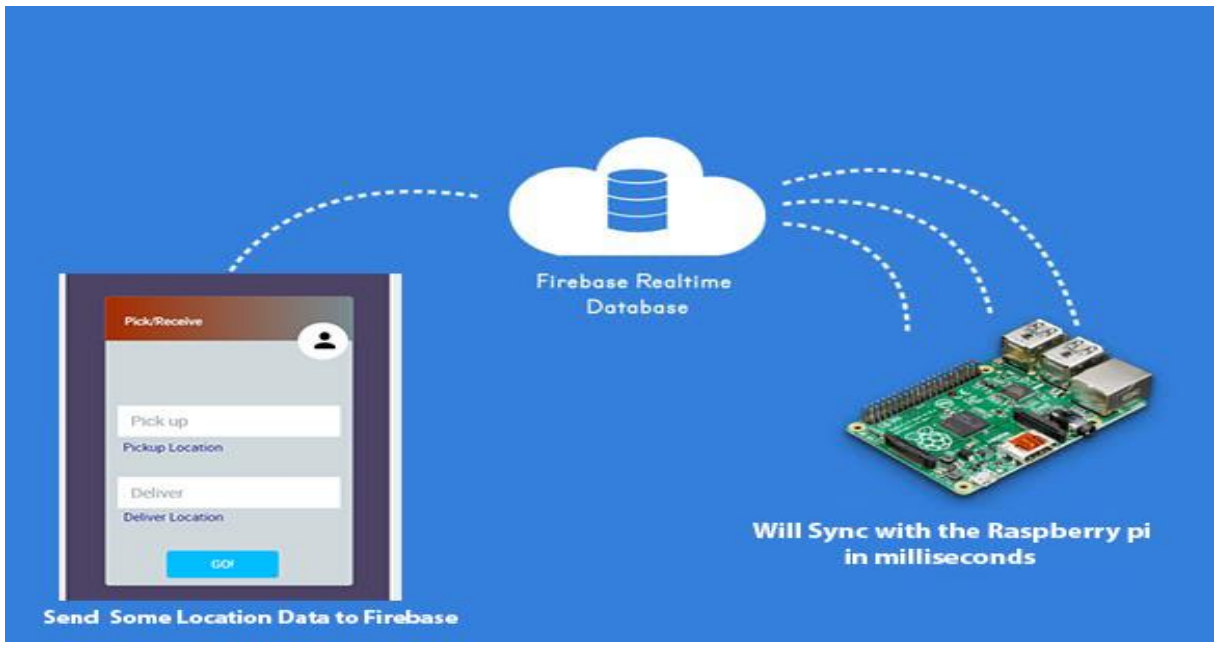


Fig 14: Data Transfer user information to Raspberry pi

CHAPTER 4

IMPLEMENTATION APPROACH

When the patient is in a critical situation, he takes the essential steps to help them.

4.1 Implementation

Firebase Database with Arduino UNO and ESP8266 Module. Storing data (such as sensor data) in a database that can be accessed from anywhere by the Internet can be very useful. Firebase makes it easy to store and retrieve data. This is a better option, which can store the data without any attack and send it from one place to another securely through WiFi. Due to which health service to the patient can be done continuously at home.

In today's medicinal services framework, patients who remain at home after surgery are checked by an overseer or a medical career. This method may not be capable of continuous monitoring, because anything may change in a well-being metric in a matter of seconds, and if a guardian or attendant is not there at the moment, more significant injury can occur. As a result of this invention, a period has been formed in which the web governs the world, and it has been proposed to add to another sharp health awareness framework in which the patient is checked on a regular basis.

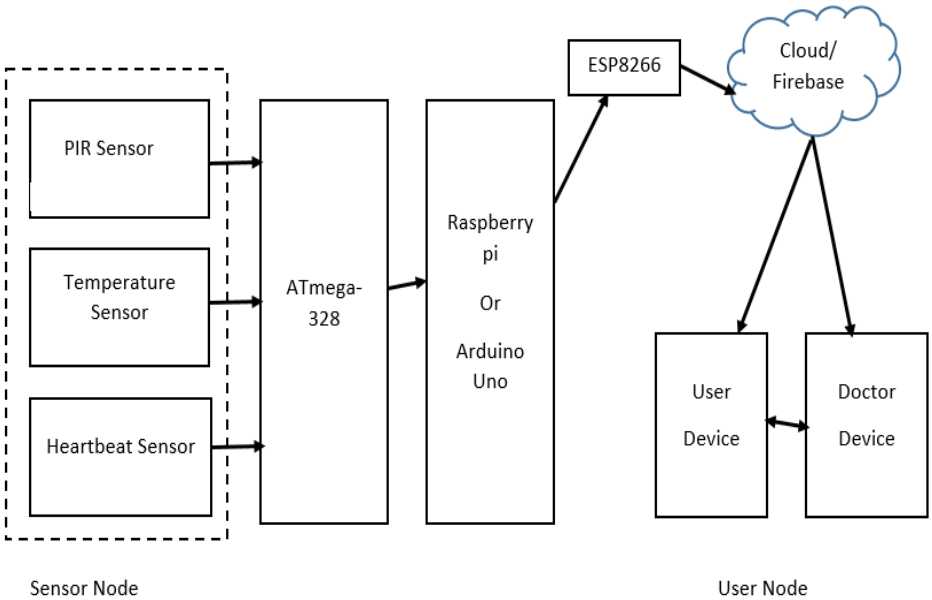


Fig 15 : Proposed Architecture

Spark is a fast and general-purpose cluster computing system for large-scale in-memory data processing. Spark has a similar programming model to Map Reduce but extends it with a data-sharing abstraction called Resilient Distributed Datasets or RDD. A Spark was designed to be fast for iterative algorithms, support for in-memory storage and efficient fault recovery. Spark Core consists of two APIs which are the unstructured and structured APIs. The unstructured API is RDDs, Accumulators, and Broadcast variables.

Objectives used

- **Sensor Node**
- **Cloud/Firebase**
- **User Node**
- This is a user-assistance layer. It is a system that allows users to access sensor

information and assess the state of patients. Client nodes is an Android application that runs on a smartphone. The user (doctor) may get sensor data and receive a push notice if the value exceeds a threshold value, as well as examine different patient details through report in an app.

4.2 Hardware Description

- **Raspberry Pi**
- **ATmega 328**
- **Temperature Sensor**
- **Motion sensor**
- **Pulse/Heart Rate Sensor**
- **ESP8266**

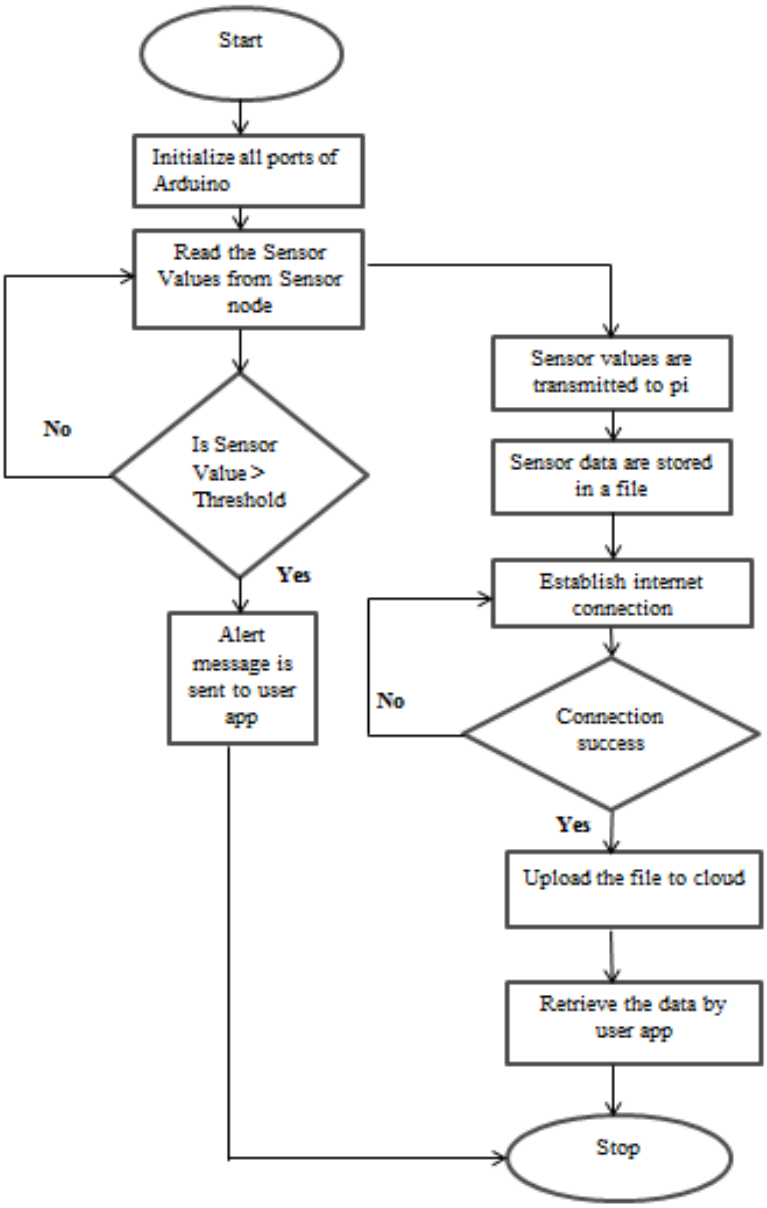
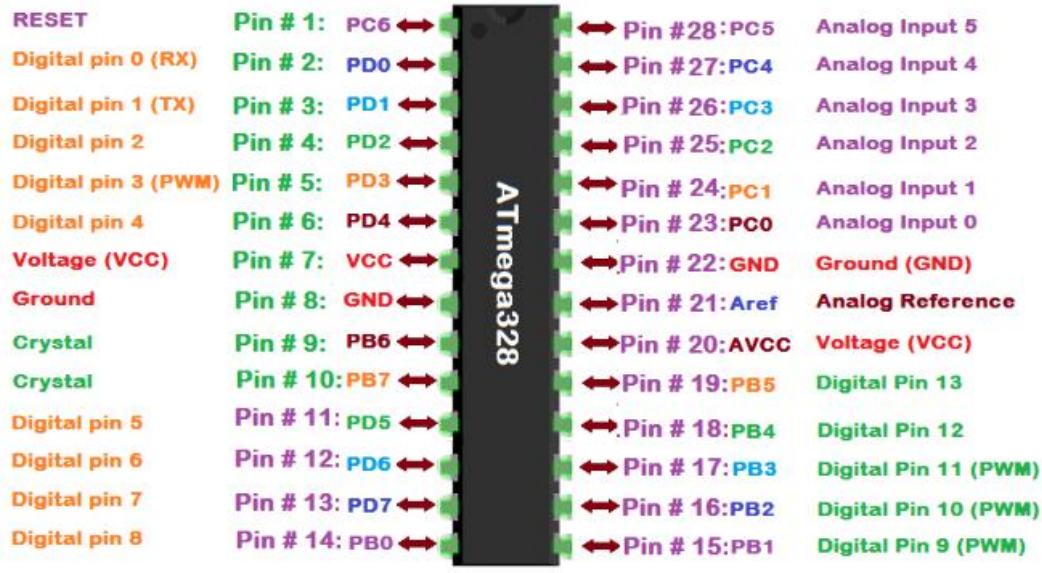


Fig 16 : Work flow module

Fig 17: Raspberry Pi Foundation

S/N.	Label	Voltage	Description
1.	3V3	3.3 volts	Anything connected to these pins will always get 3.3V of power
2.	5V	5 volts	Anything connected to these pins will always get 5V of power
3.	GND	Ground	Zero volts, used to complete a circuit
4.	GP2	GPIO pin 2	These pins are for general-purpose use and can be configured as input or output pins
5.	ID_SC/ID_SD/ DNC	Special purpose pins	

Table 1: Raspberry Pi Voltage Details



Sensor Node Sensor node consists of various sensors that are used to sense the physiological parameters like temperature, heartbeat rate, and movement. These sensed signals are sent to ATmega-328, which will convert the analog signals into digital signals, these values are transmitted to the Raspberry-pi to update the data continuously to cloud. temperature sensor is used to sense the temperature. PIR sensor is a device that detects motion of a patient. Heart beat sensor is designed to give digital output of heart beat when a finger is placed on it.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over the network (mainly the Internet). Cloud has abundant processing power, large amount of storage which can be scaled according to application needs. Modern technology is being shifted to Cloud based platform as it is suited for long-term data storage. For the implementation of proposed system, cloud storage such as Dropbox is used. Dropbox gives enough space to back up all the files and with a simple admin interface for adding new users.

User Node This is a user support layer. It is a platform from where user can access sensor data and can analyze the patient's condition. User node is an android app in an android phone. User (doctor) is able to receive the sensor data, and gets the push notification if the sensor value exceeds the threshold value and also different patient details can be viewed via report in an app.

Arduino Uno: Arduino Uno is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as

PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The detailed description of the arduino board is shown in the Figure 3. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform. Some of the key features of the Arduino Uno include: • An open source design. The advantage of it being open source is that it has a large community of people using and troubleshooting it. • An easy USB interface. The chip on the board plugs straight into the USB port and registers on to computer as a virtual serial port. This allows to interface with it as through it were a serial device. The benefit of this setup is that serial communication is an extremely easy (and time tested) protocol, and USB makes connecting it to modern computers really convenient. • An on-board LED attached to digital pin 13 for fast an easy debugging of code.

4.2 Other Methods:

4.2.1 **Temperature Sensor**: Temperature sensor is a device which senses variations in temperature across it. LM35 is a basic temperature sensor that can be used for

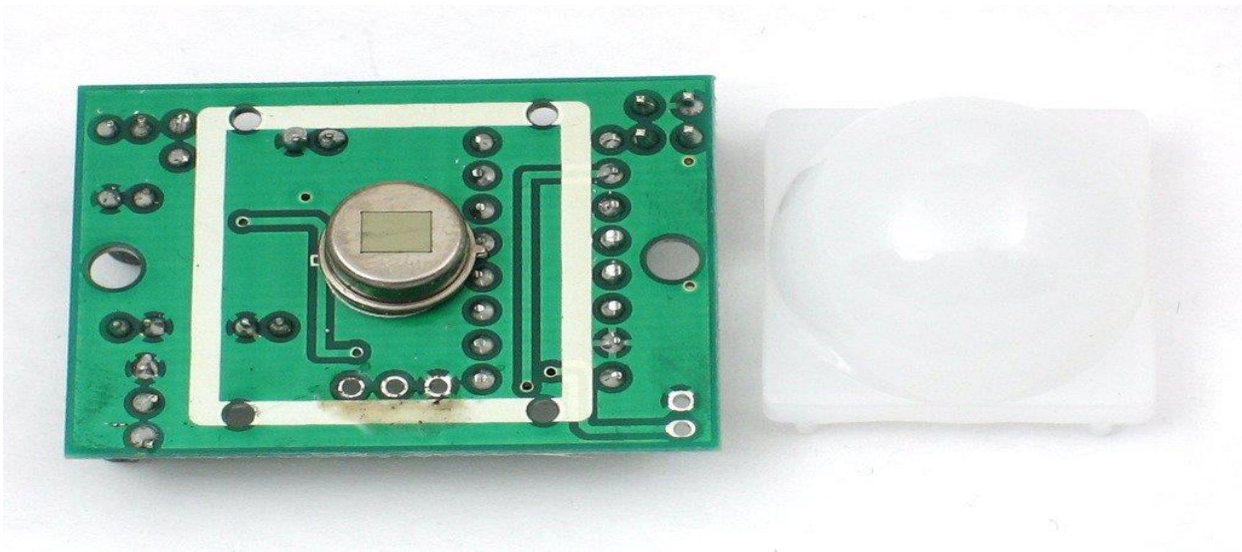
experimental purpose. It give the readings in centigrade (degree Celsius). The LM35 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature. It Operates from 4 to 30 volts and has less than 60 Micro ampere current drain. The temperature sensor can be viewed as shown in the Figure 5. The circuit connections are made as follows: • Pin 1 of the LM35 goes into +5V of the Arduino. • Pin 2 of the LM35 goes into analog pin A0 of the Arduino. • Pin 3 of the LM35 goes into ground (GND) of the Arduino

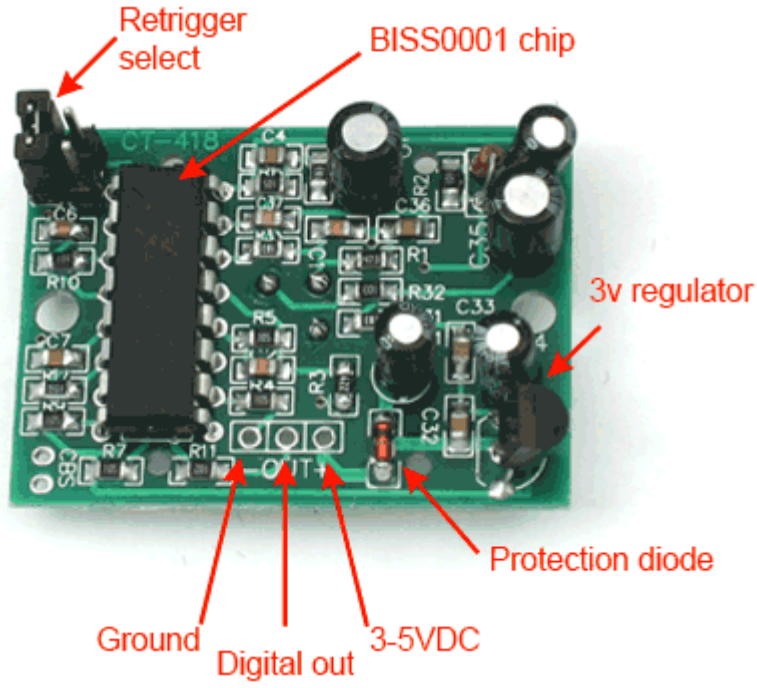
4.2.2 **Motion Sensor:** PIR sensors allows to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. They are small, inexpensive, low-power, easy to use and don't wear out. For that reason they are commonly found in appliances and gadgets used in homes or businesses. They are often referred to as PIR, "Passive Infrared", "Pyroelectric", or "IR motion" sensors. The PIR (Passive Infra-Red) Sensor is a pyroelectric device that detects motion by measuring changes in the infrared levels emitted by surrounding objects. This motion can be detected by checking for a high signal on a

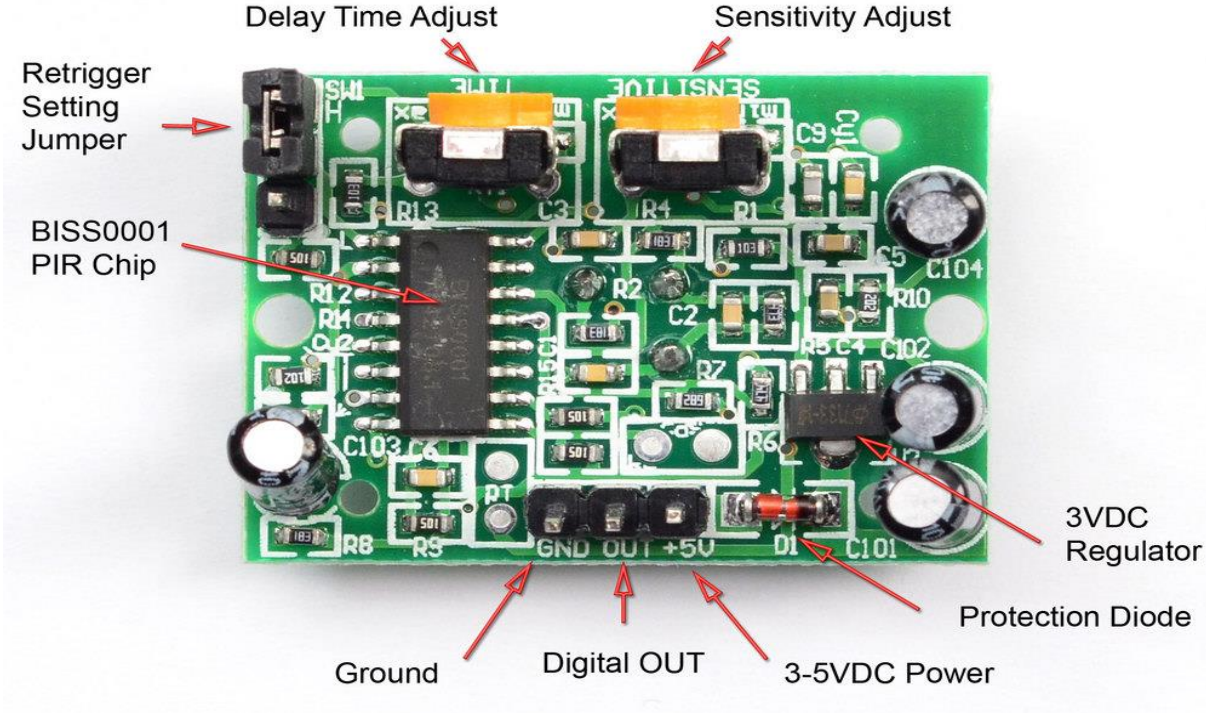
single I/O pin A PIR detector combined with a Fresnel lens are mounted on a compact size PCB together with an analog IC,SB0081, and limited components to form the module. High level output of variable width is provided. The PIR sensor has a detection range, ranging from 2-3meters. Supply voltage of 3-5v.Current drain is less than 50uA Temperature ranges from -15C to +70C. The PIR sensor back view and front view.

4.2.3 **Temperature Sensor:** A temperature sensor is a device that detects and measures hotness and coolness and converts it into an electrical signal. At TE Connectivity (TE), we design and manufacture a broad portfolio of temperature sensors – including our NTC thermistors, RTDs, thermocouples, and thermopiles – designed for efficiency and easy installation, with capacity to reliably integrate technology that responds to human behavior.

4.2.3 PIR sensors: Allow you to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. They are small, inexpensive, low-power, easy to use and don't wear out. For that reason they are commonly found in appliances and gadgets used in homes or businesses. They are often referred to as PIR, "Passive Infrared", "Pyroelectric", or "IR motion" sensors.

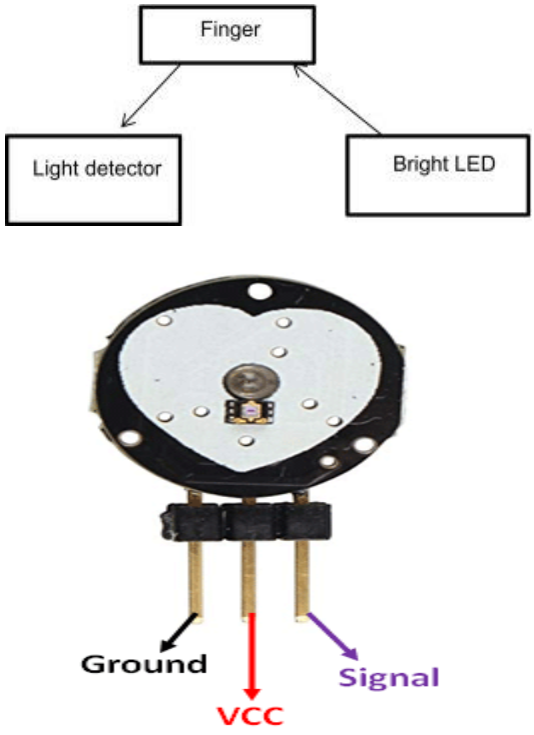



Retrigger
select
BISS0001 chip
3v regulator
Protection diode
Ground
Digital out
3-5VDC


Delay Time Adjust
Sensitivity Adjust
Retrigger
Setting
Jumper
BISS0001
PIR Chip
3VDC
Regulator
Protection Diode
Ground
Digital OUT
3-5VDC Power

4.2.4 Pulse/Heart Rate: Pulse/heart rate is the wave of blood in the artery created by contraction of the left ventricle during a cardiac cycle.

4.2.5 Sensor Heart rate is the speed of the heartbeat measured by the number of contractions of the heart per minute (bpm). The heart rate can vary according to the body's physical needs, including the need to absorb oxygen and excrete carbon dioxide. It is usually equal or close to the pulse measured at any peripheral point. Activities that can provoke change include physical exercise, anxiety, sleep, stress, illness, and ingestion of drugs. Many texts cite the normal resting adult human heart rate range from 60 to 100 bpm. Tachycardia is a fast heart rate, defined as above 100 bpm at rest. Bradycardia is a slow heart rate, defined as below 60 bpm at rest. Several studies, as well as expert consensus indicates that the normal resting adult heart rate is probably closer to a range between 50 to 90 bpm. During sleep a slow heartbeat with rates around 40 to 50 bpm is common and is considered normal. When the heart is not beating in a regular pattern, this is referred to as an arrhythmia. Abnormalities of heart rate sometimes indicate disease.



Pulse Sensor is a well-designed plug-and-play heart-rate sensor for Arduino. It can be used by students, artists, athletes, makers, and game and mobile developers who want to easily incorporate live heart rate data into their projects. The sensor clips onto a fingertip or earlobe and plugs right into Arduino. The front and back view of the heartbeat sensor. The Pulse Rate Sensor should be connected to Uno as follows:

• Signal(S) to A0 • Vcc(+) to 5V • Gnd(-) to Gnd

The methods for implementing the system is detailed in this section. While realizing the system in a sequential fashion, the sensor node, cloud, and end user device will all come into play. The data is captured by the sensor node and sent to the cloud,

where it is received by the user node. All of the Arduino's detected signals are transferred to the Raspberry Pi through serial connection. A python programme is run on the Raspberry Pi, and the results are shown in the Python shell. Dropbox cloud storage is employed in this system, and in order to access it, an account is formed that produces a key. For authentication to upload and download data, paste this Dropbox key into the Pi code. The URL created as output in the python shell is passed to the dropbox developers, and an access token is generated in the dropbox developers, which is copied to the output window. On the Pi desktop, the sensor output is shown, and the same data is saved in a file. The identical file will be uploaded to cloud storage whenever an internet connection is established. The user App retrieves sensor data from the cloud. If the sensor value exceeds the threshold value, it also receives a push notice.

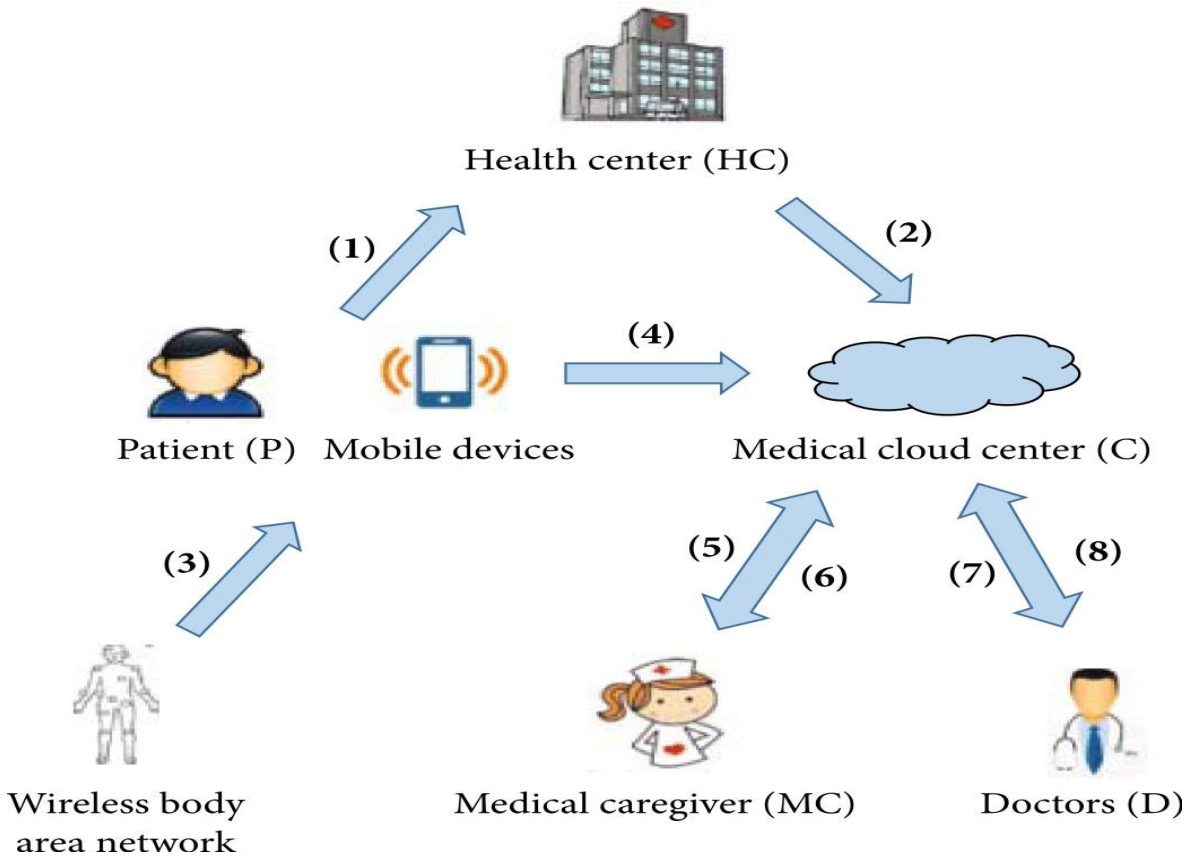


Fig 18: Architecture of cloud-assisted wireless body area network in mobile emergency medical care system.

Figure shows a safe authentication and key agreement technique for a cloud-assisted WBAN system based on extended chaotic maps. Before being sent, the health data acquired by WBAN's body sensors will be encrypted. The monitored patient can permit medical caregivers to access his or her health things saved in the cloud in order to provide real-time analysis with continuous remote monitoring on stream-oriented health items, which not only offers home care but also enhances life quality. The suggested approach may successfully handle the difficulty of participant authentication in mobile emergency medical care systems, according to security and performance studies.

Data Encryption

Cryptography is a security system for exchanging information and communicate. The encryption technique converts plaintext, also known as the original message, into ciphertext, as seen in below Figure. The message is sent from the sender to the receiver through the public channel. After that, the communication is encrypted and converted to plaintext.

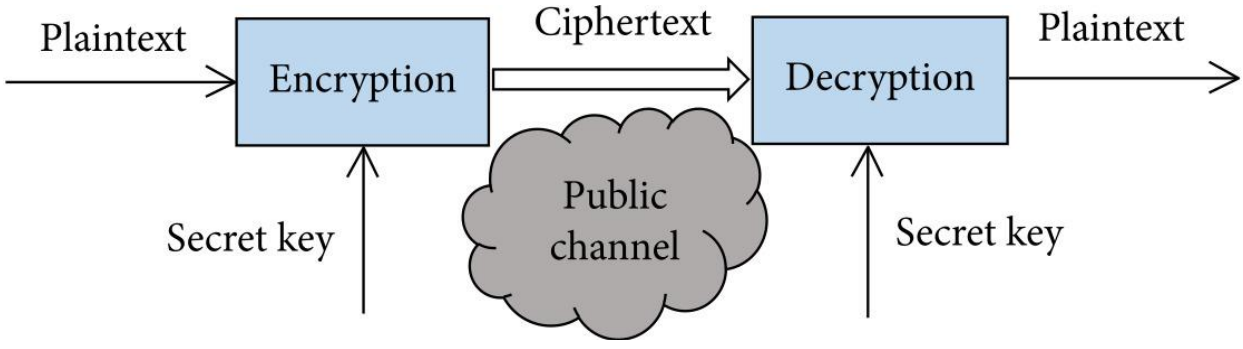


Fig 19 : Common model of data encryption and decryption.

CHAPTER 5

RESULT

The Future work of the project is very essential in order to make the design system more advanced. In the designed system the enhancement would be connecting more sensors to internet which measures various other health parameters and would be beneficial for patient monitoring i.e. connecting all the objects to internet for quick and easy access. Establishing a Wi-Fi mesh type network to increase in the communication range.

Compare Previous and our proposed method ESP-IOT-CBHCS for Cost, accuracy, sensitivity.

This study proposes ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM infrastructure. This involves in monitoring the patient health from remote area.	Machine learning can be used to analysis the ECG data instead of manual monitoring. This helps to unsupervised the process and also involves in reducing the cost.	Average response time of 50 request is 45 ms Measure is approximately 97.0 when the number of clusters is 2 Accuracy
The voice signal is represented using the local binary pattern (LBP) on a Mel-spectrum representation of the voice signal	Scalability can be further increased by using the smart devices, and microphone This method doesn't involve in handling large amount of data	Accuracy LBP + ELM = 90.1% and LBP + GMM = 95.7%
The framework transfers ECG and other data related to the healthcare professionals. Monitoring is based on the mobile devices and sensors	Machine learning can be applied to monitor the signal and involves in reducing errors and increases the accuracy Extracting more features from the data involves in increasing the execution time	PSNR: existing = 58.38 and proposed = 64.35 Classification accuracy: While extracting 37 features = 91.1% Execution time: while using three instance server = 3.3 ms
IoT messages are encrypted using the IoT group key and shared to the patient.	Flexibility and scalability are need to be increased	When number of attributes is 60, Encryption cost = 0.025 s and access policy update query cost = 0.0011 s
This research involves in solving the complexity and heterogeneity of data in IoT by tracing the data back to the router using Petri Nets	This method needs to develop an unsupervised model to process in the real-time system effectively	Accuracy = 86%, sensitivity = 91%, and precision = 94%

We can connect to all the other branches of the concerned hospital and thus the critical patient's data can be sentand observed for better treatment. Healthcare costs can be reduced because issues can be addressed before they become acute, which could lead to fewer hospital visits. It will be easier for relatives and other remote caregivers to keep track of their relative's health from a distance. In the home we will guide one educatedperson instead of doctor about treatment with respect to basic medicine when the sensor value reaches greater than threshold value. Instead of medical application we can use our system in industrial and agricultural application by using sensors like humidity sensors, fertility check sensors, and many more.

CHAPTER 6

CONCLUSION

The project Remote Patient Monitoring System is a telemedicine application which allows the doctor to view the patient's vital signs and parameters remotely and dynamically in real time. A smartphone-based health monitoring system has been presented in this project. By using the system, the healthcare professionals can monitor, diagnose, and advice their patients all the time. The physiological data are stored and published online. Hence, the healthcare professional can monitor their patients from a remote location at any time. The system is power efficient, cost effective, flexible and robust solution supporting a unique mobile based computational platform. It is easy to use, fast, accurate, high efficiency, and safe (without any danger of electric shocks).

In this project, the realized system can be a prototype for health care system to monitor patient's health status continuously. The system is comprised of low-power profile sensors to measure various physiological parameters of the patient. Raspberry pi is used for this application because of its multi-tasking capability and low power consumption. Dropbox is used for cloud storage. Also, this system can be installed easily in all the hospitals and huge data obtained can be stored in the database, which are very much valuable. Even the results can be made to be accessed from mobile through an application. In contrast to other conventional medical equipment, this system has the ability to save data for future reference. Finally, the reliability and validity of thissystem have been ensured via field tests. The field tests show that our system can produce medical data that are similar to those produced by the existing medical equipment.

REFRENCES

[1] Megha Koshti, IoT Based Health Monitoring System by using Raspberry Pi and ECG signal, M.E. Student, Department of ENTC (VLSI and EMB), Genba Sopanrao Moze College of Engineering, *Balewadi, Pune, Vol 5, May 2016.*

[2] Dr.M.Pallikonda Rajasekaran , R.Kumar, An IOT Based Patient Monitoring System Using Raspberry Pi, Department of Electronics and Communication Engineering, *Kalasalingam University Tamilnadu, India , April 2010.*

[3] Branko Perii, A Custom Internet of Things Healthcare System, Faculty of Technical Sciences *University of Novi Sad, Serbia, March 2013.*

[4] Pooja Navdeti , Patient Parameter Monitoring System using Raspberry Pi, International Journal Of Engineering And Computer Science, *ISSN:2319-7242 , Volume 5 ,Issue -03, pp:16018-16021, March 2016.*

[5] Adivarekar JS, Chordia AD, Baviskar HH, Aher PV, Gupta S. Patient Monitoring System Using GSM Technology, International journal of mathematics and Computer Research, *March 2013.*

[6] Purnima, Neetu Rout and Rahul Tiwary , International Journal of Advanced Researchin Electrical, Electronics and Instrumentation Engineering, *Vol. 3, Issue 1 , January 2014.*

[7] Mendrela Biswas, Rupali S. Landge and Bhagyashree A. Mahajan, Raspberry Pi Based Patient Monitoring System using Wireless Sensor Nodes, *Volume 3, Issue: 04, Apr- 2016.*

[8] Junaid Mohammed, Abhinav Thakral, Adrian Filip Ocneanu, Colin Jones,

ChungHorng Lung, Andy Adler, Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing, IEEE International Conference on Internet of Things (iThings 2014) Green Computing and Communications (GreenCom2014) and Cyber-Physical, *pp:256-263, 2014.*

Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019, 8, 768. [CrossRef]

[9] Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A Secure Framework for IoT-Based Healthcare System. In Proceedings of the International Ethical Hacking Conference 2018, Kolkata, India, 5 October 2018; Advances in Intelligent System and Computing. Chakraborty, M., Chakrabarti, S., Balas, E.V., Mandal, J.K., Eds.; Springer Nature: Singapore, 2019; Volume 811, pp. 383–393.

[10] Nandyala, C.S.; Kim, H. From Cloud to Fog and IoT-Based Real-Time U-Healthcare Monitoring for Smart Homes and Hospitals. Int. J. Smart Home 2016, 10, 187–196. [CrossRef]

[11] Maksimovi´c, M. Improving computing issues in the Internet of Things driven e-health systems. In Proceedings of the International Conference for Young Researchers in Informatics, Mathematics, and Engineering, Kaunas, Lithuania, 1 April 2017; Volume 1852, pp. 14–17.

[12] Yeh, K.H. A Secure IoT-Based Healthcare System with Body Sensor Networks. IEEE Access 2016, 4, 10288–10299. [CrossRef]

[13] Deelip, S.A.; Sankpal, S.V. IOT based Smart and Secure Health Care System

Analysis & Data Comparison. Int. J. Res. Appl. Sci. Eng. Technol. 2020, 8, 394–398.

[14] Sanjay, S.; Shekokar, N. Toward Smart and Secure IoT Based Healthcare System. In Internet of Things, Smart Computing and Technology: A Roadmap Ahead, Studies in Systems, Decision and Control; Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V., Hassanien, A.E., Eds.; Springer Nature AG: Cham, Switzerland, 2020; Volume 266, pp. 283–303.

[15] Farahani, B.; Firouzi, F.; Charkabarty, K. Healthcare IoT. In Intelligent Internet of Thing, From Device to Fog and Cloud; Firouzi, F., Chakrabarty, K., Nassif, S., Eds.; Springer Nature AG: Cham, Switzerland, 2020; pp. 515–537.

[16] Abouelmehdi, K.; Beni-Hssane, A.; Khaloufi, H.; Saadi, M. Big data security and privacy in healthcare A Review. Procedia Comput. Sci. 2017, 113, 73–80. [CrossRef]

[17] Connor, Y.O.; Rowan, W.; Lynch, L.; Heavin, C. Privacy by design informed consent and internet of things for smart health. Procedia Comput. Sci. 2017, 113, 653–658.

[18] Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput. Commun. 2020, 153, 311–335. [CrossRef]

[19] Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. J. Ind. Inf. Integr. 2020, 18, 100–129. [CrossRef]

[20] Ray, P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Syst. J.

2020, 2020, 1–10. [CrossRef].

[21] Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review. Wirel. Commun. Mob. Comput. 2019, 2019, 1–20. [CrossRef].

[22] Semantha, F.H.; Azam, S.; Yeo, K.C.; Shanmugam, B. A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics 2020, 9, 452. [CrossRef]

[23] Wu, J.; Tian, X.; Tan, Y. Hospital evaluation mechanism based on mobile health for IoT system in social networks. Comput. Biol. Med. 2019, 109, 138–147. [CrossRef]

[24] Khatoon, N.; Roy, S.; Pranav, P. A survey on Applications of Internet of Things in Healthcare. In Internet of Things and Big Data Applications. Intelligent Systems; Khatoon, N., Roy, S., Pranav, P., Eds.; Springer Nature: Cham, Switzerland, 2020; Volume 180, pp. 89–106.

[25] Tuli, S.; Basumatary, N.; Singh-Gill, S.; Kahani, M.; Chand-Arya, R.; Wander, G.; Buyya, R. HealthFog: An ensemble deep learning-based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Gener. Comput. Syst. 2020, 104, 187–200. [CrossRef] Symmetry 2020, 12, 1191 32 of 35

[26] Gupta, P.; Pandy, A.; Akshita, P.; Sharma, A. IoT based Healthcare Kit for Diabetic foot Ulcer. In Proceedings of the ICRIC 2019, Jammu, India, 8–9 March 2019; Lecture Notes in Electrical Engineering. Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S., Eds.; Springer Nature: Cham,

Switzerland, 2019; Volume 597, pp. 15–22.

[27] Elmisery, A.M.; Rho, S.; Aborizka, M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Clust. Comput. 2017, 22, 1611–1638. [CrossRef]

[28] Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. IEEE Trans. Ind. Inform. 2018, 14, 1656–1665. [CrossRef]

[29] Shirley, M.A.J.; A, M.C.; Phil, M.; Ed, M. A cloud IoT based smart patient health monitoring system. Adalya J. 2020, 9, 963–968.

[30] Khader, A.H.A.; Subasri, K. Fog Assisted-IoT Enabled Patient Health monitoring. Adalya J. 2020, 9, 525–530.

[31] Swaroop, K.N.; Chandu, K.; Gorrepotu, R.; Deb, S. A health monitoring system for vital signs using IoT. Internet Things 2019, 5, 116–129. [CrossRef]

[32] Wilt, T.; Versluis, A.; Goedhart, A.; Talboom-Kamp, E.; van Delft, S. General practitioners' attitude towards the use of eHealth and online testing in primary care. Clin. eHealth 2020, 3, 16–22. [CrossRef]

[33] Kang, J.J.; Larkin, H. Intelligent personal health devices converged with IoT networks. J. Mob. Multimed. 2017, 12, 197–212.

[34] Wang, X.; Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Gener. Comput. Syst. 2020, 112, 320–329. [CrossRef]

[35] Yamin, M. IT applications in healthcare management: A survey. Int. J. Inf. Technol. 2018, 10, 503–509. [CrossRef]

[36] Mohammed, D.; Meri, A. IoT Service Utilization in Healthcare. In Internet of Things (IoT) for Automated and Smart Applications; Ismail, Y., Ed.; IntechOpen: London, UK, 2019; pp. 1–27.

[37] Cha, S.; Hsu, T.; Xiang, Y.; Yeh, K. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. IEEE Internet Things J. 2019, 6, 2159–2187. [CrossRef]

Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions. IEEE Commun. Mag. 2017, 55, 26–33. [CrossRef] 40. Mohanty, M.N.; Das, S. Advances in Intelligent Computing and Communication. In Lecture Notes in Networks and Systems Proceeding of ICAC 2019; Springer Nature Singapore Pte Ltd.: Singapore, 2020

ANNEXURE

ANNEXURE 1 : PUBLISHED PAPER

Link :

https://ijariie.com/FormDetails.aspx?MenuScriptId=215413

ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM

Deepika Dhawan
Department of Computer Science and Engineering,
Integral University, Lucknow.
Faiyaaz Ahmad
Assistant Professor Department of Computer Science and Engineering
Integral University, Lucknow.

Abstract

one of humanity's greatest difficulties is health. In the recent decade, healthcare has gotten a lot of attention. Not just for sensory equipment, but also for communication, recording, and display equipment, technology plays a significant role in healthcare. It is critical to keep track of numerous medical markers as well as the post-operative days. As a result, the most recent trend in healthcare communication methods utilizing the Internet of Things (IoT) has been adopted. Due to its superior technology, the patient monitoring system has recently become one of the most significant advancements. At this time, a modern strategy is required. The underlying issue with the old technique is that in severe cases, health care experts must be present at the patient's location at all times to check symptoms on a frequent basis. To overcome this issue, health professionals must design a dependable patient monitoring system that allows them to monitor their patients remotely. The project is a wireless health monitoring system based on mobile devices that may deliver real-time online information on a patient's physical status. The Raspberry Pi is employed as an important element of the processing in this project, as are sensors like as temperature, pulse/heart rate, and PIR. These sensors are wired to an Arduino board, and reads the sensor readings and sends them to the Raspberry Pi through serial connection. The sensor data is now saved in a file on the Pi, which is then transferred to the cloud over the Internet. Finally, this uploaded data is retrieved through the user app. The same data is then transferred to the patient and doctor via Firebase to further improve treatment by obtaining patient information in a timely manner.

Keywords *-- Health Care System, Raspberry Pi board; Heartbeat sensor, Temperature sensor; Cloud; Internet of things, Esp8266.*

I. INTRODUCTION

The Internet of Things (IoT), which uses a number of interconnected devices and networks to deliver digital solutions and monitoring systems across healthcare systems, is a game-changing technology in this field. Security is a significant concern in the creation of an IoT-based healthcare system since it deals with sensitive and secret patient information.

The internet has a significant influence on our day-to-day lives in a variety of ways. The basic idea behind this widely acknowledged technology is to link items to the Internet in a simple and effective manner. When items or devices are connected to the Internet, users may access and control them from anywhere in the world. These gadgets may also be operated with the help of computers, which allows users to configure the device [1],[4]. Under certain situations, the gadgets can conduct a series of operations. To communicate, these gadgets use sensors, microcontrollers, and transceivers. Military, business, healthcare, retail, and transportation are some of the most common uses of wireless communication networks.

These networks can be wired, cellular, or ad hoc. In society and industry, wireless sensor (WSNs), actuator networks, and vehicle networks have all attracted a lot of interest. The rising use of Internet of Things (IoT) gadgets and IoT networks in recent years has made them vulnerable to different security assaults. To provide confidentiality, authentication, access control, and integrity, among other things, effective security and privacy

protocols must be deployed in IoT networks. A complete assessment of security and privacy problems in IoT. Is presented in this research. Unfortunately, the bulk of these devices and apps are not built to withstand security and privacy attacks, resulting in a slew of security and privacy vulnerabilities in IoT networks, including confidentiality, identification, and integrity of data, access control, and secrecy[2]. Information security is a concern for both cloud consumers and cloud service providers. Because there is a risk of cloud-based attacks that compromise security features such as confidentiality, availability, and integrity. Intrusion Detection Systems (IDS) are used to improve the system's security and resilience to both internal and external threats. The basic objective of an intrusion detection system is to identify an intrusion and, if required or practicable, to take steps to eliminate it. There are primarily two approaches for detecting intrusions [3].

II. LITERATURE REVIEW

Several attempts have been undertaken in the domain of IoT data processing and storage. Some existing relevant work in the area of IoT data protection in the cloud service may be summarized as follows:

Health is a fundamental capability that people require to properly sense, feel, and act, and as such, it is a key step in the development of both the individual and the environment in which they live [3]. As a result, proper ways and means must be provided to enable optimal health care based on parameter monitoring and direct provision of medical aid.

Development and application of new technologies, particularly internet Online and Wireless also known as internet of Things (IoT), offer a worldwide framework for the development of health care system infrastructure [5][2]. This results in an e-health system that provides a vital set of information to all participants (patients, nursing and medical personnel, and health insurance companies) in real time, regardless of their current location. In many circumstances, real-time model parameters are not accurately recorded in clinics and hospitals, making it difficult for hospitals to monitor patients' health status on a regular basis. Constant monitoring of ICU patients is also impossible.

This method is useful in dealing with problems like these. This project is intended for use in hospitals to monitor and measure different characteristics such as temperature, heart rate, and movement. The findings may be recorded and shown on a monitor using a Raspberry Pi. The result is then saved in the cloud and communicated to the user's end application over Wi-Fi. Doctors can get the findings using an app.

III. OBJECTIVE OF THE PROJECT

The project's goal is to create a dependable patient monitoring system that allows doctors to remotely check a patient's health state. The doctor regularly monitors the patient in this initiative without ever visiting the patient. Physiological characteristics such as temperature, heart rate, and mobility are sensed using a variety of sensors. These detected signals are sent to the Raspberry Pi through ADC, which converts analogue impulses to digital signals, allowing the data to be updated continually. Data is delivered to the cloud over Wi-Fi and stored, after which it is wirelessly sent to user end application. As a result, the doctor may view the patient's data while seated in his cabin.

When the patient is in a critical situation, he takes the essential steps to help them.

Firebase Database with Arduino UNO and ESP8266 Module. Storing data (such as sensor data) in a database that can be accessed from anywhere by the Internet can be very useful. Firebase makes it easy to store and retrieve data. This is a better option, which can store the data without any attack and send it from one place to another securely through WiFi. Due to which health service to the patient can be done continuously at home.

IV. PROBLEM DEFINITION

In today's medicinal services framework, patients who remain at home after surgery are checked by an overseer or a medical career. This method may not be capable of continuous monitoring, because anything may change in a well-being metric in a matter of seconds, and if a guardian or attendant is not there at the moment, more significant injury can occur. As a result of this invention, a period has been formed in which the web governs the world, and it has been proposed to add to another sharp health awareness framework in which the patient is checked on a regular basis.

V. PROPOSED SYSTEM/METHODOLOGY

The complete system may be broken down into three parts: Sensor Node, Cloud Backend, and User Node. The raspberry-pi receives and analyses sensor data via an Atmega-328, which converts analogue values to

digital and sends them to cloud storage and the user over the internet. Figure 1 depicts a comprehensive block schematic of the system. This primarily contains the Sensor Node, Cloud Backend, and User Node.

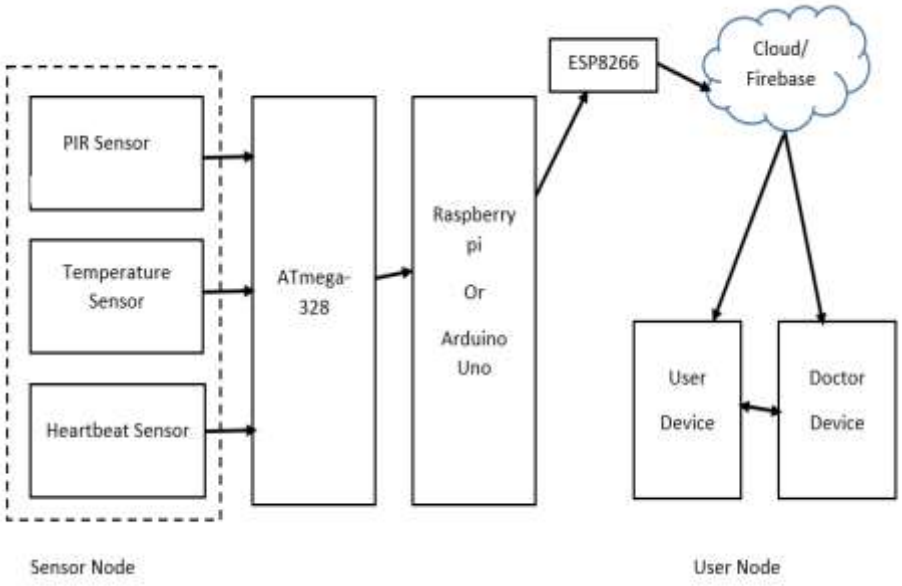


Fig-1: Block Diagram of Remote Patient monitoring system.

Spark is a fast and general-purpose cluster computing system for large-scale in-memory data processing. Spark has a similar programming model to Map Reduce but extends it with a data-sharing abstraction called Resilient Distributed Datasets or RDD. A Spark was designed to be fast for iterative algorithms, support for in-memory storage and efficient fault recovery. Spark Core consists of two APIs which are the unstructured and structured APIs. The unstructured API is RDDs, Accumulators, and Broadcast variables.

Processing: Large-scale datasets are frequently noisy, duplicated, and contain a variety of data kinds, posing significant hurdles to knowledge discovery and data modelling. In general, intrusion detection algorithms work with one or more forms of raw input data, such as the SVM algorithm, which exclusively works with numerical data. As a result, we prepare the data and transform the dataset's categorical data to numerical data.

Objectives used

- Sensor Node
- Cloud/Firebase
- User Node

This is a user-assistance layer. It is a system that allows users to access sensor information and assess the state of patients. Client nodes is an Android application that runs on a smartphone. The user (doctor) may get sensor data and receive a push notice if the value exceeds a threshold value, as well as examine different patient details through report in an app.

Hardware Description

- **Raspberry Pi**
- **ATmega 328**
- **Temperature Sensor**
- **Motion sensor**
- **Pulse/Heart Rate Sensor**
- **ESP8266**

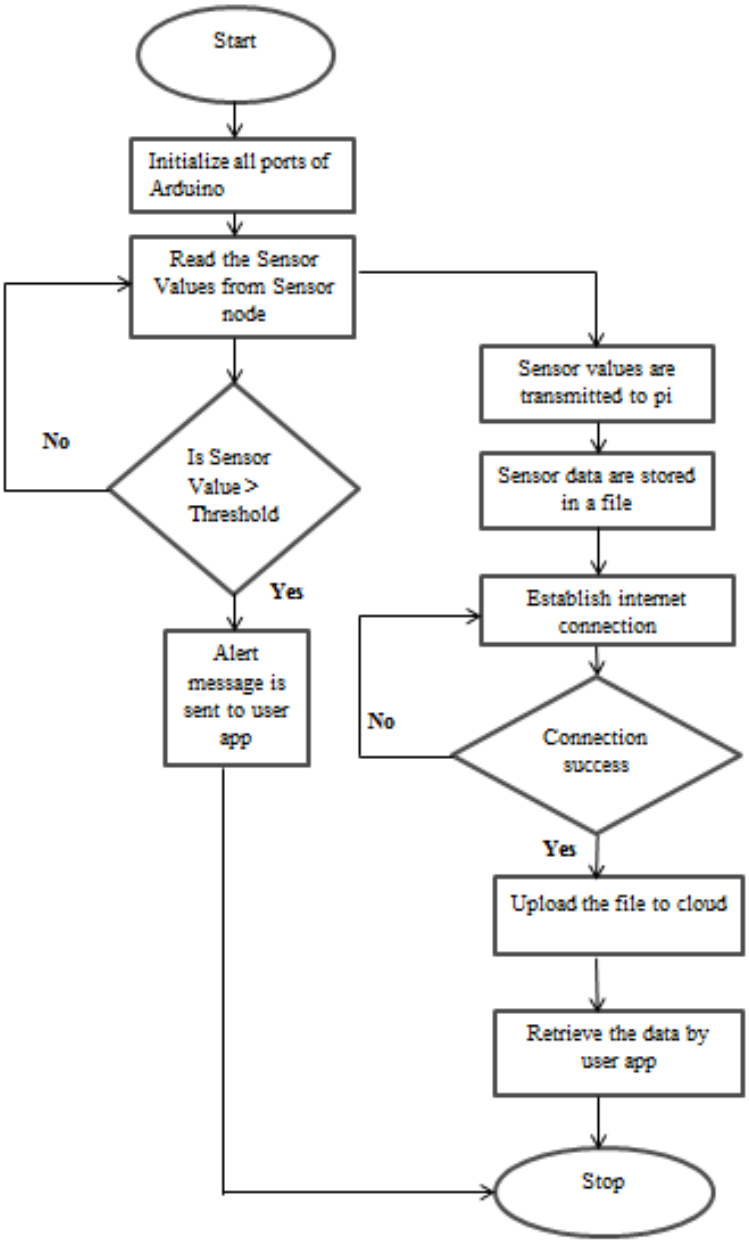


Fig-2: Proposed Flowchart for Remote Patient Monitoring System -an IoT based approach.

VI. REFERENCE

[1] Megha Koshti, IoT Based Health Monitoring System by using Raspberry Pi and ECG signal, M.E. Student, Department of ENTC (VLSI and EMB), Genba Sopanrao Moze College of Engineering, *Balewadi, Pune, Vol 5, May 2016.*

[2] Dr.M.Pallikonda Rajasekaran , R.Kumar, An IOT Based Patient Monitoring System Using Raspberry Pi, Department of Electronics and Communication Engineering, *Kalasalingam University Tamilnadu, India , April 2010.*

[3] Branko Perii, A Custom Internet of Things Healthcare System, Faculty of Technical Sciences *University of Novi Sad, Serbia, March 2013.*

[4] Pooja Navdeti , Patient Parameter Monitoring System using Raspberry Pi, International Journal Of Engineering And Computer Science, *ISSN:2319-7242 , Volume 5 ,Issue -03, pp:16018-16021, March 2016.*

[5] Adivarekar JS, Chordia AD, Baviskar HH, Aher PV, Gupta S. Patient Monitoring System Using GSM

Technology, International journal of mathematics and Computer Research, *March 2013.*

[6] Purnima, Neetu Rout and Rahul Tiwary , International Journal of Advanced Researchin Electrical, Electronics and Instrumentation Engineering, *Vol. 3, Issue 1 , January 2014.*

[7] Mendrela Biswas, Rupali S. Landge and Bhagyashree A. Mahajan, Raspberry Pi Based Patient Monitoring System using Wireless Sensor Nodes, *Volume 3, Issue: 04, Apr- 2016.*

[8] Junaid Mohammed, Abhinav Thakral, Adrian Filip Ocneanu, Colin Jones, ChungHorng Lung, Andy Adler, Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing, IEEE International Conference on Internet of Things (iThings 2014) Green Computing and Communications (GreenCom2014) and Cyber-Physical, *pp:256-263, 2014.*

[9] Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019, 8, 768. [CrossRef]

[10] Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A Secure Framework for IoT-Based Healthcare System. In Proceedings of the International Ethical Hacking Conference 2018, Kolkata, India, 5 October 2018; Advances in Intelligent System and Computing. Chakraborty, M., Chakrabarti, S., Balas, E.V., Mandal, J.K., Eds.; Springer Nature: Singapore, 2019; Volume 811, pp. 383–393.

[11] Nandyala, C.S.; Kim, H. From Cloud to Fog and IoT-Based Real-Time U-Healthcare Monitoring for Smart Homes and Hospitals. Int. J. Smart Home 2016, 10, 187–196. [CrossRef]

[12] Maksimovi´c, M. Improving computing issues in the Internet of Things driven e-health systems. In Proceedings of the International Conference for Young Researchers in Informatics, Mathematics, and Engineering, Kaunas, Lithuania, 1 April 2017; Volume 1852, pp. 14–17.

[13] Yeh, K.H. A Secure IoT-Based Healthcare System with Body Sensor Networks. IEEE Access 2016, 4, 10288–10299. [CrossRef]

[14] Deelip, S.A.; Sankpal, S.V. IOT based Smart and Secure Health Care System Analysis & Data Comparison. Int. J. Res. Appl. Sci. Eng. Technol. 2020, 8, 394–398.

[15] Sanjay, S.; Shekokar, N. Toward Smart and Secure IoT Based Healthcare System. In Internet of Things, Smart Computing and Technology: A Roadmap Ahead, Studies in Systems, Decision and Control; Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V., Hassanien, A.E., Eds.; Springer Nature AG: Cham, Switzerland, 2020; Volume 266, pp. 283–303.

[16] Farahani, B.; Firouzi, F.; Charkabarty, K. Healthcare IoT. In Intelligent Internet of Thing, From Device to Fog and Cloud; Firouzi, F., Chakrabarty, K., Nassif, S., Eds.; Springer Nature AG: Cham, Switzerland, 2020; pp. 515–537.

[17] Abouelmehdi, K.; Beni-Hssane, A.; Khaloufi, H.; Saadi, M. Big data security and privacy in healthcare A Review. Procedia Comput. Sci. 2017, 113, 73–80. [CrossRef]

[18] Connor, Y.O.; Rowan, W.; Lynch, L.; Heavin, C. Privacy by design informed consent and internet of things for smart health. Procedia Comput. Sci. 2017, 113, 653–658.

[19] Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput. Commun. 2020, 153, 311–335. [CrossRef]

[20] Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. J. Ind. Inf. Integr. 2020, 18, 100–129. [CrossRef]

[21] Ray, P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Syst. J. 2020, 2020, 1–10. [CrossRef].

[22] Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review. Wirel. Commun. Mob. Comput. 2019, 2019, 1–20. [CrossRef].

[23] Semantha, F.H.; Azam, S.; Yeo, K.C.; Shanmugam, B. A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics 2020, 9, 452. [CrossRef]

[24] Wu, J.; Tian, X.; Tan, Y. Hospital evaluation mechanism based on mobile health for IoT system in social networks. Comput. Biol. Med. 2019, 109, 138–147. [CrossRef]

[25] Khatoon, N.; Roy, S.; Pranav, P. A survey on Applications of Internet of Things in Healthcare. In Internet of Things and Big Data Applications. Intelligent Systems; Khatoon, N., Roy, S., Pranav, P., Eds.; Springer Nature: Cham, Switzerland, 2020; Volume 180, pp. 89–106.

[26] Tuli, S.; Basumatary, N.; Singh-Gill, S.; Kahani, M.; Chand-Arya, R.; Wander, G.; Buyya, R. HealthFog: An ensemble deep learning-based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Gener. Comput. Syst. 2020, 104, 187–200. [CrossRef] Symmetry 2020, 12, 1191 32 of 35

[27] Gupta, P.; Pandy, A.; Akshita, P.; Sharma, A. IoT based Healthcare Kit for Diabetic foot Ulcer. In

Proceedings of the ICRIC 2019, Jammu, India, 8–9 March 2019; Lecture Notes in Electrical Engineering. Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S., Eds.; Springer Nature: Cham, Switzerland, 2019; Volume 597, pp. 15–22.

[28] Elmisery, A.M.; Rho, S.; Aborizka, M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Clust. Comput. 2017, 22, 1611–1638. [CrossRef]

[29] Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. IEEE Trans. Ind. Inform. 2018, 14, 1656–1665. [CrossRef]

[30] Shirley, M.A.J.; A, M.C.; Phil, M.; Ed, M. A cloud IoT based smart patient health monitoring system. Adalya J. 2020, 9, 963–968.

[31] Khader, A.H.A.; Subasri, K. Fog Assisted-IoT Enabled Patient Health monitoring. Adalya J. 2020, 9, 525–530.

[32] Swaroop, K.N.; Chandu, K.; Gorrepotu, R.; Deb, S. A health monitoring system for vital signs using IoT. Internet Things 2019, 5, 116–129. [CrossRef]

[33] Wilt, T.; Versluis, A.; Goedhart, A.; Talboom-Kamp, E.; van Delft, S. General practitioners' attitude towards the use of eHealth and online testing in primary care. Clin. eHealth 2020, 3, 16–22. [CrossRef]

[34] Kang, J.J.; Larkin, H. Intelligent personal health devices converged with IoT networks. J. Mob. Multimed. 2017, 12, 197–212.

[35] Wang, X.; Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Gener. Comput. Syst. 2020, 112, 320–329. [CrossRef]

[36] Yamin, M. IT applications in healthcare management: A survey. Int. J. Inf. Technol. 2018, 10, 503–509. [CrossRef]

[37] Mohammed, D.; Meri, A. IoT Service Utilization in Healthcare. In Internet of Things (IoT) for Automated and Smart Applications; Ismail, Y., Ed.; IntechOpen: London, UK, 2019; pp. 1–27.

[38] Cha, S.; Hsu, T.; Xiang, Y.; Yeh, K. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. IEEE Internet Things J. 2019, 6, 2159–2187. [CrossRef]

[39] Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions. IEEE Commun. Mag. 2017, 55, 26–33. [CrossRef] 40. Mohanty, M.N.; Das, S. Advances in Intelligent Computing and Communication. In Lecture Notes in Networks and Systems Proceeding of ICAC 2019; Springer Nature Singapore Pte Ltd.: Singapore, 2020

ANNEXURE 2

Second Paper : Communicated

ADCIS 2022 (author)

ADCIS 2022 Submission 58

Update information
Update authors
Update file

The submission has been saved!

Submission 58	
Title	ENHANCING SECURITY AND PRIVACY IN IOT CLOUD BASED HEALTHCARE SYSTEM
Paper:	(Jun 04, 04:11 GMT)
Author keywords	Health Care System Raspberry Pi board Heartbeat sensor Temperature sensor Cloud Internet of things Esp8266
Abstract	One of humanity's greatest difficulties is health. In the recent decade, healthcare has gotten a lot of attention. Not just for sensory equipment, but also for communication, recording, and display equipment, technology plays a significant role in healthcare. It is critical to keep track of numerous medical markers as well as the post-operative days. As a result, the most recent trend in healthcare communication methods utilizing the Internet of Things (IoT) has been adopted. Due to its superior technology, the patient monitoring system has recently become one of the most significant advancements. At this time, a modern strategy is required. The underlying issue with the old technique is that in severe cases, health care experts must be present at the patient's location at all times to check symptoms on a frequent basis. To overcome this issue, health professionals must design a dependable patient monitoring system that allows them to monitor their patients remotely. The project is a wireless health monitoring system based on mobile devices that may deliver real-time online information on a patient's physical status. The Raspberry Pi is employed as an important element of the processing in this project, as are sensors like as temperature, pulse/heart rate, and PIR. These sensors are wired to an Arduino board, and reads the sensor readings and sends them to the Raspberry Pi through serial connection. The sensor data is now saved in a file on the Pi, which is then transferred to the cloud over the Internet. Finally, this uploaded data is retrieved through the user app. The same data is then transferred to the

	patient and doctor via Firebase to further improve treatment by obtaining patient information in a timely manner.
Submitted	Jun 04, 04:11 GMT
Last update	Jun 04, 04:11 GMT
Status of using third-party material in your article	I am not using third-party material for which formal permission is required

Authors						
first name	last name	email	country	affiliation	Web page	corresponding?
Deepika	Dhawan	maildeepika21@gmail.com	India	Integral University		✓
Faiyaz	Ahamad	faiyaz@iul.ac.in	India	Integral University		✓

Copyright © 2002 – 2022 EasyChair

ANNEXURE 3

PLAGIARISM REPORT

RE-2022-22292-(2)-plag-report

ORIGINALITY REPORT

15%	21%	13%	17%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ijariie.com Internet Source	7%
2	www.mdpi.com Internet Source	4%
3	www.duo.uio.no Internet Source	2%
4	Sureshkumar Selvaraj, Suresh Sundaravaradhan. "Challenges and opportunities in IoT healthcare systems: a systematic review", SN Applied Sciences, 2019 Publication	1%
5	Elahe Fazeldehkordi, Olaf Owe, Josef Noll. "Security and Privacy Functionalities in IoT", 2019 17th International Conference on Privacy, Security and Trust (PST), 2019 Publication	<1%
6	www.hindawi.com Internet Source	<1%
7	www.scribd.com Internet Source	<1%

8	Submitted to Salalah College of Technology Student Paper	<1 %
9	Submitted to University of Teesside Student Paper	<1 %
10	Submitted to Engineers Australia Student Paper	<1 %
11	Submitted to Ibra College of Technology Student Paper	<1 %
12	Submitted to University of Greenwich Student Paper	<1 %
13	ijesc.org Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		