

Design & Implementation of data privacy & security using IoT sensors in remote health monitoring system

^[1]Sandeep. K. V. ^[2]Dr. T. C. Manjunath

^[1]Research Scholar, VTU Research Centre, Dept. of Electronics & Communication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka
Visvesvaraya Technological University, Belagavi-590018, Karnataka

&

Assistant Professor, Dept. of Electronics & Telecommunication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka

^[2]Research Supervisor, Professor & HOD, Dept. of Electronics & Communication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka
Visvesvaraya Technological University, Belagavi-590018

Email: ^[1]sandeep.kv38@gmail.com, ^[2]tcmanju@iitbombay.org

Abstract: In this research article, the design & implementation of data privacy & security using IoT sensors in remote health monitoring system is presented. The concept of 'things' is expected to be broadened by the Internet of Things paradigm to encompass a wider range of entities, including intelligent machines, sensors, people, and any other IoT objects that is accessed at any time and from any location. Most favourable uses of IoT is in the medical sector, among its many other uses. Further, IoT systems' enormous attack surface and vulnerabilities need to be watched over and secured. Security is crucial for IoT solutions in the medical sector. This study examines several IoT applications in healthcare with a focus on the data security features of IoT devices, which include remote patient monitoring systems. This work proposed here discussed about design steps and implementing same for an IoT-based smart framework for real-time, round-the-clock monitoring of human temperature, heartbeat, and movement detection. Three IoT sensors are coupled with the Raspberry model. This model is given the sensing data for processing and secure cloud storage. The gadget encrypts the parameter data using the Python Bcrypt algorithm, and since a powerful algorithm is used for both encryption and decryption, the user may access the decrypted data after the decryption process. By verifying the user credentials, authentication concepts are applied. Privacy and security to patient's data is achieved. There will be fewer opportunities to decode it because a passwords are hashed in Python with BCrypt algorithm. Since every user or computer can be authenticated and BCrypt encryption and decryption methods are used, this method solves some of the security problems in IoT networks.

Keywords: Security, Internet of Things, Python, Bcrypt algorithm, decryption, encryption

1. Introduction

IoT's fundamental guiding concept is the transparent connection of items to the Internet. As a result, data is exchanged amongst all things, providing users with information in a more secure manner. By 2020, Cisco Systems predicts that there will be 50 billion Internet-connected devices, and it is expected that many physical objects, such as computers and sensor actuators, will be distributed with unique addresses and the capability to securely transfer data, ranging from routine daily activities to confidential medical records.

IoT is a technology that provides an integration technique for all these physical things that have embedded technologies to be coherently connected and allows them to communicate, perceive, or interact with the physical environment, as well as among themselves. A linked collection of anybody, anything, anytime, anywhere, any service, and any network is what the IoT idea represents.

Healthcare is one of the most alluring IoT application areas since it offers us the chance to use different medical applications including remote health monitoring, exercise programmes, chronic illnesses, and senior care.

Security is a significant issue with IoT and healthcare. Numerous Services and Applications are provided by this invention.

The current technologies systems that store sensitive data must be kept apart and guarded that is commonly utilised by the public. In IoT security solutions, security analytics will be crucial. It's critical for today's digital businesses to strike a balance between the potential business benefits that IoT-connected products can offer and the knowledge that these same products have evolved into an alluring attack plane for hackers and cybercriminals looking to disrupt systems and steal sensitive data. End-to-end security for IoT is necessary. Unquestionably necessary is encryption.

Alice, as an example, wants to have access to her blockchain-based medical records. To make it difficult for anybody other than her to read the data, it must first be encrypted. The data is anonymised after encryption to remove any identifiable information, such a person's name or address. Alice must eventually be granted access to the data through the use of access control procedures in order to guarantee that only she can do so. The privacy, security, and anonymity of Alice's medical records are all guaranteed by these tools. Below sections describes about data privacy & security using IoT sensors in remote health monitoring system.

2. Literature Review

Arlen Baker [1], highlights about ensuring data integrity in IoT applications to avoid inaccurate and unreliable results. He discusses various techniques and strategies employed to maintain data integrity, such as encryption, authentication, and access control. Additionally, Baker emphasizes to continuous monitoring and auditing of IoT systems to detect any potential threats or vulnerabilities that could compromise data integrity.

Babu B., Srikanth K et.al. [2] discusses the potential of IoT in improving healthcare services and patient outcomes. It highlights the various applications of IoT in healthcare such as remote monitoring, telemedicine, and smart sensors. Additionally, the authors emphasize for addressing privacy, security concerns in implementing IoT solutions in healthcare.

Alsubaei F., Shiva S., Abuhussein A. [3] proposes a taxonomy for classifying the security and confidentiality hazards w.r.t the IoT in healthcare. The authors suggests health care must prioritize the applications of the security measures to protect patient data and prevent un-authorized permission for medical devices.

The taxonomy proposed by the Nausheen F., Begum S. [4] includes four categories of risks: technical, physical, operational, and legal. Each category is further divided into subcategories to give a broad framework for assessing and addressing IoT security and privacy risks in healthcare. It is important for healthcare organizations to regularly review and update their security measures to stay ahead of evolving threats in the rapidly changing landscape of IoT technology.

Yang L., Ge Y. et.al. [5] describes proposal & implementing process of a mobile health-care system specially for wheel chair users. This incorporates various sensors and wearable devices to monitor the user's health status and provide timely assistance when needed. System is created to be user-friendly and simple to use, opening it up to many users.

Seh A., Zarour M et.al. [6] highlights the increasing frequency and severity of healthcare data breaches, whose outcome is significant financial losses and reputational damage for affected organizations. The authors also discuss implementing effective cyber security measures to prevent such breaches from occurring in the first place.

3. Existing system

The IoT's acceptance has completely changed how the healthcare business operates today because it has so many potential uses, including remote monitoring and the addition of medical devices. The IoT's is utilised in healthcare for interconnected medical equipment like detectors, sensor machines, and monitoring systems that can record real-time health data. For further analysis to improve healthcare services, the detectors store the data on a centralised cloud or server. By 2024, the IoT market for healthcare is projected to reach USD \$188 billion, growing at a Compound Annual Growth Rate (CAGR) of 27.6%. The major players in this market are all attempting to capitalise on this expansion by enhancing their products or investing in the adoption of such technologies. Figure 1 shows IoT in Healthcare.

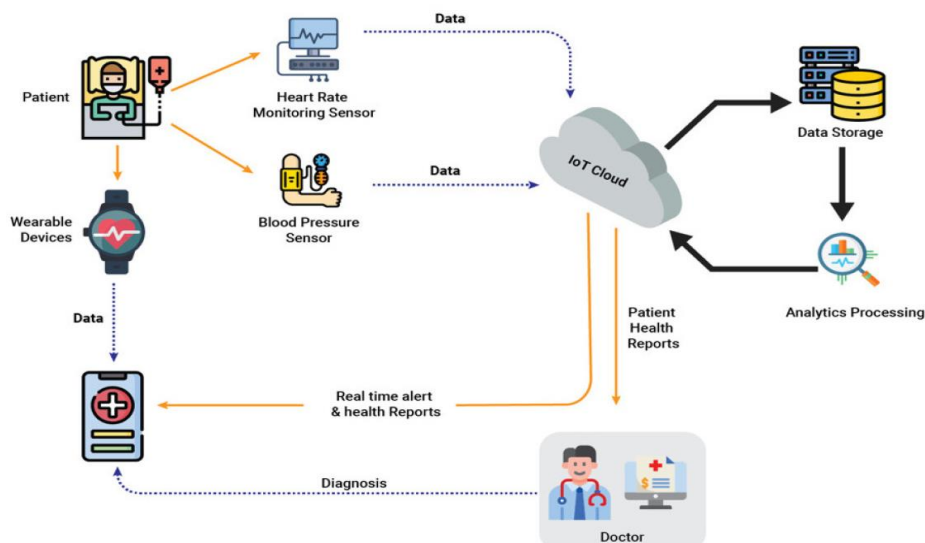


Fig. 1: IoT in Healthcare

Radical change is set to occur in the healthcare sector. A types of current digital trends have been adopted by the healthcare industry as a outcome of need to collect, store, and evaluate patient data. Below are some examples of how digital technology are revolutionising the healthcare sector:

- a) **Internet of Things:** Smart and linked solutions that are IoT enabled, such as wearable technology, smart sensors, and smart health monitoring systems, are able to unleash the potential development of the healthcare industry. They will improve the treatment by employing efficient health monitoring. The rise of IoT in the healthcare and medical industries had led to an rise in contemporary approaches like IoMT. A network of intelligent devices that speaks with one another in real-time and provide results is known as the IoMT. This decreases human mistake and ends many decision-making delays.
- b) **Cloud Computing:** Thanks to the cloud, healthcare providers may continue to offer state-of-the-art technology treatment while protecting patient data and ensuring regulatory compliance. Thus, the patient experience is taken for digital sphere. Our ability to access patient information has increased for a variety of hybrid, private, and public cloud platforms.
- c) **Artificial Intelligence (AI):** Because to AI technology, diagnosis of any illness has become more rapid and accurate. AI is used in the research and development of innovative medical products. Automating repetitive tasks done by medical staff personnel, such as timekeeping, scheduling, and standard documentation, aids in increasing productivity and reducing expenses. AI has also helped doctors analyse historical patient data in order to uncover any insights that can result in a better course of therapy.

3.1 IoT's advantages in the healthcare sector

While it comes to how applications, devices, and people interact while offering healthcare solutions, the Internet of Things is changing the healthcare sector for the next ten years. Below are few advantages on IoT adoption in the healthcare sector:

1. **Real-time monitoring** – Smart healthcare gadgets can provide patients with customised, real-time information on their health state. They remind the patient to check their health on a regular basis. In the event of any medical crises, such as heart failure or an asthma attack, the gadget alarms more quickly and allows for direct link with the doctor.
2. **Best patient experience** – Online connectivity to the healthcare system increases patient participation and provides clinicians with real-time health data that aids in more precise diagnosis.
3. **Cost Reduction** - Using IoT solutions and connected medical equipment, the doctor may remotely monitor the patient with real-time data, which speeds up the healing process and offers benefits like constant communication, decreased use of the hospital's resources and trip costs, etc.

3.2 Digital technology challenges in healthcare

Digital healthcare solutions provide a seamless digital connection with the patient by utilising IoT and big data. We can obtain real-time patient data thanks to the expanding number of medical wearable gadgets that are being connected to these systems through the internet. But before digital healthcare is deployed, the following problems should be fixed:

- To protect patient privacy, effective data security is necessary.
- Integrating several devices using various protocols adds complexity and slows the interchange of data.
- Effective memory.
- Managing data & its outcomes are needed because of the vast volume of stored data.

In conclusion, data security is very important factor to be considered in remote monitoring, its required to maintain patient's secrecy to avoid effects of data leaks. Some major concerns regarding the applications of IoMT include security, privacy, and compliance. IoT security is a major concern for hospitals and medical care facilities. The health sector has the highest number of breaches. Indeed, from 2015 to 2019, health sector accounted for 76% of all breaches, well above the other sectors, with the business and financial sector accounting for 9% .

4. Hardware Requirements

This research proposes an remotely monitoring of a health system, that monitors patient's data such as temperature DS18B20 temperature sensor, heartbeat using heartbeat sensor, gesture control using ADXL335 accelerometer. Proposed system and methodology further discusses about the implementation of IoT-based data privacy security solutions in the applications of healthcare like patient's health monitoring system.

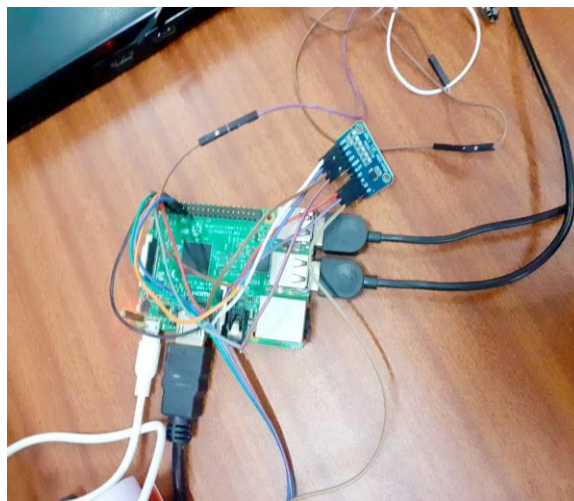








Fig. 2: Hardware setup

Figure 2 above shows the hardware requirements and its connection for set up of hardware model. Hardware components list is given in the table 1. In the table below, Raspberry Pi 3 Model B+ for interfacing IoT sensors, DS18B20 temperature sensor checking remotely patient body temperature, heartbeat sensor for monitoring heartbeat of a patient, movement detection using ADXL335 accelerometer. Jumper wires are utilized to connect all these IoT sensors to Raspberry Pi.

Table 1: List of Hardware components

SI No.	Component	
1		Raspberry Pi 3 Model B+
2		DS18B20 Temperature Sensor
3		Heartbeat sensor
4		ADXL335 Movement Sensor
5		ADS1115 A-D Converter
6		Jumper Wires

5. System Architecture

The block diagram and system architecture as discussed in above sections are given below in figure 3 below. The Raspberry Pi 3 Model B+ single-board computer, a temperature sensor, a heartbeat or pulse sensor, an accelerometer, and an analogue to digital converter make up the construction of this monitoring system. The Raspberry Pi 3 Model B+ was chosen because to its excellent technical characteristics, strong data processing performance, and lower price than other single board computers on the market. The body temperature of patients is tracked using DS18B20 temperature sensors. A heartbeat or pulse sensor is utilised to monitor a patient's heartbeat, and an ADXL335 accelerometer was employed to detect movement. ADS1115 are 16-bit, high-precision, ultra-compact analog-to-digital (A/D) converters.

The primary goal of this research is to create an autonomous system for medical care. It is divided into three major sections.

- Detection of patient's health parameters using sensors.
- Authentication of users and sending cloud data & storage.
- Providing the sensed information for viewing remotely.

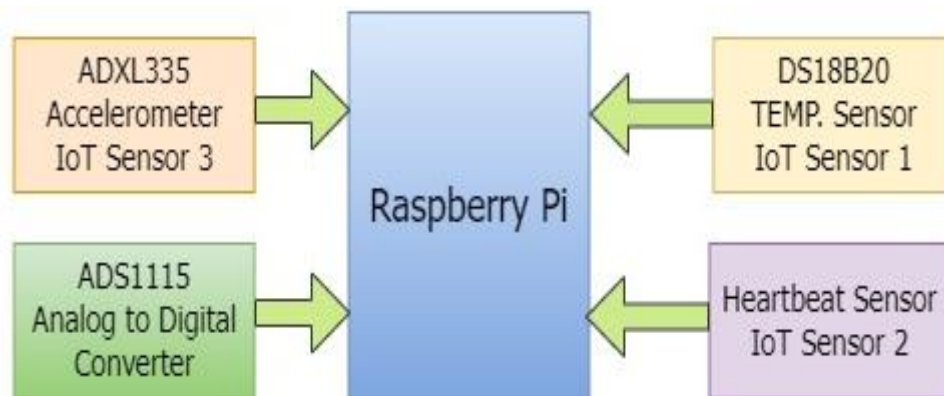


Fig. 3: System architecture

Figure 4 below shows the flowchart describing the working methodology of python coding using Bcrypt algorithm in Raspberry Pi. Three IoT sensors namely. Temperature, heartbeat and movement detection sensors will continuously sense the parameters and stores it in cloud. Authorized users like Doctor, hospitals staff can view this data remotely on regular basis and can observe variations in the data. If emergency, suitable action can be taken either by sending the ambulance to the place or alerting the doctors for advice on medication. The proposed systems will warns by sending warning SMS to authorised person if someone tries to hack the data of the health parameters of the patient. Fig. 5 below show the flow chart of proposed health monitoring system.

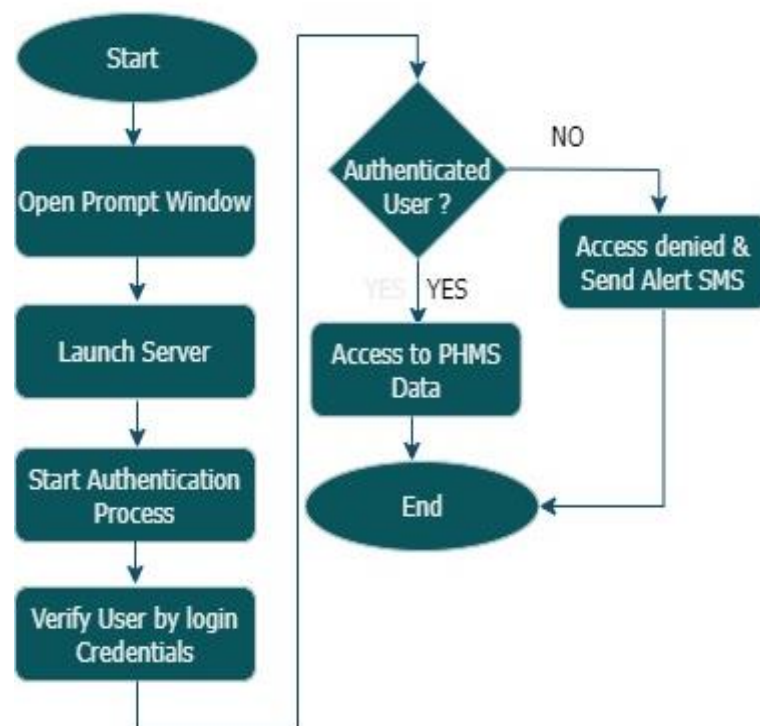


Fig. 4: Work flow of Bcrypt programming in Raspberry Pi

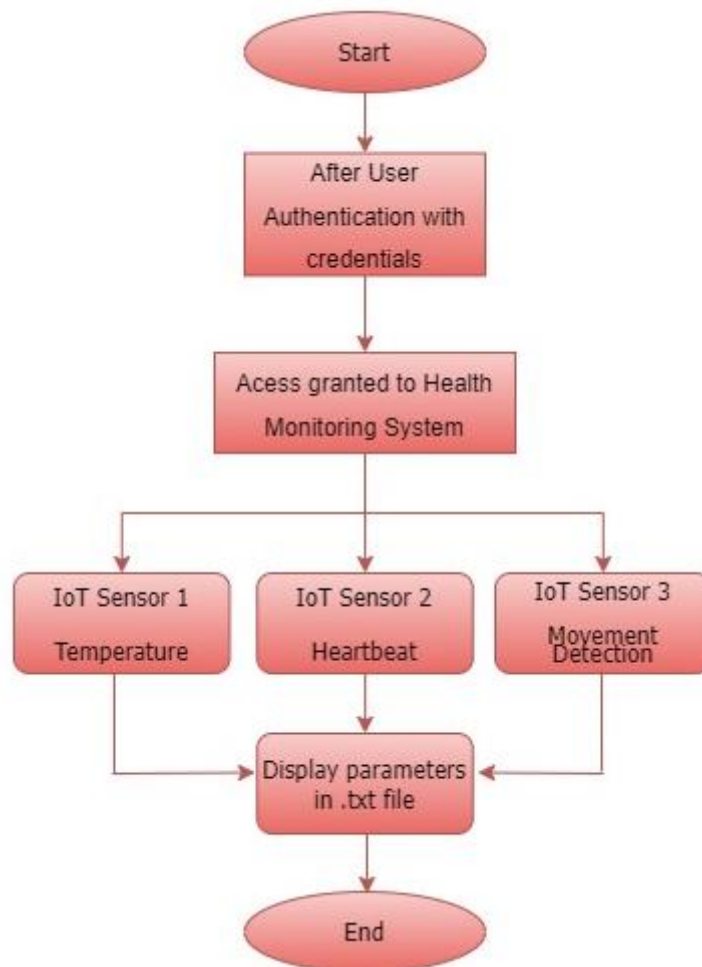


Fig. 5: Flowchart of health monitoring system

6. Implementation & Methodology

When creating the programme for the Raspberry Pi, a monitor, USB keyboard, and USB mouse were utilised. Figure 6 displays a block schematic of the system. In contrast to the keyboard and mouse, which were linked to the Raspberry Pi's USB ports, the monitor was attached to the HDMI port of the device via an HDMI cable.

6.1 Hardware Implementation

- **Temperature sensor:** Three wires of the DS18B20 temperature sensor are red, black, and yellow in hue. The Raspberry Pi's Pin 1 is linked to the red wire of the DS18B20, which is the VCC pin. The Raspberry Pi's pin 7 is linked to the DS18B20's black Gnd wire.
- **Heartbeat Sensor:** The Raspberry Pi's pin-2 is linked to the heartbeat pin's VCC. The Raspberry Pi's pin-20 is linked to the heartbeat pin's ground (GND).
- **Accelerometer Sensor:** Pin 4 of the Raspberry Pi is linked to the 5V of the ADXL335. Gnd of the ADXL335 is linked to Raspberry Pi pin 39. Additionally, the 'X' Pin of the ADXL335 is linked to A1 of the ADS1115. A2 of the ADS1115 is linked to the 'Y' pin of the ADXL335.
- **Analog-to-digital converter (ADC):** Connect VCC pin of ADC to pin-33 of Raspberry Pi. Gnd pin of ADS1115 to pin-9 of Raspberry Pi. SDA pin of ADC to pin-3 of Raspberry Pi. SCL pin of ADC to pin-5 of Raspberry Pi.

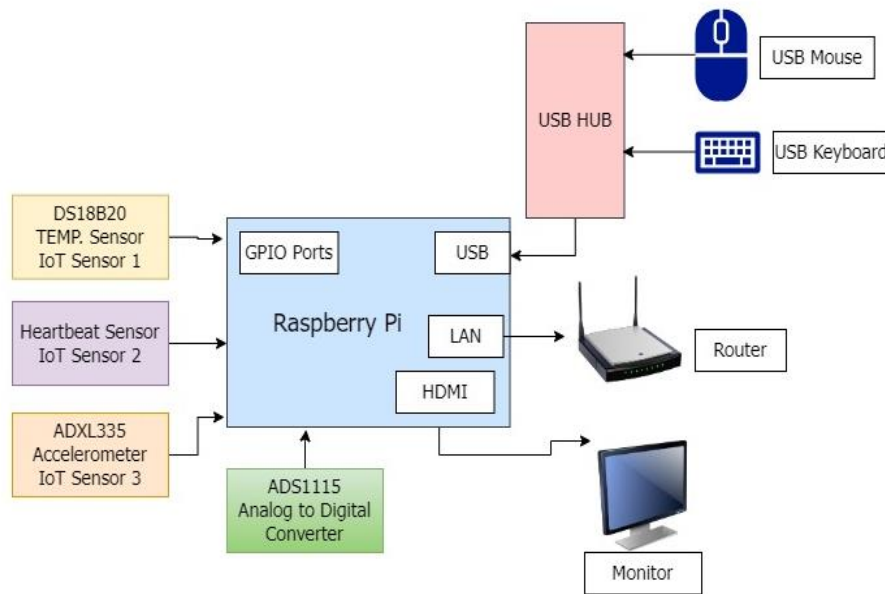


Fig. 6: Proposed model

6.2 Raspberry Pi 3 Model B+

The Raspberry Pi was chosen above other single board computers because of its excellent technological specs, fast data processing performance, and affordability. The most recent Raspberry Pi 3 model, Model B+, features a 64-bit four core CPU operating at 1.4 GHz, dual-band 2.4 GHz and 5 GHz wireless LAN, Bluetooth 4.2/BLE, faster Ethernet, and Power over Ethernet (PoE) functionality through an additional PoE HAT.

6.3 IoT Sensor-1 : Temperature sensor

DS18B20 is the sensor used for temperature measurement. It measures from -55°C to $+125^{\circ}\text{C}$ (-67°F to $+257^{\circ}\text{F}$) accuracy will be of $\pm 5\%$. It follows 1-wire protocol which has revolutionized the digital world. Because of its 1-wire protocol, we can control multiple sensors from a single pin of Microcontroller. It supplies 9-bit to 12-bit.

6.4 IoT Sensor-2 : Heartbeat sensor

Heartbeat sensor is a low-cost, very small size for Raspberrypi. It is faster and easier to get reliable pulse readings.

6.5 IoT Sensor-3 : Accelerometer ADXL335 sensor

Unintentional falls are a common cause of severe injury in the elderly population. By introducing small, non-invasive sensor in conjunction with a wireless network, this work gives more freedom living for the aged peoples & also bed ridden patients. We can identify the incidence of a fall and the location of the sufferer by using a tiny device worn around the waist and connected to a network of fixed in the home environment. A fall is detected using economical, lightweight devices MEMS-accelerometers to monitor and a person's location is determined by the intensity of RF.

6.6 ADS1115 A/D Converter

ADS1115 is an ultra-small, low-power, 16-bit precision AD converter (Analog to Digital Converter) with an internal reference voltage. It has board reference & oscillator. ADS1115 uses below 3 modes:

- **Standard:** max. of 100 KHz
- **Fast:** max. of 400 KHz
- **High speed:** upto 3.4 MHz

6.7 Software Requirements

a) Twilio SMS service:

- We can send SMS with Twilio Programmable Messaging. Twilio makes sending and receiving SMS easy.
- Twilio provides products and services to help our innovative IoT applications, connect them to reliable cellular networks worldwide, and secure them for life.
- Can be choosed from many programming language and dive in.
- Also available with libraries and Quick starts to get us sending SMS and MMS in web app, fast.

b) ngrok:

- ngrok is a simplified API-first ingress-as-a-service that adds connectivity, security, and observability to apps in one line.
- ngrok delivers instant ingress to your apps in any cloud, private network, or devices with authentication, load balancing, and other critical controls.
- It Connect remote IoT systems in one line of code.
- Manage connected devices at scale, with the same safe, scalable developer platform your team loves.
- It is all possible with help of ngrok's Device Gateway.
- Static IP addresses are neither required or provided by ngrok.
- The ngrok agent will automatically update as our address public IP changes, and we don't need to restart the agent.

c) Bcrypt Algorithm:

- Bcrypt is a hashing algorithm that transforms a plain text password into a fixed-length string of characters, called a hash.
- Bcrypt turns a simple password into fixed-length characters called a hash.
- Hashing is a one-way process, meaning that it is easy to generate a hash from a password, but hard to recover the password from the hash.
- Before hashing a password, bcrypt applies a salt — a unique random string that makes the hash unpredictable.
- Data integrity and security should always be prioritised. The BCrypt Algorithm used here is safely hash and salt passwords.
- BCrypt enables the advancement of a password security stage that can enhance local hardware innovation to defend against hazards or threats in the long term, such as attackers having the computer capacity to guess passwords twice as quickly.

7. Results and Discussions

After the initial setup of hardware connection, as seen in figure 6 above, and power supply switched on, sensors of IOT can read the parameters of patient temperature, heartbeat and movements that are as listed in table 1 above.

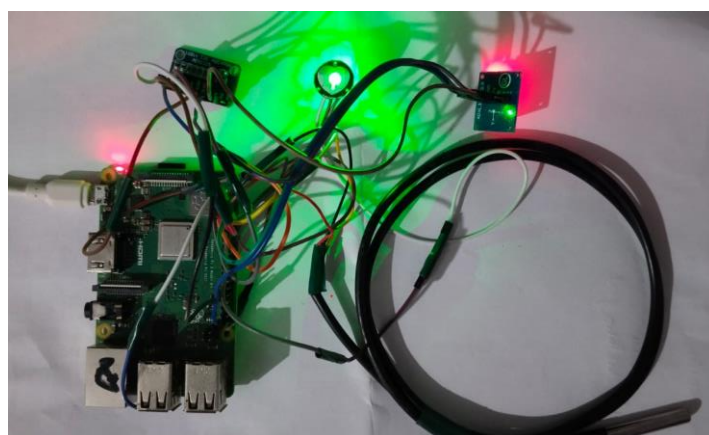
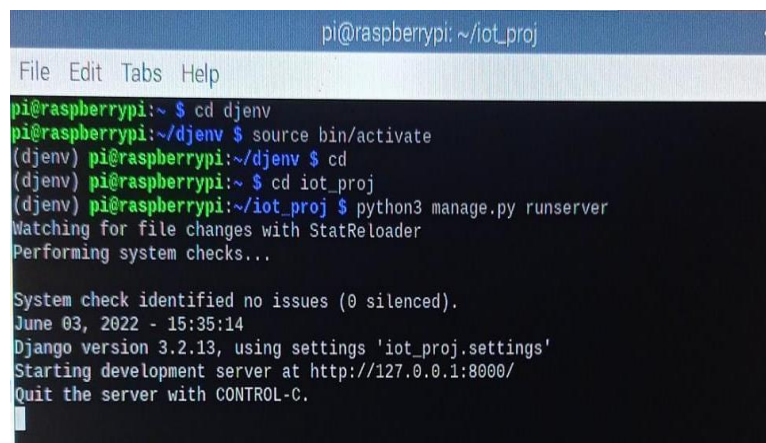


Fig. 7: Hardware setup of Raspberry Pi with sensors

Raspbian Wheezy OS was selected with raspberry-pi since the manufacturer recommends it. It runs on a Linux-based operating system. The Debian Cheezy OS has been tweaked to become the Raspbian Wheezy. The Win32 Disc Manager was used to extract the OS image to an SD card. At first, the OS was conFigured with login information and IP address settings. To ensure that the device won't ever request login information w.r.t power outage, the login information, at startup feature was deactivated. To turn the Raspberry Pi into a web server, the HTTP webserver was installed. The prompt window containing the commands to run Python as a webserver is shown in Figure 8 below. The web server will launch when the code has been run, as seen in Fig. 8 below. Figure 9 below shows the webpage to enter login username and password to access the monitored parameters like temperature, heartbeat etc. The authorized users like Doctors, patient care taker who needs to monitor these parameters, must login with correct username and password. If the entered username and password is matched with the registered ones, then access is granted to read vital parameters.



```
pi@raspberrypi: ~/iot_proj
File Edit Tabs Help

pi@raspberrypi:~$ cd djenv
pi@raspberrypi:~/djenv$ source bin/activate
(djenv) pi@raspberrypi:~/djenv$ cd
(djenv) pi@raspberrypi:~$ cd iot_proj
(djenv) pi@raspberrypi:~/iot_proj$ python3 manage.py runserver
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).
June 03, 2022 - 15:35:14
Django version 3.2.13, using settings 'iot_proj.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

Fig. 8: cmd prompt window showing server address

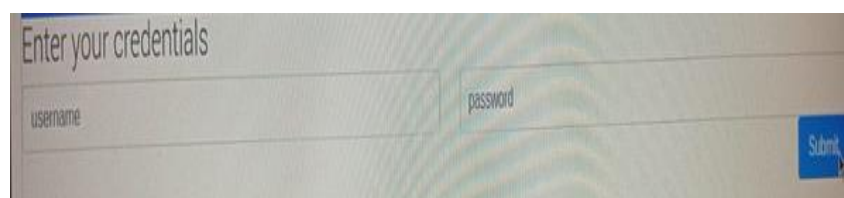


Fig. 9: Interface to authenticate user

After entering the correct username and password, the user name check the parameters in the next web page whose screenshot is in the figure 10 below.

IoT sensor 1 gives patient body temperature, IoT sensor 2 gives heartbeat of a patient and IoT sensor 3 gives information of movement of a patient. Figure 11 below shows the temperature fetched by the IoT sensor 1.



Fig. 10: Webserver for proposed model

```
temp=
30.9
30.4
30.4
31.4
31.4
31.3
31.4
30.2
24.5
```

Fig. 11: Results of IoT sensor 1

If anyone trying to access the encrypted patient data without authorization enters the erroneous password, access is instantly blocked and short message service (SMS) is sent using the twilio free trial account. SMS messages will be delivered to a specified or authorised person's mobile phone number for tracking IoT sensor data. Figure 12 below from a Twilio trial account illustrates an SMS message. It will say "someones trying to hack your account" in the message. SMS messages will be delivered right away each time an unauthorised individual tries to grab the data. The password can be changed by the authorised person with this notice. In this manner, hackers and unauthorised users may be prevented from accessing patient health details. Data security and privacy are attained.

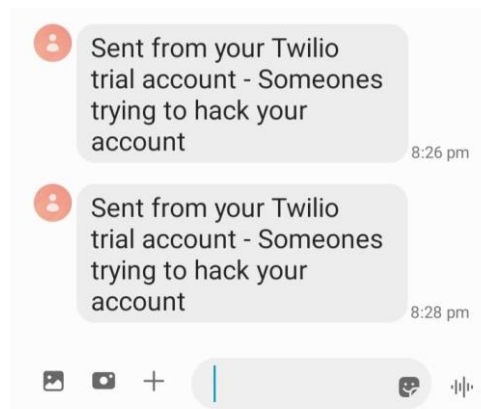


Fig. 12: Warning SMS alert received in registered mobile

8. Conclusion

Applications of IoT in Healthcare have the potential to revolutionise the healthcare industry, allowing medical practitioners to give more efficient and accurate treatments. Healthcare providers may improve patient outcomes, save medical expenses, and provide more personalised treatment using internet. IoTs are altering and revolutionising the healthcare industry, from connected medical devices to virtual health aides.

References

- [1] Arlen Baker, "Maintaining data integrity in Internet of Things applications", *an article on Data Integrity in IoT Applications*. <http://files.iccmedia.com/pdf/windriver160823.pdf>
- [2] Babu B., Srikanth K., Ramanjaneyulu T., Narayana I. "IoT for Healthcare." *International Journal of Science and Research*, volume 5 issue 2. February 2016.
- [3] Alsubaei F., Shiva S., Abuhussein A. "Security and Privacy in the Internet of Medical Things: taxonomy and Risk Assessment." *2017 IEEE 42nd Conference on Local Computer Networks Workshops*. DOI: 10.1109/LCN.Workshops.2017.72. 2017.
- [4] Nausheen F., Begum S. "Healthcare IoT: Benefits, Vulnerabilities, and Solutions." 2018.
- [5] Yang L., Ge Y., Li W., Rao W. Shen W. "A Home Mobile Healthcare System for Wheelchair Users." *2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design*. 2014.
- [6] Seh A., Zarour M., Alenezi M., Sarkar A., Agrawal A., Kumar R., Khan R. "Healthcare Data Breaches: Insights and Implications." May 2020.
- [7] Sandeep K.V., Dr. T.C.Manjunath, "Design and implementation of security mechanism by user authentication for voting system based on Fernet encryption and Blockchain technique", Scopus Indexed

- Journal Article, SCImago Journal & Country Rank - Quartile 3 (Q3) Journal, SJR 2022 Rating 0.25, *Journal of European Chemical Bulletin*, Section A-Research paper, e-ISSN 2063-5346, H-Index 11, Vol. 12, Special Issue 6 (Si6), pp. 3354 – 3369, 2023.
- [8] Sandeep K V, Dr.Sayed Abdulhayan, “Implementation of Data Integrity using MD5 and MD2 Algorithms in IoT Devices”, *Palarch's Journal Of Archaeology Of Egypt/Egyptology-PJAEE(Scopus Q3)*, vol. 17, no. 7, pp. 7388 - 7395, ISSN: 1567-214X, Nov. 2020.
- [9] Sandeep K.V., Manjuanth T.C., “A Novel Mechanism for Design and Implementation of Confidentiality in Data for the Internet of Things with DES Technique”, *6th IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, I-SMAC 2022, Dharan, Tribhuvan University, Purwanchal Campus, Nepal, IEEE XPLORE COMPLIANT ISBN: 978-1-6654-6941-8, IEEE DVD Part Number: CFP22OSV-DVD; ISBN: 978-1-6654-6940-1, Paper ID 561, 10-12, pp. 109-114, November 2022. DOI:10.1109/I-SMAC55078.2022.9987268.