# A SECURED IoT-BASED HEALTHCARE MONITORING SYSTEM

**Jenny, E.F.[1*], Chukudebe, G.[2], Ndinechi, M.[2] and Chukwuchekwa, N.[2]**

[1]Federal University of Technology Owerri, Imo State, Nigeria

[2]Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

*Corresponding email: jeoebicom@gmail.com

## ABSTRACT

*A secured IoT-based healthcare monitoring system is a technological framework designed to monitor patients' health parametric remotely using IoT technology, while ensuring the integrity, confidentiality, and availability of sensitive health data. Current healthcare monitoring often relies on manual checks or less frequent data collection, which lacks the real-time, secure, and efficient remote monitoring systems for patients' vital signs, which can lead to delayed medical responses and increased risks of severe health complications. Additionally, the transmission of sensitive health data over networks can be vulnerable to unauthorized access, compromising patient confidentiality. There is a need for an efficient, secure, and scalable solution that enables real-time monitoring of vital health parameters, ensuring both the integrity and confidentiality of the data while facilitating immediate medical intervention when required. This IoT-based healthcare monitoring system aims to address these issues by providing a reliable and secure platform for continuous patient monitoring and data transmission. The IoT-based healthcare monitoring system was developed using body sensors (LM35 for temperature and SEN 11547 for pulse) connected to an ESP32 microcontroller to collect and transmit vital health data, such as temperature, heart rate, and blood pressure, to a web server. The system utilizes a GSM module (SIM900) for communication between the microcontroller and mobile devices, while ensuring data security through two-factor authentication. A local XAMPP server stores and displays real-time data, updating every 5 seconds. The system was tested on 10 volunteers, Health parameters were measured, stored and displayed on the website, while alerts were sent to care giver registered mobile whenever there is an abnormality. It is recommended to further enhance the system's scalability, incorporate advanced encryption methods to strengthen data security, and utilize The Global Positioning System (GPS) for patient tracking and safety.*

**Keywords:** Internet-of-things, Data security, website, microcontroller

## 1 INTRODUCTION

A secure IoT-Based Healthcare Monitoring System refers to a system in which applications and services are driven by data collected from devices that are embedded with body sensors, software, and other technologies over the internet to monitor and manage the health of individuals remotely, securing patient's information [1]. A secure healthcare monitoring system leveraging IoT facilitates continuous, remote monitoring of patient's vital signs through interconnected devices, sensors, and data analytics platforms, ensuring timely interventions and personalized care plans [2]. Most care providers, especially healthcare companies in developing countries lack advanced architecture and data management systems to manage data collected from multiple sources, while health monitoring which usually involve frequent visit to the hospital for check-up which can be tiresome [3]. The purpose of this work to develop and implement a secure IoT-based healthcare monitoring system using body Sensors, microcontrollers, database management systems, and a website. Data security and privacy are also addressed to securely and

efficiently transmit data between source and destination nodes by implementing a robust authentication mechanism and access controls to ensure only authorized users can access information. This will enable the continuous real-time health monitoring of patient's vital signs, early detection of health issues, and significant cost savings for both patients and healthcare providers, and enhanced healthcare system efficiency by automating data collection and reducing the need for manual interventions.

### 1.1 Architecture for IoT-Based Healthcare Monitoring System

IoT-Based Healthcare Monitoring System has four important layers. These include sensing layer, network layer, middleware layer, and application layer. A general architecture of IoT-based healthcare monitoring system is illustrated in Figure 1.

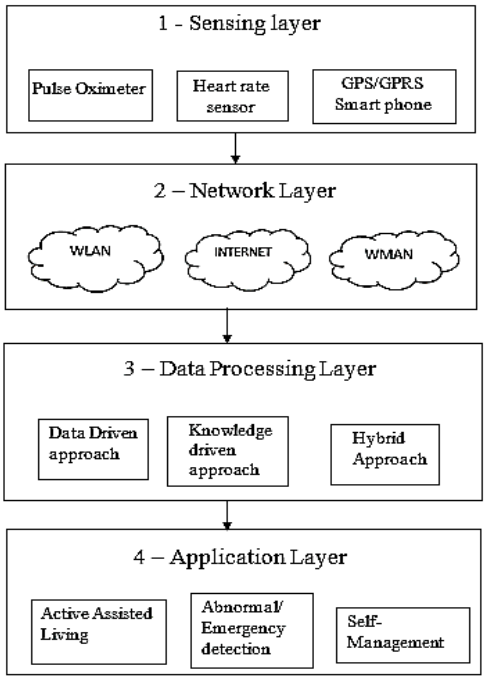



Figure 1. IoT- Based Healthcare Monitoring Architectural

The sensing layer utilizes various sensors to detect the users' health condition both physically, mentally, and emotionally [4]. Body sensors could be either invasive (i.e. which can be inserted into human body) or non-invasive as shown in table 1. When implanted or attached to the human skin do not disturb the person's activity but could record the physiological parameters during any particular activity.

Table 1. Invasive and non-invasive body sensors

| S/n | Invasive/implantable sensors | Non-invasive/wearable sensors |
|---|---|---|
| 1 | Pacemaker | Glucose sensor |
| 2 | Cochlear implants | Electrocardiogram (ECG) |
| 3 | Implantable defibrillators | Electromyography (EMG) |
| 4 | Wireless capsule endoscope | Electroencephalogram (EEG) |
| 5 | Electronic pill for drug delivery | Temperature sensor |
| 6 | Deep brain stimulator | Blood pressure sensor |
| 7 | Retina implants | Pulse oximeter |
| 8 | | Oxygen |

The network layer enables efficient and secure data transmission to corresponding data process units [5]. This includes: Wireless Communication Protocols: Bluetooth Low Energy (BLE) [6], Wi-Fi, Zigbee [7]. Mobile and Web Applications: examples are APIs (Application Programming Interfaces) [8], and Web Services. Cellular Networks: 4G/LTE, 5G [9], LoRaWAN (Long Range Wide Area Network) [10], NFC (Near Field Communication) [11]. The third layer is the Data Processing module, which is responsible analyzing and extracting valuable insights from patient data obtained from the first layer. Examples are: Descriptive Analytics [12], Diagnostic Analytics, Predictive Analytics, Prescriptive Analytics [13], Anomaly Detection [14], and so on. The fourth layer is the Application Layer Healthcare monitoring systems have a wide range of applications. These include: Remote patient monitoring [15], chronic disease management, [16], post-surgery monitoring [17], medication adherence [18], fitness and wellness tracking [19], emergency response [20]' mental health monitoring [21], and so on. Security Challenges in IoT-Based Healthcare monitoring system. Security and Privacy Concerns: The IoT nodes may collect sensitive personal information or become vulnerable to cyberattacks, data breaches, insecure communications, and unauthorized access, posing significant risks to patient safety and confidentiality, hence suitable policies and regulations need to be enacted at the global and national levels to ensure benefit realization and safe use [22]. Addressing these concerns requires robust encryption protocols, access controls, and ongoing cyber-security measures [23]. The security requirements include cyber security and cyber resiliency. Cyber security requirements are divided into two parts: CIA Triad (confidentiality, integrity, and availability) and non-CIA (authentication, privacy, authorization, auditing, and accountability). Cyber resiliency requirements include reliability, safety, maintainability, survivability, performability, and information security [24].

## 2 REVIEWS ON RELATED WORK

There are several studies on secure healthcare monitoring systems using microcontrollers, GSM modules, and websites. In A Secure Framework for IoT-Based Healthcare System described by authors in [25], a secure framework for IoT-based healthcare system that provides confidentiality, integrity, and authentication within a public IoT-based communication network was developed by utilizing a cryptosystem to ensure secure communication and entity authentication between the smart sensors, local processing units (LPU), and gateway. The data security was tackle using Raspberry Pi series platform. Author in [26], introduced a secure IoT-based healthcare system that operates through BSN architecture. The system utilizes robust crypto-primitives to construct two communication mechanisms for ensuring transmission confidentiality and providing entity authentication among smart objects, the local processing unit and the backend BSN server. The system was implemented with the Raspberry PI platform to demonstrate the practicability and feasibility of the presented mechanisms. In Design and implementation of smart healthcare monitoring system using Field-Programmable Gate Array (FPGA) described by authors in [27], a comprehensive healthcare monitoring system was developed by blending IoT and VLSI (Very Large-Scale Integration). Six sensors were used to capture the data from the hospital environment while Nexys4 Artix7 was used as a processor. The condition of the patients is conveyed via the Thing Speak website and telephonic calls/SMS to relatives, and medical staff. In Secure Data Transmission beyond Tier 1 of Medical Body Sensor Network described in [28], the security system was designed to secure data transmission between two tiers, implemented in the cloud. Doctor's fingerprint information was used for the authentication of doctor's identity, while the Back end of the implemented system was controlled by PHP and AJAX, the front end was designed using HTML 5 and CSS. Physiological data of patients are transmitted from personal digital assistant (PDA) to doctor via cloud server with confidentiality and authenticity. Here, secure key distribution was done in order to prevent man-in-middle attack on secret key. Authors in [29] developed a system that monitors vital health parameters and transmits the data through wireless communication using a Wi-Fi module. The data can be accessed at any time using the IOT platform (Thing speak). In case of any abnormal behavior, the caretaker and the doctors were notified immediately through a message service. An IoT based solution designed with Arduino UNO, Nodemcu, and Global System for Mobile Communication (GSM) modules to measure body temperature, pulse rate, Oxygen saturation, room temperature, and air quality in a smart home setting in the Design and implementation of

a feasible model for the IoT based ubiquitous healthcare monitoring system for rural and urban areas is also capable of transmitting the sensitive health information to medical centers and caregivers in real time [30]. In Secure IoT communications for smart healthcare monitoring system described In [31], the system integrates artificial intelligence technology, such as neural networks and fuzzy systems in a secure healthcare monitoring system to enable the system to work as a smart healthcare model that decides the priority by itself depending on the collected health parameters from the sensor nodes. The raw data was converted into linguistic representation, with the help of logic-based algorithm, which is trained in fuzzy-based inference system (FBIS) to get the status of the patient.

## 3 METHODOLOGY

This research aims to develop and implement a secure IoT-based healthcare monitoring system using body Sensors, microcontrollers, database management systems, and a website.

### 3.1 System Description

The system block diagram is depicted in figure 2. Here, patients' vital parameters such as heart rate and body temperature will be measure using the pulse sensor, and LM35 temperature sensor respectively. The microcontroller (ESP32) is used to process and transmit this information to the Sever. Both the patients and monitoring team can access the data via their web portals individually. This is achieved with the use of a local host website which consist of a database consisting of tables for storing users' profiles, authentication and the monitoring parameters (patient's vital signs) and web portals that enable visualization and data access. With the aid of the GSM module, the caregiver and monitoring team can receive an alert message when there is an abnormality.

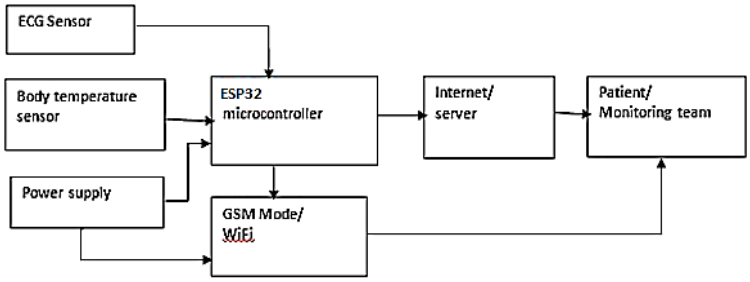



Figure 2. block diagram of the system

### 3.2 The system hardware requirements

The system hardware requirements include the following components. Temperature Sensor LM35: This sensor is used to monitor the user's body temperature and sends the data to the ESP32 microcontroller. Pulse Sensor Module SEN-11574: The pulse sensor monitors the user's heart rate and sends the data to the ESP32 microcontroller. ESP32 Microcontroller: This microcontroller is responsible for processing sensor data, sending data to the website, and communicating with the SIM900 module. SIM900 GSM/GPRS Module: This module is used to send SMS alerts to the mobile phone in emergency situations. Mobile Phone: The mobile phone is used to receive alerts in emergency situations.

### 3.3 The software requirements for the system

The software components required for this system include the Arduino IDE, which is used to program the ESP32 microcontroller and SIM900 module; XAMPP, a web server that hosts the database, hospital website and displays patient data from the ESP32 module; and MySQL, a database used to store the sensor data received from the ESP32 module, and other patient's data.

### 3.4 Flow chart for the heart rate monitoring part

When the system is ON, the pulse sensor measures the heart rate continuously and until it exceeds the threshold, SMS messages will be sent to the care provider's mobile phone for appropriate actions using the GSM module. The flow chart for the hearth rate monitoring system is shown in Figure 3.

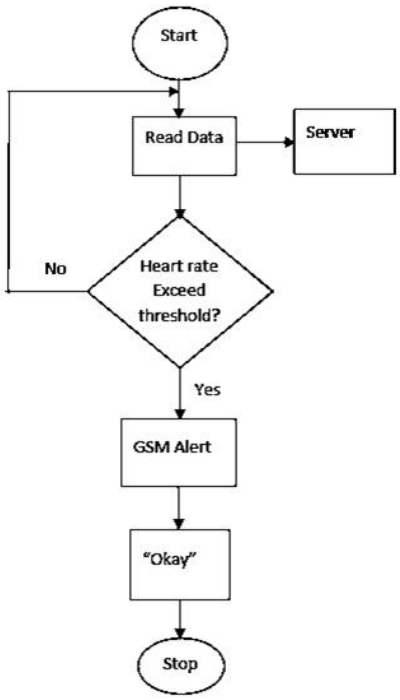



Figure 3. Flow chart for the heart rate monitoring part

### 3.5 Flow Chart for The Temperature Monitoring Part

The temperature sensor will continuously monitor the patient's temperature. Once the temperature exceeds the predefined threshold, an alert will be sent to the care provider's mobile phone. Additionally, both the temperature readings and the alert will be stored in the database and displayed on the patient's portal on the website for real-time monitoring. The flow chart for the temperature monitoring part is shown in Figure 4.

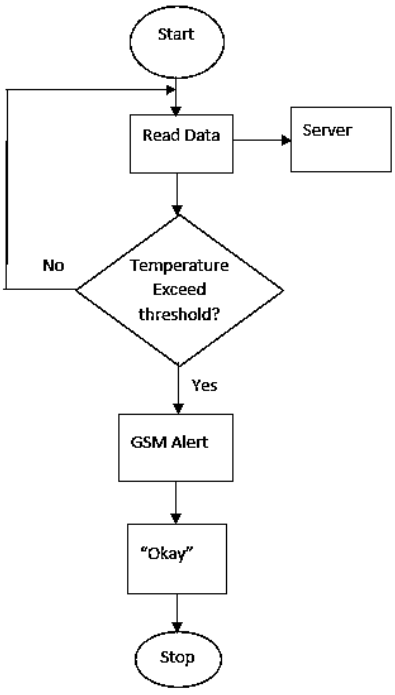



Figure 4. Flow chart for the temperature monitoring part

### 3.6 Circuit Diagram

The circuit diagram (Figure 5) was designed using Proteus 8 professional. It shows how the esp32 is connected to the sensors and the GSM module.

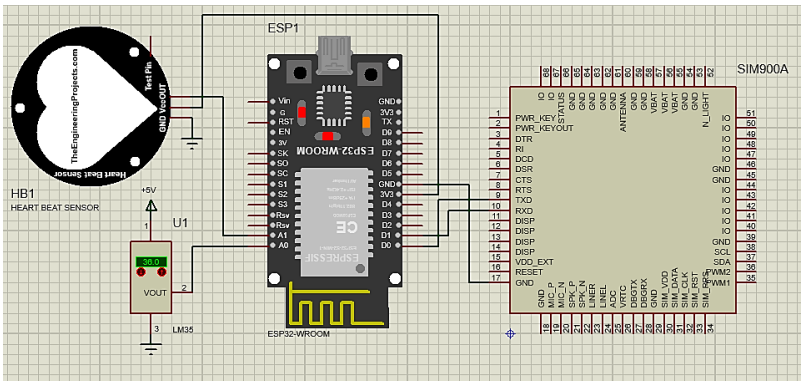



Figure 5. Circuit Diagram

### 3.7 Data Security Method for The System

The communication model between the source and destination nodes is shown in figure 6. When a sensor node needs to transmit the periodical information to the server, the server will verify the identity of the source node. This is achieved using network password validation and one-time-password.

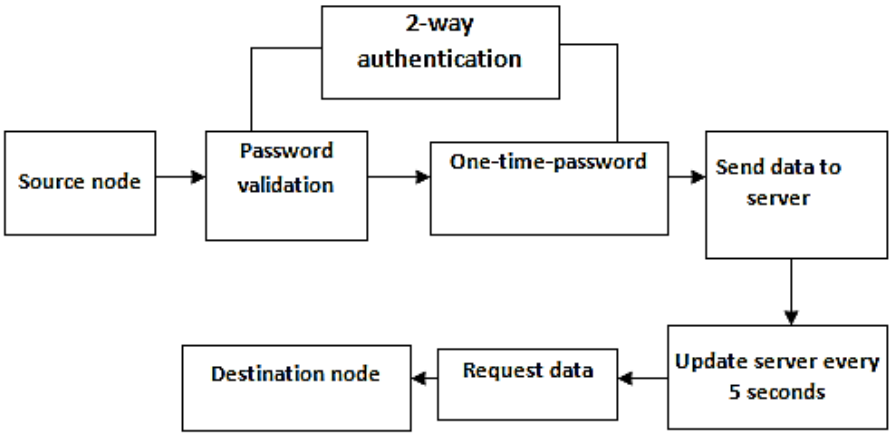



Figure 6. Source-destination data communication model

The system uses two-factor authentication (2FA) to enhance security by requiring both a password and a One Time Password (OTP) for access. Users must enter their email and password to log in, after which an OTP is generated and sent to their registered email for verification.

## 4 RESULTS AND DISCUSSION

### 4.1 The Database Table

The result of the hospital database management system is presented in figure 7. From the result, the database table it which consists of tables for admin profile, user (patient) profile, and doctor information. It also includes the tables for authentication and sensor data (patient's monitoring parametric). Each time a party registers or logs in, values are stored in the designated table.

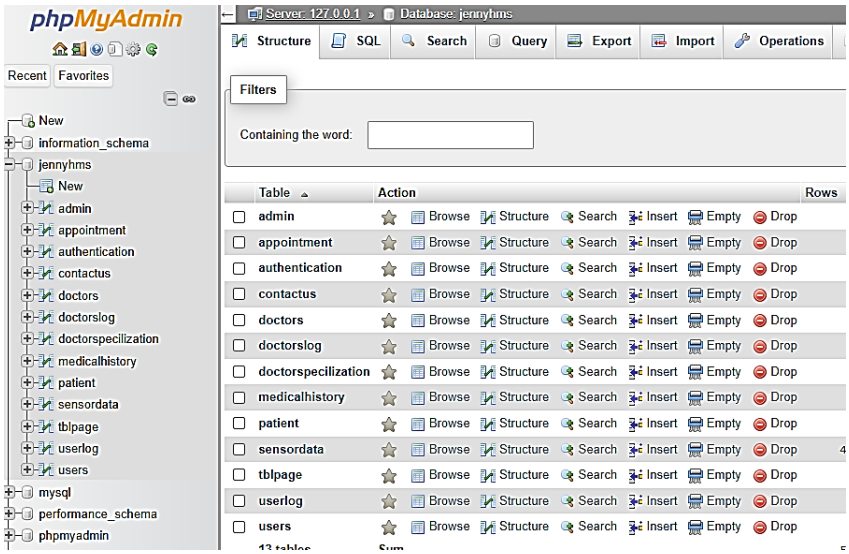



Figure 7. The Database Management System

## 4.2 The Website Homepage

From the system description, the website Homepage (figure 8) is a component of the website consisting of the header that provides links to the various user's profile, patient's monitoring parameters, logins (admin login, doctor login and patient login) and authentication, and other links which contains information about the website.

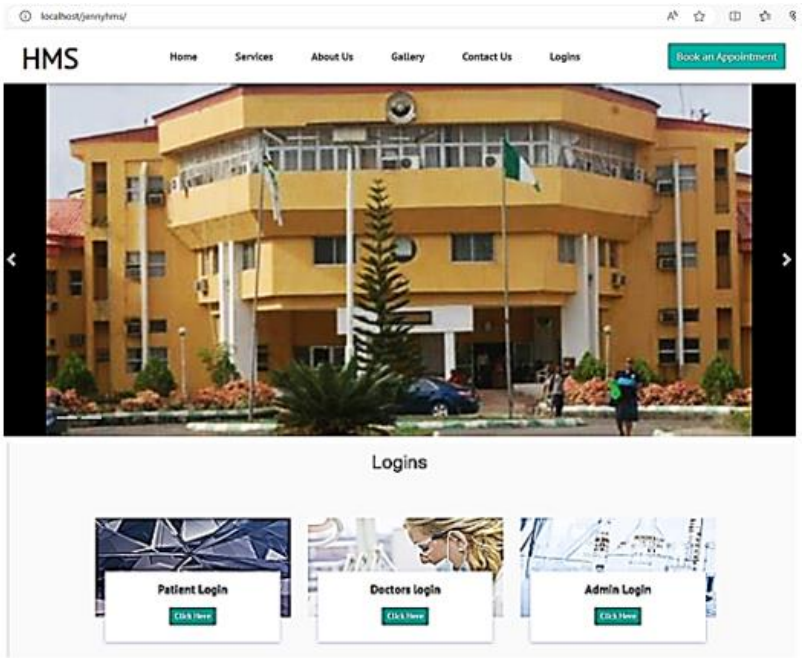



Figure 8. The website Homepage

## 4.3 Data security

Result from the data security model described in section 3.7, is presented in figure 9. Users are required to login using their username (email adress) and password supplied during registration. once this is entered, an OTP will be sent to the user's email Figure 9(b). Entring the correct otp will allow the user to access their portal.

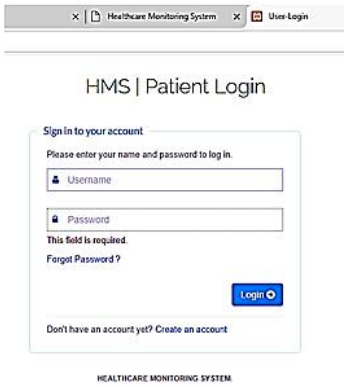



Figure 9(a). Patient Login form

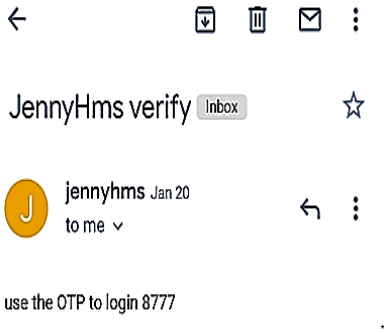
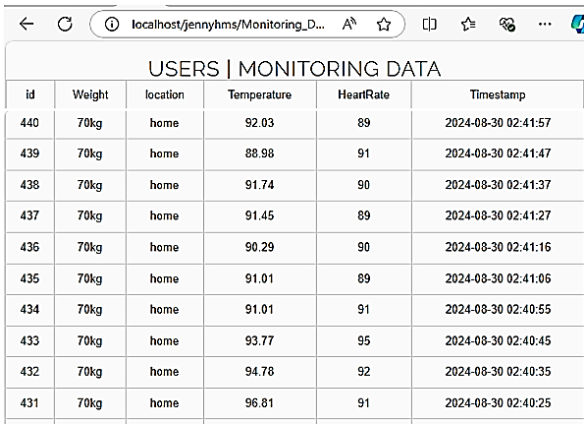



Figure 9 (b). OTP sent to email address

### 4.4 Data visualization

The sensor readings (patient's vital parameters) described in section 3, are displayed in the monitoring_data section on the patient's dashboard and sensor data table in the database. The weight and location displayed are entered manually, while the temperature, heart rate is measured from the sensors. The results are displayed in Figure 10 below.




| id | Weight | location | Temperature | HeartRate | Timestamp |
|---|---|---|---|---|---|
| 440 | 70kg | home | 92.03 | 89 | 2024-08-30 02:41:57 |
| 439 | 70kg | home | 88.98 | 91 | 2024-08-30 02:41:47 |
| 438 | 70kg | home | 91.74 | 90 | 2024-08-30 02:41:37 |
| 437 | 70kg | home | 91.45 | 89 | 2024-08-30 02:41:27 |
| 436 | 70kg | home | 90.29 | 90 | 2024-08-30 02:41:16 |
| 435 | 70kg | home | 91.01 | 89 | 2024-08-30 02:41:06 |
| 434 | 70kg | home | 91.01 | 91 | 2024-08-30 02:40:55 |
| 433 | 70kg | home | 93.77 | 95 | 2024-08-30 02:40:45 |
| 432 | 70kg | home | 94.78 | 92 | 2024-08-30 02:40:35 |
| 431 | 70kg | home | 96.81 | 91 | 2024-08-30 02:40:25 |

Figure 10. Data visualization on website

### 4.5 SMS alert

Result from the registered GSM phone number is presented in Figure 11. Whenever the temperature or heart rate exceeds the normal range (threshold), a warning message is sent to the healthcare provider's registered mobile number.

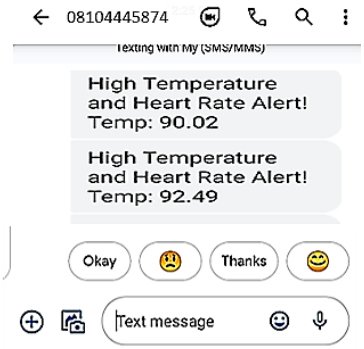



Figure 11. SMS warning alert sent to healthcare provider's phone number

Figure 12 shows the graphical representation of the pulse measured by one of the volunteers. A Statistics evaluation was conducted to check if the readings are normal and also to check the system stability. This was done by calculating the mean values, deviations and variance from the result.

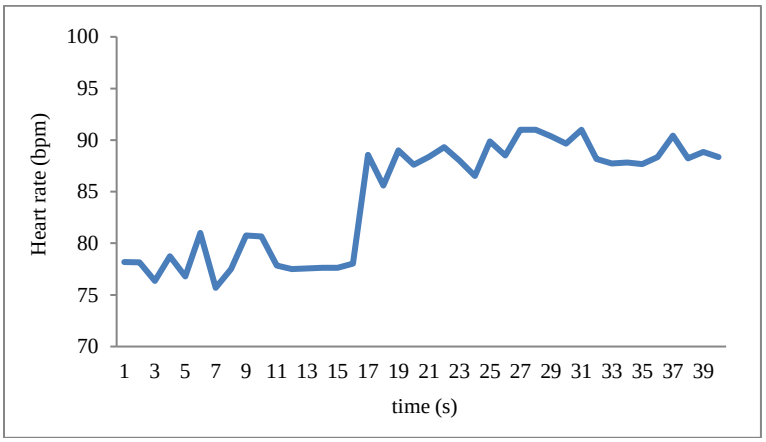



Figure 12. Graph of heart rate *vs* time

From the result, the heart rate Variability is low. The heart rate readings vary by approximately 4.36 bpm around the mean, while the Deviation is 4.3616 bpm. This shows the accuracy and reliability of the system. From the result, the temperature readings vary by approximately 1.23 $^{0}$F around the mean. The low variability indicate that the system has a high degree of stability.

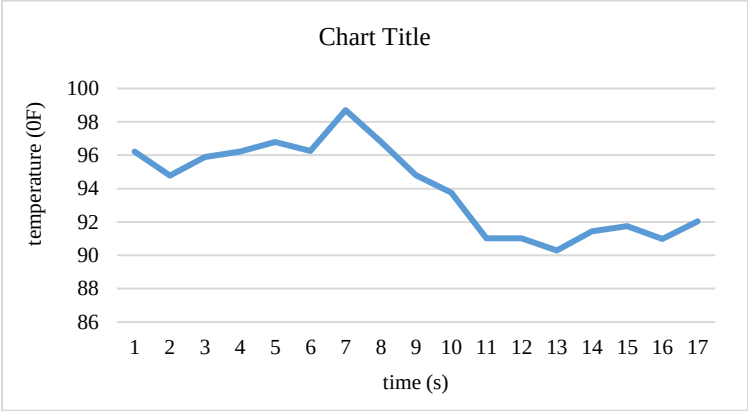



Figure 13. Graph of temperature *vs* time

## 5 CONCLUSIONS

An IoT-based healthcare monitoring system is designed to enhance patient care by enabling real-time monitoring of health metrics through connected devices. This was achieved in this work by utilizing body sensors to continuously collect data, an ESP32 microcontroller which process and sends the data to the internet, SIM900 GSM module to facilitate seamless communication between the monitoring system and the care giver, and a dedicated website interface that records and displays the health parameters. Cybersecurity requirements such as confidentiality, integrity, authentication, privacy, and authorization were also put in place using the 2-way authentication techniques. The system is able to provide real-time monitoring of patient's vital signs remotely, enabling prompt response to any irregularities detected. The effectiveness of the system was evaluated through various tests, demonstrating its reliability and accuracy in capturing vital signs data, Furthermore, the system's ability to promptly alert caregivers or medical professionals in case of abnormal readings enhances its utility in healthcare applications, particularly in remote patient monitoring scenarios, Future enhancements may include integrating additional sensors for comprehensive health monitoring and including of GPS function for Patient Location Tracking.

## REFERENCE


1. Zia, U.A., Mohammad, G.M, Mohammed, J.U., Md. Humayun, K.M.D. and Jiabul H. (2018). Internet of Things-Based Patient Health Monitoring System Using Wearable Biomedical Device. *International Conference on Innovation in Engineering and Technology*, pp. 27-29.
2. Maqbool, S., Iqbal, M.W., Naqvi, M.R., Arif, K., Ahmed, M. and Arif, M. (2020). IoT-Based Remote Patient Monitoring System. *2020 International Conference on Decision Aid Sciences and Application*, pp. 1255-1260.
3. Abdulmalek, S., Nasir, A., Jabbar, W.A., Almuhaya, M.A.M., Bairagi, A.K., Khan, M.A. and Kee, S.H. (2022). IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. *Healthcare*, vol. 10, pp. 1- 10.
4. Singh, S.K., Singh, R.S., Pandey, A.K., Sandeep, S.U., Ankit, C. (2021). IoT-Based Data Analytics for the Healthcare Industry. *Intelligent Data-Centric Systems*, pp. 9-29.
5. Guo, W., Xiong, N., Vasilakos, A.V., Chen, G. and Cheng, H. (2018). Multi-source temporal data aggregation in wireless sensor networks. *Wirel. Pers. Commun*, vol. 56, no. 3, pp. 359-370.
6. Ketu, S. and Mishra, P.K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, vol. 9, issues C, pp. 1-31.
7. Dhanvijay, M.M. and Patil, S.C. (2019). Internet of Things: A survey of Enabling technologies in healthcare and its applications. *Computer Networks*, vol. 153, pp. 113-131.
8. Klochko, O.V., Fedorets, V.M., Mazur, M.V. and Liulko, Y.P. (2023). An IoT system based on open APIs and geolocation for human health data analysis. *CTE Workshop Proceedings*, vol. 10, pp. 399-413.
9. Sodhro, A.H. and Shah, M.A. (2017). Role of 5G in medical health. ICIEECT 2017. *International Conference on Innovations in Electrical Engineering and Computational Technologies, Institute of Electrical and Electronics Engineers Inc*., pp. 1-5.
10. Misran, N., Islam, M.S., Gan, K.B., Amin N. and Islam, M.T. (2019). IoT Based Health Monitoring System with LoRa Communication Technology. *2019 International Conference on Electrical Engineering and Informatics*, pp. 514-517.
11. Sun, X., Zhao, C., Li, H., Yu, H., Zhang, J., Qiu, H., Liang, J., Wu, J., Su, M., Shi, Y. and Pan, L. (2022). Wearable Near-Field Communication Sensors for Healthcare. *Materials, Fabrication and Application. Micromachines*, vol. 13, no. 5, 784.
12. Hassani, S. and Dackermann, U. (2023). A Systematic Review of Optimization Algorithms for Structural Health Monitoring and Optimal Sensor Placement. *Sensors (Basel, Switzerland)*, vol. 23, no. 6, pp. 2-63.
13. Shukla, S. (2023). Real-time Monitoring and Predictive Analytics in Healthcare: Harnessing the Power of Data Streaming. *International Journal of Computer Applications*, vol. 185, pp. 32-37.
14. Chen, Z., Liang, N., Zhang, H., Li, H., Yang, Y., Zong, X., Chen, Y., Wang, Y. and Shi, N. (2023). Harnessing the power of clinical decision support systems: challenges and opportunities. *Open heart*, vol. 10, no. 2, e002432.
15. Mantena, S., and Keshavjee, S. (2021). Strengthening healthcare delivery with remote patient monitoring in the time of COVID-19. BMJ health & care informatics, vol 1, issue 28, e100302. https://doi.org/10.1136/bmjhci-2020-100302
16. Peyroteo, M., Ferreira, I.A., Elvas, L.B., Ferreira, J.C. and Lapão, L.V. (2021). Remote Monitoring Systems for Patients with Chronic Diseases in Primary Health Care: Systematic Review. *JMIR mHealth and uHealth*, vol. 12, issue 9, e28285.

17. Spaulding, A., Loomis, E., Brennan, E., Klein, D., Pierson, K., Willford, R., Hallbeck, M.S. and Reisenauer, J. (2022). Postsurgical Remote Patient Monitoring Outcomes and Perceptions: A Mixed-Methods Assessment. Mayo Clinic proceedings. *Innovations, quality & outcomes*, vol. 6, no. 6, pp. 574-583.

18. Mason, M., Cho, Y., Rayo, J., Gong, Y., Harris, M. and Jiang, Y. (2022). Technologies for Medication Adherence Monitoring and Technology Assessment Criteria: Narrative Review. *JMIR mHealth and uHealth*, vol. 3, issue 10, e35157.

19. Tang, M.S.S., Moore, K., McGavigan, A., Clark, R.A. and Ganesan, A.N. (2020). Effectiveness of Wearable Trackers on Physical Activity in Healthy Adults: Systematic Review and Meta-Analysis of Randomized Controlled Trials. J*MIR mHealth and uHealth*, vol. 7, issue 8, e15576.

20. Antevski, K., Girletti, L., Bernardos, C.J., de la Oliva, A., Baranda, J. and Mangues-Bafalluy, J.A. (2021). 5G-Based eHealth Monitoring and Emergency Response System: Experience and Lessons Learned. *IEEE Access*, vol. 9, pp. 131420-131429.

21. Kang, M. and Chai, K. (2022). Wearable Sensing Systems for Monitoring Mental Health. *Sensors*, vol. 3, issue 22, pp. 1-14.

22. Chukwudebe, G.A., Ogu, R.E. and Fawei, J.E. (2021). Critical Requirements for Sustainable Deployment of IoT Systems in Nigeria. *Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace (Cyber Nigeria)*, pp. 119-126.

23. Muhammad, A.H., Bin, H., Mohammad, I.H., Bin, Y., Muhamad, N.B.I. (2023). Security and Privacy Issues in Internet of Things (IoT). *TechRxiv*, pp. 1-14.

24. Nasiri, S., Sadoughi, F., Tadayon, M.H. and Dehnad, A. (2019). Security requirements of internet of things-based healthcare system: A survey study. Acta Informatica Medica, vol. 27, no. 4, pp. 253–258.

25. Kumar, A., Nag, C.A., Ghosh, D. and Chanda, K. (2018). A Secure Framework for IoT-Based Healthcare System. *Proceedings of International Ethical Hacking Conference Advances in Intelligent Systems and Computing*, vol. 811, pp. 383-393.

26. Kuo-Hui, Y. (2016). A Secure IoT-based Healthcare System with Body Sensor Networks. *IEEE Access*, pp. 10288-10299.

27. Badiganti, P.K, Peddirsi, S., Rupesh, A.T.J. and Tripathi, S.L. (2022). Design and implementation of smart healthcare monitoring system using FPGA. *In Proceedings of First International Conference on Computational Electronics for Wireless Communications*, pp. 205-213.

28. Springer, S. S., and Biswas, S. (2018). Secure Data Transmission Beyond Tier 1 of Medical Body Sensor Network. Proceedings of International Ethical Hacking Conference. *Advances in Intelligent Systems and Computing*, vol. 811, pp. 405-418.

29. Latha, K., Sravanth, G., Pavan, K.V. and Nagarjuna, B.V.S. (2020). An IoT based Patient Monitoring System using Arduino uno. *International Research Journal of Engineering and Technology*, vol. 7, issue 7, pp. 3170-3174.

30. Bhuiyan, M.N., Billah, M.M., Bhuiyan, F., Bhuiyan, M.A.R., Hasan, N., Rahman, M.M. and Niu, M (2022). Design and implementation of a feasible model for the IoT based ubiquitous healthcare monitoring system for rural and urban areas. *IEEE Access*, vol. 10, pp. 91984-91997.

31. Zouka, E.H.A. and Hosni, M. (2021). Secure IoT communications for smart healthcare monitoring system. *Internet of Things (Netherlands)*, vol. 13, pp. 1-14.