Blood Pressure Monitoring System using Remote and Secure Data Transmission

Christopher James Labrador*, Gillian Claire Cancio, Krizia Dianne Congson,
Kerr Jason Quevedo, Rhea Ann Verallo, and James Michael Cañete
Department of Computer Engineering, University of San Carlos, Philippines, 6000
cjmlabrador@usc.edu.ph, gilliancancio@gmail.com, kdcongson@gmail.com
boiboigq@gmail.com, rheaannverallo@gmail.com, jmccanete@usc.edu.ph

Abstract

Health and vitals monitoring trend has risen in the medical industry. The aid of technology on medical measurements and procedures has revolutionized medical evaluations which minimized time allocation and human errors in the industry. Technology also paved the way to advance medical services by providing data from monitoring devices for analytics in patient assessment and evaluation. That said, it is also essential that a patient's record will be secured and confidential as it undergoes system processes. This study focuses on the remote and secure transmission of data within a multi-node system that is centralized in blood pressure monitoring. This will present ideal devices, protocols, and procedures to realize how data can be transmitted from one component to the other while incorporating security techniques to serve its purpose for medical analytics.

Keywords: Internet of Things (IoT), Bluetooth, LoRaWAN, ESP32, Blood Pressure

1 Introduction

Health of the people is an important factor in a developing country. This presents that when people are healthy, it helps in the country's cumulative level of economy, thus, improving a person's lifestyle and dynamics. This is one of the reasons why health presents a great challenge to the country, and people are finding ways in order to improve health and seek for methods to easily access help when addressing important health issues. Developing countries, such as the Philippines, are faced with a great number of patients with hypertension - one of the leading causes of death. The World Health Organization (WHO) has estimated that, by the year 2025, the amount of people who will experience hypertension would be more than 1.56 billion worldwide [1] .

Constant technological evolution in different fields has addressed the needs of the people in ways that it makes things easier to access. In the perspective of the medical industry, innovative devices such as wireless body sensors and digital wearables have emerged and have been widely used globally with the aid of technology. This capacitated the industry to monitor patient vitals remotely, assess changes and fluctuations in medical status, process and store confidential data securely within a closed system, and more. That said, this has revolutionized the procedures in the medical industry in terms lessening cost in time and manpower and providing more accurate and unbiased readings obtained from advanced devices.

It is integral that there exists a patient record confidentiality as stated in Article II Section 6 of the Philippine Medical Association Code of Ethics that "the physician should hold as sacred and confidential whatever may be discovered or learned pertinent to the patient even after death, except when required in

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 6, Article No. 11 (December 15, 2020)
*Corresponding author: Department of Computer Engineering, University of San Carlos, Talamban, Cebu City, Cebu, Philippines, 6000, Tel: +63-32-230-0100 local 263.

the promotion of justice, safety, and public health". This, therefore, holds firm on the concept that each patient data recorded should be made only between a doctor and a patient. It is still a matter of importance that the technological incorporation in data monitoring should not be exempted from the written code. No matter which angle it is viewed, a technological innovation with lackluster security performance would not be a recommended monitoring alternative in the medical industry. Ergo, it should be emphasized that this code is universal.

1.1 Background of the Problem

Developing countries are usually faced with problems related to health because they cannot afford good medical care [2] . It is unfortunate that the Philippines is one of the countries that encounter such problems. One of the major causes of mortality in our country is High Blood Pressure or Hypertension. According to the Department of Health [4], out of 514,745 registered deaths in 2013, 118,740 of which are caused by heart disease. Dr. Amado Nazal, medical director of Pharex Health Corp, stressed the importance of regular blood pressure monitoring of patients diagnosed with high blood pressure [1].

Regular and personal check up and evaluation by a medical professional is one problem that patients experience especially those who live in remote provinces. Time and lifestyle factors affect this type of occurrence. Accuracy in blood pressure data collection can be faulty especially in an environment where medical staff is often rushed or do more load than they can carry due to understaffing [7] . Given the current resources such as microcontrollers and digital measuring devices, it is now easier to come up with a new system to address these issues. Providing a solution that is accessible, portable, and secure is necessary.

Internet of Things (IoT) is the emergence of networks that interconnect constrained devices that transmit and receive data. Constrained devices like Radio-Frequency Identification (RFID), which is a minute electronic device capable of providing a unique identifier for an object, smart cards and sensors that are able to gather data and send it over a network towards the receiver for data processing. If implemented properly, remote monitoring is possible. Together with IoT, several other wireless transmission media have emerged to address data communication in a more advanced and resilient way through the use of wireless modules in a system network. However, the network should not only focus on the transmission of data. IoT, itself, is not different from the networks available in the market in terms of security. It is also capable of network attacks such as Denial of Service (DOS), Brute Force, Man in the Middle and more. A mishap in the security protocol may lead to loss of life, asset and integrity.

Due to the characteristic of IoT, cryptographic algorithms should complement the constrained resources of the device used. That being said, creating a system that remotely and securely monitors blood pressure is possible but it needs further research to provide a solution that is low-cost, secure and available.

1.2 Goals and Objectives

Goal of this study is to provide a system that can support a remote blood pressure monitoring through secure data transmission using lightweight cryptography using of Internet of Things.

- To enable communication between a Microcontroller, NodeMCU ESP-32, to upper arm blood pressure monitor via Bluetooth communication.

- To develop a web application that will display the cumulative blood pressure data of the patient. This will enable the attending physician to keep track of the blood pressure of the patient.

- To securely transmit recorded data from the upper arm blood pressure monitoring device to the web application through the implementation of Elliptic Curve Integrated Encryption Scheme (ECIES) and Elliptic Curve Diffie-Hellman (ECDH).
- To implement a network transmission protocol that is suitable for low-power microcontrollers through the implementation of Long Range Wide Area Network (LoRaWAN).

1.3 Scope and Limitation

This study focuses on three fundamental areas which play an important role in the progression of the study. These are (1) finding the appropriate modules/devices to deliver the data from the system using the lowest power and longest range possible, (2) remotely delivering data from the sensor node to the other nodes (LoRa node, MQTT node, Application node) using the selected wireless transmission medium, and (3) securely delivering the integrity of data to the system nodes. The study will be essential to create and build the system in accordance to the goals and objectives of the study that focuses on low power-consumption, secure data-encryption, long-range device IoT implementation. The results of the readings of the device in the study would be done or further discussed in this paper.

In terms of data gathering, indicator levels (Level 1, Level 2 and Level 3) that identifies the normal, warning and critical stage of the blood pressure of the patient, will be indicated based on his/her medical assessment (age).

This study is limited to the three fundamental parts mentioned above. The type and life of the energy source of the device will be a part of the system but will not be a part of the study. The current implementation of the study is limited to the microcontroller used in the study, which is Heltec ESP32.

2 Related Work

Over the last decade there have been numerous developments in technology which interconnects devices to suit man's lifestyle. From cellular phones evolving to smartphones, to watches that do not only tell time but also allow users to answer calls, monitor heart rate and even sync data to devices.

All of these are products of the emerging platform of Internet-of-Things (IoT). As this trend is rising, one of the most prominent areas it has been applied to is healthcare. According to Niewolny (2013), it is particularly useful in clinical care, remote monitoring and early intervention/prevention [13]. The difference between IoT in healthcare from the traditional healthcare is the data acquired. Traditional healthcare deals with clinical data, that is gathered when patients submit themselves for tests or consultation. Meanwhile, IoT in healthcare measures lifestyle data through the noninvasive wearable tech worn by the user [15]. Furthermore, digital health advisors have emerged in smartphones, as stated by Dimitrov (2016), which would interpret and analyze health and well-being of the patient [6]. With the advantages stated above, researchers are taking steps to create solutions that are lightweight in terms of power consumption, portability and robustness.

With the emergence of the Internet of Things, industrial innovations took its place in the advancement of collecting and processing data from the interconnected entities in the system. As IoT is becoming more popular, so are the wireless media used for network connections. One particular medium is the LoRaWAN which has a large area radius range and low power consumption [8].

In the study of M. S. Mahmoud and A. A. H. Mohamad (2016), they focused on the efficiency of power consumption in wireless communication techniques that would be applicable for Internet of Things applications [8]. They stated that there are three things to consider in selecting the wireless technology to be used. First is the maximum throughput, next is the power consumption and lastly the maximum distance range. For short range connectivities, Wi-Fi has been used despite its tremendous

Table 1: Spreading Factors and their corresponding Ranges, Time on Air, and Bitrate

Spreading Factor ($at 125kHz$)	Bitrate (bps)	Range (km)	Time on Air (ms)
SF7	5470	2	56
SF8	3125	4	100
SF9	1760	6	200
SF10	980	8	370
SF11	440	11	740
SF12	290	14	1400

power consumption. In the study conducted it was found out that for the long range connectivity and low power consumption, LoRaWAN is the best candidate protocol.

There are many protocols specifically designed to fit IoT's characteristic [16]. One of which is Mdhaffar et.al (2017)'s IoT-based health monitoring via LoRaWAN [10]. Their paper, made use of LoRaWAN, to monitor blood pressure, glucose and temperature. In their research, experiments were conducted to measure the area coverage of the network as well as its power consumption. With this, they concluded that LoRaWAN's power consumption is significantly lower than long range cellular solutions, such as GPRS/3G/4G.

According to the study of F. Adelantado et. al (2017), they analyzed LoRaWAN on what it can do and what it cannot do [4]. They inspect it according to its capacity and the limitation of its network size. First they put into consideration the duty cycle which determines the limitation of the network size. Spreading Factor (SF) is used in transmitting each frames and the higher the SF is, the longer the distance or range of the communication. SF is defined as the log_2 of the chip rate (R_c) over the symbol rate (R_s),

$$SF = log_2(R_c/R_s) \tag{1}$$

Differences in the bitrate, range, and time on air with respect to its spreading factor is illustrated in Table 1. From it we can see that the higher the spreading factor is, the larger is its range. However, this also denotes an increase in air time which results to slower data transmission ending in an off-period duration [4].

According to the study of K. Mikhaylov et.al, as the number of devices increases, the performance rate of LoRaWAN decreases [12]. They further put into consideration the reliability and densification drain network capacity of LoRaWAN. Its reliability is attained by recognizing the frames in the downlink. For the different classes of LoRaWAN there are different ways in transmitting frames. In the end devices in Class A, acknowledgement is sent in one of the vacant receive windows. In the end devices in Class B, acknowledgment is sent either in one of the vacant receive windows or in a supplementary time-synchronized window. Lastly in the end devices in Class C, acknowledgement can be sent at an unspecified time [4].

According to Michaelski (2017), LoRaWAN's transmission begins in the end nodes which consists of the sensors. Once sensors have gathered data, the end nodes send a signal to the nearest gateway. The data in the gateway uses Frequency Shift Keying (FSK), in order to efficiently transmit data towards the server, Chirp Spread Spectrum (CSS) is applied. Once data has entered the gateway, it comes in chirps or symbols of digital information which is then transformed into a frequency domain and lastly, into a modulated signal for efficient transport. The gateway and the network server is connected through standard IP connections, like Ethernet or 3G [11].

In the context of implementing a system designed for constrained devices and low-bandwidth Message Queue Telemetry Transport (MQTT) is an ideal choice as a messaging protocol. In a study conducted by Pal, Sumpit, et. al, (2007), they stated that MQTT has a small mail box for communicating

with other MQTT applications connected to its server. This mechanism enables MQTT applications to conserve battery life [14]. This property of MQTT makes it suitable for lightweight systems. Furthermore, MQTT works on a publish/subscribe protocol and to enable connection between server and client, the client send a CONNECT message to the MQTT broker which, in return, will reply a CONNACK message if connection is established. Only after the establishment can the client publish/subscribe to a topic. The topic is the only information circulating around the broker and it is what the clients can subscribe into which enables security because the clients don't need to know each other rather only communicate over the topic. Whenever a client wants to obtain information, it must subscribe to a topic in the MQTT broker which will then check if that client has the right to access the data. On the other hand, if a client wants to send something over the network, it must publish a topic. In their research, they concluded that it is feasible to send sensor data from one client to another through the MQTT protocol[14].

IoT's ability to interconnect different entities is still very prone to network attacks such as Denial of Service (DOS), Man-in-the-middle, Eavesdropping, Masquerading, Saturation and Differential Attack [5]. Lapses in data security, may lead to disastrous events and may eventually lead to loss of life. In that light, privacy constraints from legislations such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) were implemented. With this, security in Healthcare IoT systems must assure the confidentiality of the data being transmitted [9].

Encryption of LoRa Packets makes use of symmetric keys known to the Node, the Network Server and potentially the Application Server behind the system. Messages that pass through the LoRa channel are encrypted through AES-128 in counter mode (CTR). Man-in-the-middle attacks are then prevented because the symmetric keys (App Session Key and Network Session Key) used are only known by the Node and the Network Server.

AES-128 is a classification of Advanced Encryption Standard algorithm which is a block cipher encryption algorithm published by National Institute of Standards and Technology way back in the year 2000 [3]. This encryption scheme has the capability to protect data from attackers and prevents them from breaking the encrypted data.

3 Methodology

3.1 Conceptual Framework

Figure 1 shows the system's conceptual framework. Being IoT-integrated, a network of different nodes are present in the diagram. The data gathering starts from the BP Monitor which transmits the blood pressure reading, via bluetooth, to an Android device application. Further data transmission is performed over a LoRaWan network, passing through a LoRa transceiver connected to the MCU and forwarded to the LoRa gateway, respectively. Communication between the Network Server and Database transpires with the aid of the MQTT Broker which is responsible for receiving messages and distributing them to authorized users via its publish/subscribe protocol.

3.2 Data Flow Diagram

Data flow is illustrated in Figure 2 showing how the data is relayed from each and every node in the system. The data running through the system are blood pressure data and web application user (Doctor) credentials and information.

Functions available to the user is to measure blood pressure, which will be encrypted in the ESP-32, remotely sent to the LoRaWAN network, enter the network server and forwarded to the MQTT broker, where the data is stored in the database (Firebase). On the medical attendant's end, login credentials will be asked for identity verification. This is one way of protecting the confidential data. After the blood

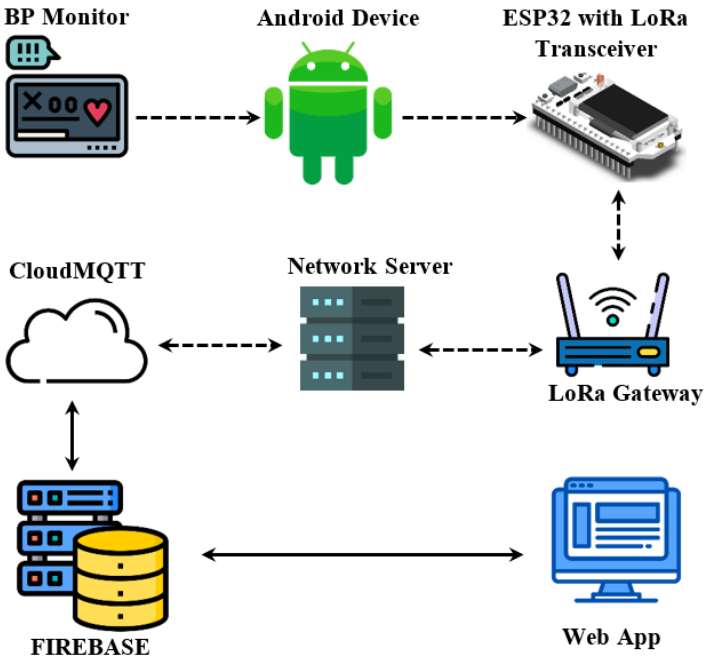


Figure 1: Conceptual Framework of the system together with the devices involved

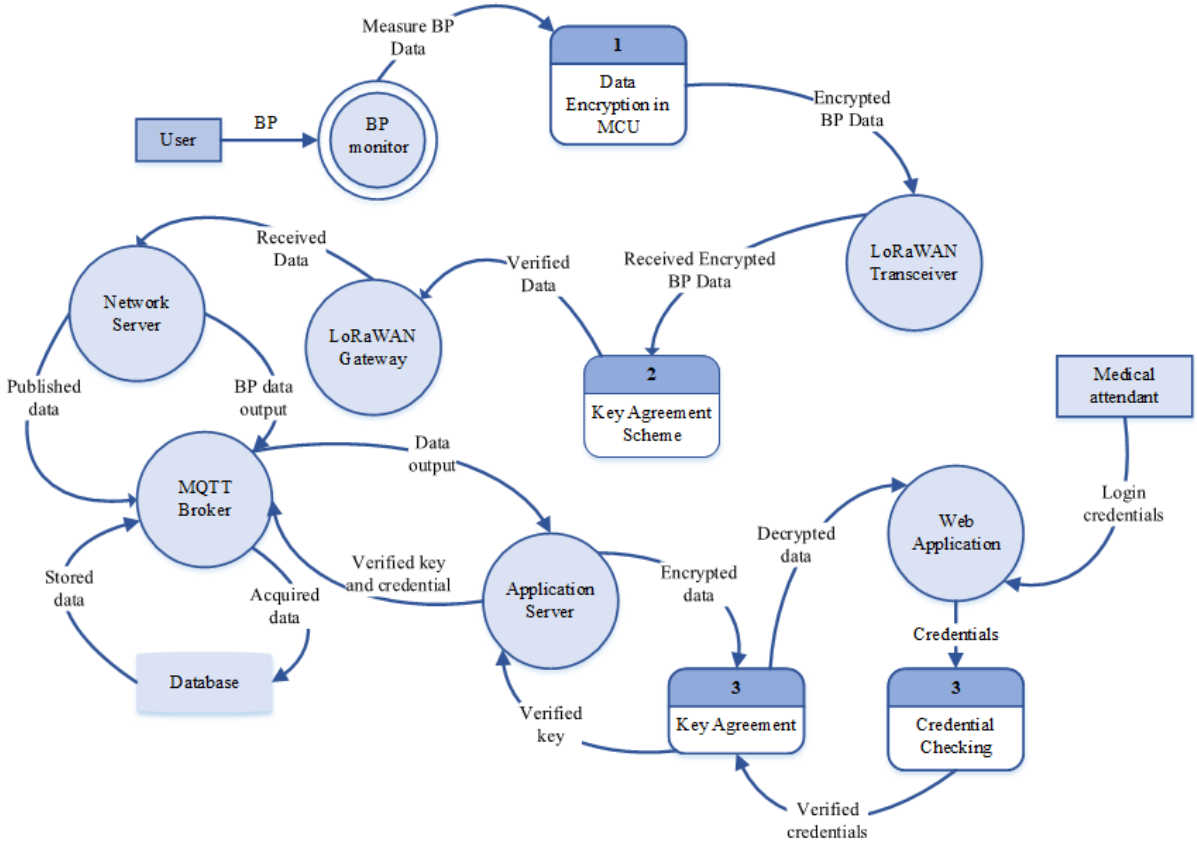


Figure 2: Data Flow diagram

pressure data measurement, AES will be performed to ensure that the encrypted data is secured. Once the node completes and verifies the security requirements, such as identification of Network and Application Session Keys, it will send the decrypted data to the database, and display it to the web application.

3.3 Procedure

Activities in the system are illustrated in the main system flow (refer to Figure 3). The data gathered by the microcontroller from the BP monitor is encrypted before the transmission. Data transmission from the microcontroller to the database is done wirelessly and over the LoRaWAN and MQTT. Once the symmetric keys needed for further operation has been verified, the data goes through the MQTT broker and is stored to the database. The system checks for doctor's request for access, and if a request is available, the system verifies its credentials, else the system continues to wait for request. The patient data will be decrypted as it reaches the database and those data will be displayed on the web application using a verified user with correct credentials.

Using an Omron Automatic Upper Arm Blood Pressure Monitor with IoT Starter Kit, blood pressure data taken after a patient performs a measurement will be sent to an Android device via Bluetooth. This means that the patient will have to turn on the BP device first. The Android application publishes the measured data to the ESP32 for encryption before it will be transmitted on air. Since the Android

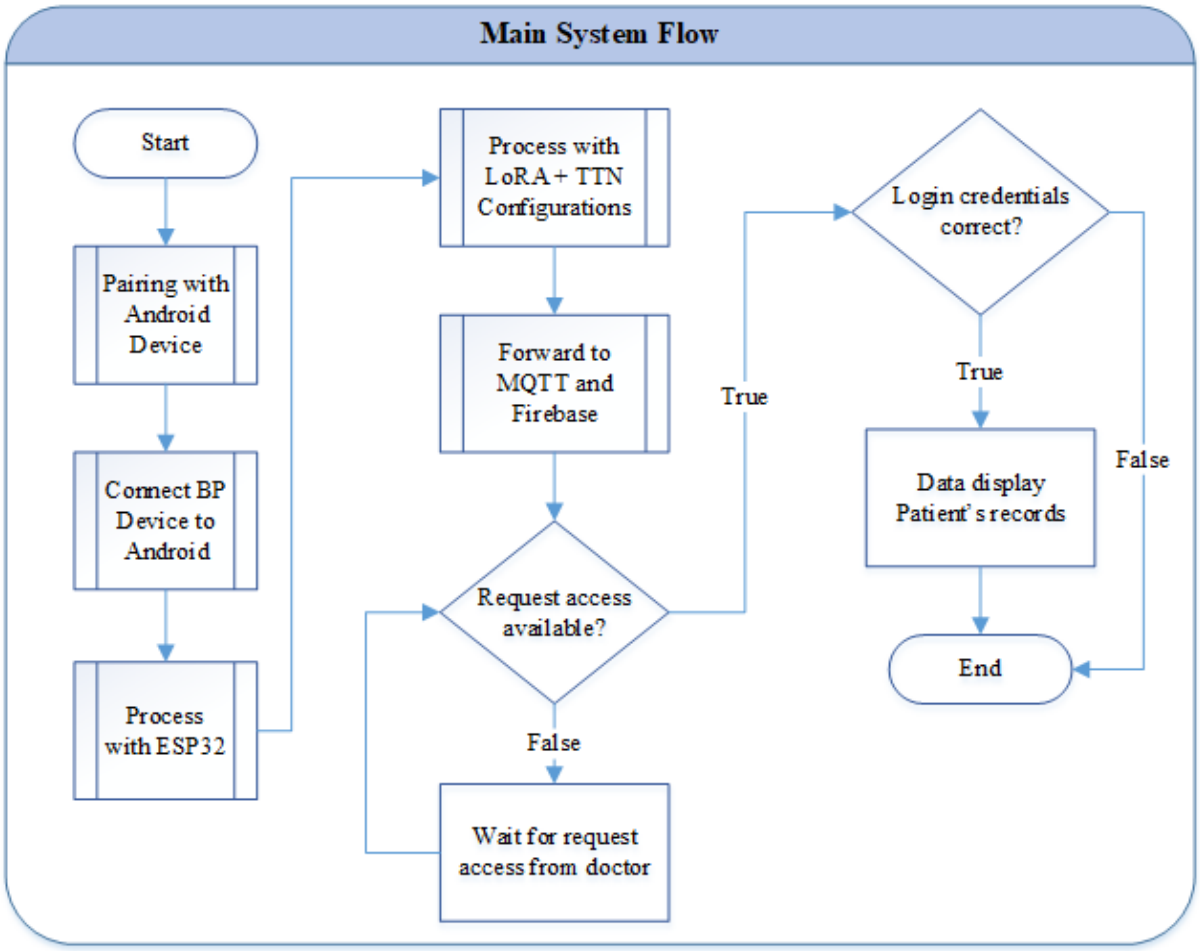


Figure 3: Main System Flow

application gathers the measurement frequency of the patient, it will have the capacity to alert the patient when he/she needs to take the blood pressure reading as prescribed by the doctor.

In order to secure the integrity of the LoRa channel, the LoRa packets are encapsulated to include LoRa frames, and the message/payload encrypted using AES-128 in CTR mode.

Data received by the LoRa Public Gateway is stored in the Database along with the patient's identification. In order to access the patient's information, the doctor is required to provide his credentials. If the credentials submitted are authorized to access the patient's information, the web application will display the patients and patient data/information to the doctor.

A LoRa Transceiver is used in the system. The transceiver, attached to the MCU, searches for the nearest gateway it could find. The gateway is established as a hat on a RaspberryPi node. This gateway receives the encrypted data from the MCU-Transceiver node which it forwards to the network server for further data processing.

As for the system to receive the data, a public gateway is needed thus implementing it accordingly. The implementation of the public gateway needs two (2) requirements; the software components and the hardware components - Rasbian OS, and Single Channel Packet Forwarder, Raspberry Pi ver 2/3, Dragino LoRa Hat 433 MHz and a microSD card.

Assembling the necessary hardware components should be accomplished before implementing the software component. The Lora Pi hat should be mounted to the Raspberry Pi considering the pin configuration of the Raspberry Pi. In the Pi hat, orienting the antenna wisely would be crucial in terms of range and line of sight of the end nodes. After mounting the Pi hat in place and having the antenna in a good angle, insert a microSD card where a Raspbian OS is installed. Next, a single-channel packet forwarder needs to be installed to enable the LoRa Hat functionality. After everything installed, proceed to building the channel of the gateway.

MQTT broker will listen and is always ready to receive data from any network client. It will serve as the middle-man between the sensor network, which contains the BP node, LoRa gateway and Network server, and the web application. After the sensor network gathers the blood pressure data of the patient, it will subscribe to the broker which, then, publishes the data to the database and stores it. The database publishes the data to the web application.

User interface will be done through a web application where the patient's medical attendant can see his/her data. These data include personal information and the blood pressure data that is being transmitted in the multi-node system.

Required functionalities include a login page which would land into a homepage, once credentials have been authenticated, that would contain menus for the following: (1) user/medical attendant information, (2) patient list that would require verification through password upon opening, which will then enable him to furthermore access his patients' profile with medical record display, and (3) a notifications panel.

Credential verification is done on the login page. This is to ensure that they are the one logging in, the patient listed is correctly assigned to them, and they have knowledge of the password to display the confidential patient data. The patient's profile will have to enlist the patient's information and blood pressure measurements. Before the user can see the patients, he/she should have authenticated credentials by encoding the password used upon login. The profile should also have the patient's contact information so the medical attendant can assess the data being transmitted into the system from the patient's BP monitor.

Along with these, a notification panel should be present in order to inform the medical attendant that the device has finished measuring the blood pressure of the patient and the data has been sent over to the network. Figure 4 will show the Use Case diagram of the user interface. The diagram will present the pages that will be available on the user interface along with their corresponding functions to meet the system's ends.

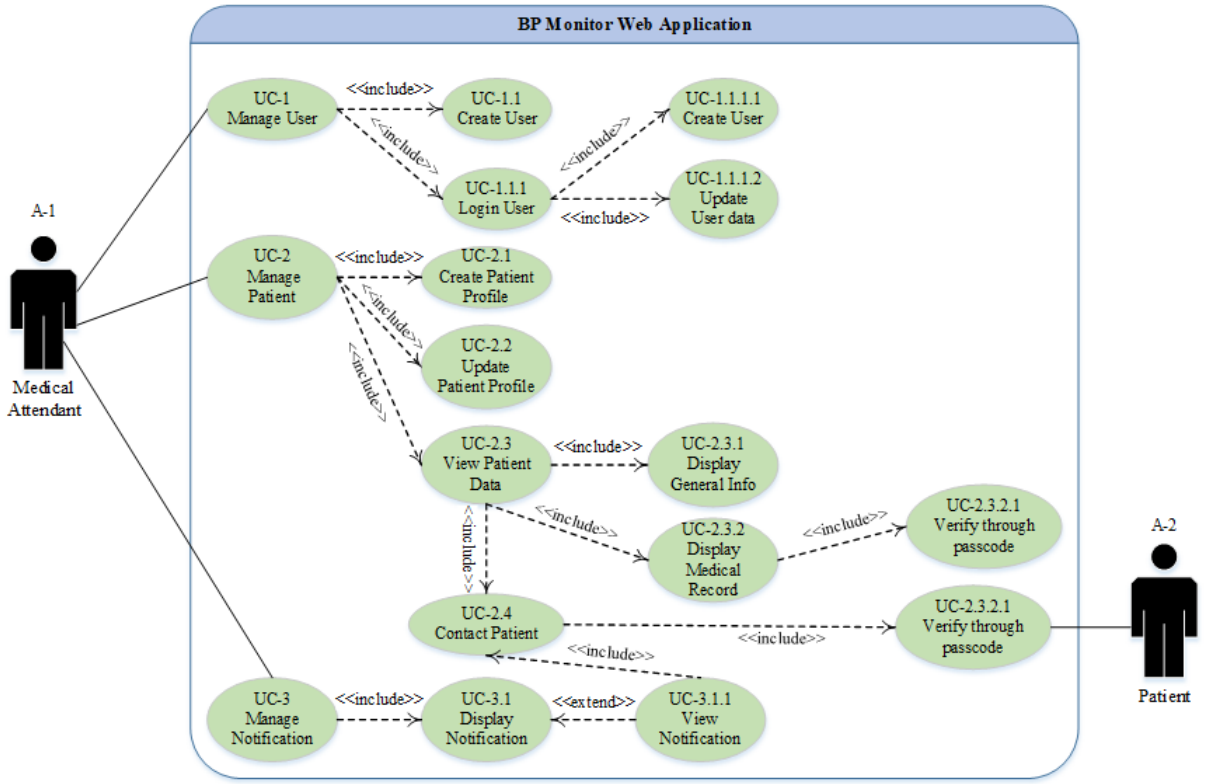


Figure 4: Use Case Diagram of the User Interface

Based on the use cases, the web application will be able to show the patient's medical record history. A bar graph will also be included to show the patient's blood pressure rate with respect to time. The bar graph will have the indicator levels to determine whether the data recorded is normal, borderline, or high.

As per the indicator, each patient will be assigned a normal rate that will be based on their age. Figure 6 shows a normal blood pressure reading in relation to its equivalent average demographic counterpart. The table shows each age range and the blood pressure stages defined as hypotension (low), normal, pre-hypertension (borderline), hypertension stage 1 and 2 (high). This will be the default basis for the proposed system (with the exemption of hypotension).

In terms of leveling, the patient data record will have an indicator, as mentioned. For Level 1 indicated in green (normal), there will be regular monitoring. The first trigger factor will be Level 2 - indicated in orange- which means that there needs to be a consultation, personal or remote, with the doctor. Level 3 (high) which will be designated with color red is the highest level and would imply that there should be an immediate emergency response. Systolic and Diastolic measurements are differentiated based on the shades of its colors. Thus, a darker shade of green indicates a normal systolic measurement, and a lighter shade indicates a normal diastolic measurement. The same representation goes for the other levels.

For consultation purposes, the patients will need to have their contact information such as email address and contact number on their profile so the doctor can easily contact them. Levels 2 and 3 require medical attention so patient notification is advised. Additionally, if the physical consultation is urgent (Level 2 and 3), the system will automatically send a notification to the patient that there is a need for him/her to have physical consultation. The system includes a script that would automatically forward an SMS notification to the patient, should the need arise.

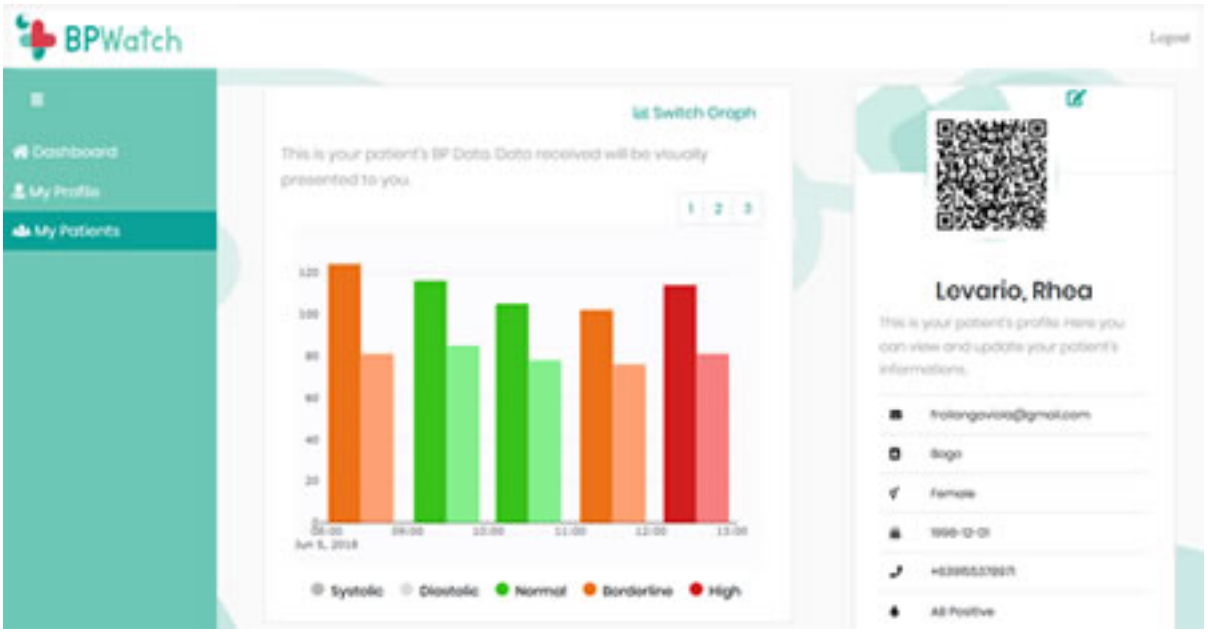


Figure 5: Web Application

Age	Hypotension (Low BP)		Normal BP		Prehypertension		Hypertension Stage 1		Hypertension Stage 2	
	S	D	S	D	S	D	S	D	S	D
17-19	< 90	< 60	< 120	< 85	< 120	< 80	<140	< 89	< 150	< 100
20 - 24	< 90	< 60	< 120	<79	< 125	< 82	<140	<85	<150	< 100
25 - 29	< 90	< 60	< 121	< 80	< 132	< 83	< 140	< 88	< 150	< 100
30 - 34	< 90	< 60	< 122	< 81	< 134	< 85	< 140	< 90	< 160	< 100
35 - 39	< 90	< 60	< 123	< 82	< 135	< 86	< 142	< 91	< 162	< 101
40 - 44	< 90	< 60	< 125	< 83	< 137	< 87	< 144	< 92	< 164	< 102
45 - 49	< 90	< 60	< 127	< 84	< 139	< 88	< 146	< 93	< 166	< 103
50 - 54	< 90	< 60	< 129	< 85	< 141	< 89	< 148	< 94	< 168	< 104
55 - 59	< 90	< 60	< 131	< 86	< 143	< 90	< 150	< 95	< 170	< 105
60+	< 90	< 60	< 134	< 87	< 146	< 91	< 153	< 96	< 173	< 106

S: Systolic Pressure *D: Diastolic Pressure*

Figure 6: Blood Pressure (BP) Chart based on Age

Post-processing features of the system includes data storage. In a study conducted by Berthelsen (2014), a system that gathers data from diverse sensors needs to implement NoSQL Databases. The advantages of NoSQL Databases include highly flexible data modeling and better scalability, which plays a critical part in the implementation of IoT systems. In the current study, Firebase is used as the database for the current system's post-processing features. With its features like real-time database, authentication, cloud storage and hosting, Firebase is the best fits the current system.

3.4 Software and Hardware Requirements

The user shall be equipped with an upper arm cuff BP monitor that will be paired to an Android device. A Heltec ESP-32 with LoRa transceiver attached for LoRa transmission. The minimum requirements of the BP monitor is Bluetooth connectivity and the memory function. The doctor shall be equipped with

a Desktop computer. The minimum requirements of the desktop computer is internet connectivity and a web browser. The NodeMCU ESP-32 must be able to transmit data to the server wirelessly through a LoRa gateway. A LoRa public gateway is required in order to implement data transmission in the network.

3.5 Testing Plan

System testing is considered a set of investigative processes that a system must undergo to ensure the quality of the system. Negligence in system testing may lead to system failure which may cause harm not only to the users but also to the company. Thus, the types of testing that is carried out by the researchers are the following: endurance testing and beta testing.

Endurance testing is done with the developers which will serve as the initial system testing to check how the system will act in long-term usage. The final testing which is beta testing is done with the users to check if the system gathers the blood pressure data during the time set by the doctor and sends the accurate data to the database which will then be displayed in the web application.

Beta testing is executed in three (3) days. Two doctor accounts were be created which were monitored by the researchers. Furthermore, three (3) blood pressure readings were sent over the network coming from one (1) actual blood pressure reading where the BP device will be used, and two (2) generated signals. Doctor A was assigned to one generated signal which sends data within an hourly interval. Doctor B, however, was assigned with a generated signal, which also sends data within an hourly interval, and an actual blood pressure reading, which sends data in an interval depending on how often the doctor needs the hypertensive patient's blood pressure reading. This set-up is for the researchers to check if the network can handle data traffic. The patient can use the device in the comfort of his office as long as it is connected to the gateway.

This study addresses the problem of mortality rate caused by hypertension in rural areas. This is done by providing constant monitoring through a blood pressure system that uses remote and secure data transmission. Furthermore, the researchers make a comparison if the data stored in the blood pressure device and displayed in the web application are the same. This is to verify the credibility of the system since inaccuracies in data read by the device and sent over the network will result to inappropriate diagnosis by the doctor.

The data can be viewed by the doctor in a form of graph, where all the readings are plotted, which is a part of the web application. The data that has been stored in the blood pressure monitor and the data that has been transmitted in the network would be put in table form for easier comparison and analysis. In order to compare if the data that has been transmitted has no error, the received data in the database will be put side-to-side with the data prior to encryption.

4 Results and Data Interpretation

As far as tests go, the first day testing experienced fluctuations in relaying the data coming from the dummy signals relayed to the database. As shown in figure 7, the first day testing in Scenario A and B has a 50% success rate (2 fail and 2 success) of data reception on the database. On the first day, Dummy A and Dummy B used the same microcontroller which continuously sent data. Meanwhile, the actual data used a separate microcontroller reserved solely for that purpose. The successfully received data were completely stored on the database. However, the reception failure was due to human error resulting for monitoring operation on the microcontroller to terminate. Restarting its monitor yielded an error, so the microcontroller was flashed. Because of this, both the microcontrollers used the same device ID. Failure in data transmission was due to downlink error in the TTN. The TTN used downlink

scheduling in MQTT API, in which it replaced the currently scheduled downlink. Since all devices used the same LoRa device ID, only one payload was forwarded to the MQTT API, the rest were either replaced/overlapped. For day 1, a total of 12 data packets were transmitted but only 66.67% of all the data completed the transmission from both ends of the system (BP Node to WebApp).

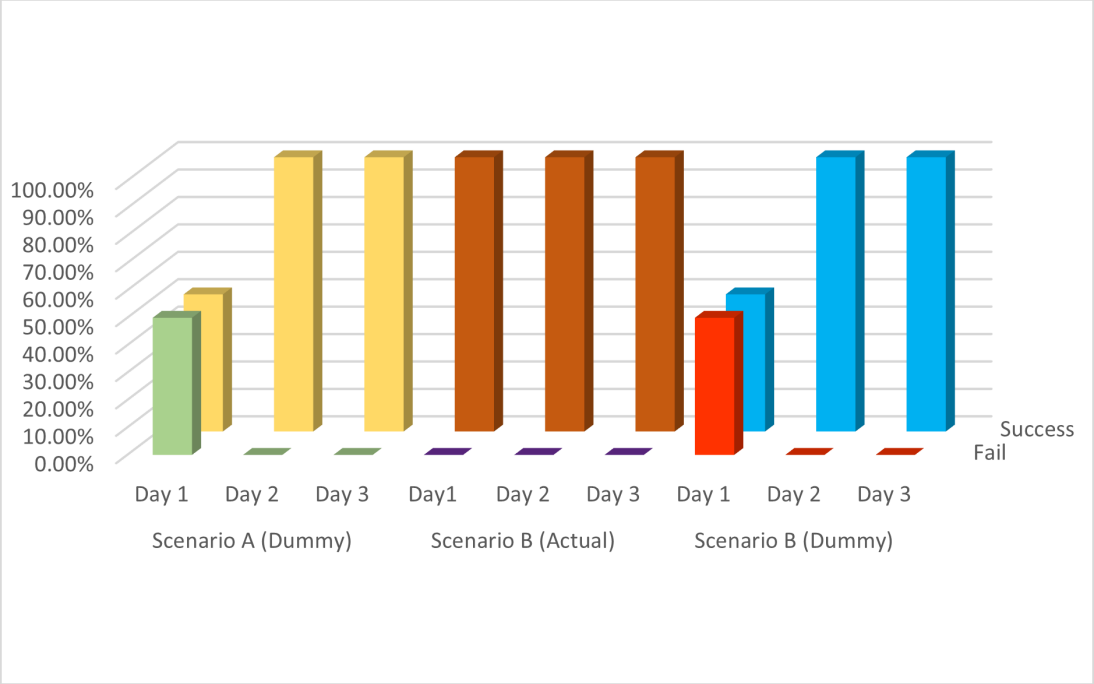


Figure 7: Data Reception Success Rate

Second day testing produced accurate results as the bugs that have occured during the first day testing were fixed. The error in using similar LoRa Device ID was traced hence, the microcontrollers were flashed with different LoRa ID. This time Dummy A, B, and Actual Data used different microcontrollers. A hundred percent of all the eighteen (18) data packets were transmitted successfully from both ends of the system. The data packets were sent with an average of about 3 seconds apart.

For the last day of testing, accurate data results continued to be produced by the system. Like the second day, a hundred percent of all the data sent from the end devices appeared on the web application of their corresponding doctors.

4.1 Deployment and Maintenance

In the deployment stage of the system, the researchers provided instructional media with regards to the system operation. The media are in print, visual, and/or personal instructions (depending on the availability of the researchers) through demonstration on the system's usage. The patient is able to measure blood pressure data from his/her blood pressure monitor. On the other end, the medical attendant have access to the data acquired from the system and use it to assess the patient's condition for further medical procedures.

Default contact information of the researchers are affixed with the product for reachability in cases of system concerns. This is for the users of the system to address their inquiries and complaints should there be system bugs or dysfunctionality.

4.2 Major Ethical Considerations

Ethical considerations pertain to how the actions of others may impose harm to other people. Three critical issues in conducting research are the following: respect for privacy, harmlessness of the act, and informed consent. Since the research involves medical data of the patient, which is considered as confidential, the data gathered by the system should be protected. To ensure the privacy of the user, the proposed system will only allow data access to the designated healthcare attendants of the patient. Furthermore, the system will also make sure that the data is secured during transmission and that no embezzlement of data will be done. After the study, the researchers will delete all information provided by the participants to ensure data privacy. Lastly, the data that the researchers gathered will be solely intended for the purpose of the research with the consent of the testers.

5 Recommendations

For future researches, the researchers recommend to use hardware devices that are easily compatible with each other in terms of workability. It is recommended to use an MCU with LoRa transceiver having the same frequency plan as the LoRa Gateway being used. It is also recommended to use a Blood Pressure Monitoring device that is IoT-ready since it has features that are non-proprietary and can be integrated when creating such a system.

References

[1] More than 1b people expected to have hypertension by 2025. `http://www.philstar.com/health-and-family/2015/10/27/1515383/more-1b-people-expected-have-hypertension-2025`, 2015. [Online; accessed 16-November-2020].

[2] What are problems faced by developing countries? `https://www.enotes.com/homework-help/what-are-problems-faced-by-developing-countries-544853`, 2015. [Online; accessed 16-November-2020].

[3] A. Abdullah. Advanced encryption standard (aes) algorithm to encrypt and decrypt data. 06 2017.

[4] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne. Understanding the limits of lorawan. *IEEE Communications Magazine*, 55(9):34–40, 2017.

[5] I. Batra, A. K. Luhach, and N. Pathak. Research and analysis of lightweight cryptographic solutions for internet of things. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, ICTCS '16, New York, NY, USA, 2016. Association for Computing Machinery.

[6] D. V. Dimitrov. Medical internet of things and big data in healthcare. *Healthcare Informatics Research*, 22(3):156–163, 2016.

[7] J. Handler. The importance of accurate blood pressure measurement. *The Permanente Journal*, 13(3):51–54, 2009.

[8] M. S. Mahmoud and A. A. H. Mohamad. A study of efficient power consumption wireless communication techniques/ modules for internet of things (iot) applications. *Advances in Internet of Things*, 6(2):19–29, 2016.

[9] K. Malhotra, S. Gardner, and R. Patz. Implementation of elliptic-curve cryptography on mobile healthcare devices. pages 239 – 244, 05 2007.

[10] A. Mdhaffar, T. Chaari, K. Larbi, M. Jmaiel, and B. Freisleben. Iot-based health monitoring via lorawan. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, pages 519–524, 2017.

[11] T. Michaslki. Explaining lorawan. `https://ubidots.com/blog/explaining-lorawan/`, Mar 2019. [Online; accessed 16-November-2020].

[12] K. Mikhaylov, J. Petäjäjärvi, J. Haapola, and A. Pouttu. D2d communications in lorawan low power wide area network: From idea to empirical validation. In *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 737–742, 2017.

[13] D. Niewolny. How the internet of things is revolutionizing healthcare. `https://www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf`, 2013. [Online; accessed 16-November-2020].

[14] S. Pal. Study and implementation of environment monitoring system based on mqtt. 03 2017.

[15] R. Pugh. A future of mobile-centric healthcare could save lives. `https://www.theguardian.com/healthcare-network/2016/aug/05/future-mobile-centric-healthcare-save-lives`, 2016. [Online; accessed 16-November-2020].

[16] P. Sethi and S. Sarangi. Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017:1–25, 01 2017.

Author Biography

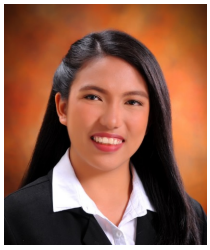
Christopher James M. Labrador received his B.S. and M.Eng. degrees in Computer Engineering from the University of San Carlos, Philippines, in 2007 and 2015 respectively. He is currently a lecturer in the Department of Computer Engineering in the said university. His research interests include Computer Networks, IOT applications, and distributed systems.

James Michael C. Cañete received his B.S. degree in Computer Engineering from the University of San Carlos, Philippines, in 2009 and is currently finishing his M.Eng. degree, also in Computer Engineering. He is currently a lecturer in the Department of Computer Engineering in the said university. His research interests include Image Processing, Embedded Systems, and Computer Systems.

Gillian Claire G. Cancio received her B.S. degree in Computer Engineering from the University of San Carlos, Philippines, in 2018. Currently, she is working as a Software Engineer at Kyocera Document Solutions Development Philippines, Inc. Her research interests include embedded system design and development, internet of things, and software design and development.

Krizia Dianne N. Congson received her B.S. degree in Computer Engineering from the University of San Carlos, Philippines, in 2018. Her research interests include embedded system design and development, internet of things, and software design and development.

Kerr Jason Q. Quevedo received his B.S. degree in Computer Engineering from the University of San Carlos, Philippines, in 2018. He is a project manager in Full Scale, a tech services company based in the USA. His research interests include embedded system design and development, internet of things, and software design and development.



Rhea Ann R. Verallo received her B.S. degree in Computer Engineering from the University of San Carlos, Philippines, in 2018. She is currently working as an Account Executive at IPv4 Mall Ltd. Her research interests include embedded system design and development, internet of things, and software design and development.