Monitoring Individual Medical Record by Using Wearable Body Sensors

Jagadeesh Gopal, E. Sathiyamoorthy and R. Mohamad Ayaaz

Abstract Every single essential sign has an immediate effect in human services, so body sensors are utilized for consistent social insurance checking. In existing techniques, the sensors are embedded or wear by the client and the sensor information are exchanged and put away in the restorative server. In this proposed framework is for a healing facility condition the specialists and attendants can access the client's therapeutic data from the Blynk server. The wearable sensor's on the patient's body is associated with an Arduino board the detected data is transmitted by transfer hub and put away in the cloud which will be access by the Blynk server and get the data to the Blynk application so that the patient and the doctors can access the data or the records of the particular patient and even the medical staff. The specialists and attendants can get to the patient's medicinal data from the Blynk application. Individual medical record [IMR] can be access by the doctors and the medical staff to analyze the patient condition.

1 Introduction

1.1 Background

In recent times, Individual Medical Records (IMR) has risen as a patient-driven model of wellbeing data trade. An IMR benefit permits a patient to make, oversee, and control it is close to home well-being information in one place through the web, which has made the capacity, recovery, and sharing of the restorative data more efficient [1]. A wearable body sensor network (WBSN) framework has been proposed to send in medicinal situations. The remote framework in the WBSN utilizes restorative groups to get physiological information from sensor hubs. The therapeutic groups are chosen to lessen the impedance and in this manner increment the conjunction of sensor hub gadgets with other system gadgets accessible at medicinal focuses. The gathered

J. Gopal · E. Sathiyamoorthy (✉) · R. Mohamad Ayaaz
School of Information Technology and Engineering, VIT, Vellore, India
e-mail: esathiyamoorthy@vit.ac.in

S. C. Satapathy et al. (eds.), *Smart Intelligent Computing and Applications*,
Smart Innovation, Systems and Technologies 105,
https://doi.org/10.1007/978-981-13-1927-3_38

information is put away utilizing with the help IMR (Individual Medical Records) which is completely tolerant and controlled structure. The entryway hubs associate the sensor hubs to the neighborhood or the Internet [2]. In a doctor's facility zone to render nature of administration the framework comprises of a portable care gadget, which is in charge of catching and remotely sending the patient's ECG information, a wireless multi-hop relay network (WMHRN) that is accountable for handing off the information sent by the previous, and A residential gateway (RG), which is in charge of social event and transferring the got ECG information to the remote care server through the Internet to do the patient's well-being condition observing and the administration of neurotic information. A crisis ready administration utilizing short message benefit (SMS), in view of the location of irregular variety of HR, is additionally utilized as a part of the RG to further upgrade the medicinal services benefit quality. Hande Alemdar, Cem Ersoy in "Remote sensor systems for human services: A review" Says about the difficulties and different security issues in remote sensor systems, for example, security low power utilization, un-pretentiousness, adaptability, vitality effectiveness, security and give a thorough investigation of the advantages and difficulties of these frameworks [3].

1.2 Problem Statement

Each and every key sign specifically influences social protection, so body sensors are used for relentless restorative administrations watching. In existing procedures, the sensors are implanted or wear by the customer and the sensor data is traded through PDA (Personal Digital Assistant) and store in the restorative server. In proposed technique, Individual Medical Records (IMR) comes into play. Individual Medical Records (IMR) is totally tolerant controlled system which gives extra security and flexibility. This information is secured on outcast servers, i.e., cloud advantage providers. Nowadays there are a lot of security stresses over all IMRs from unapproved get to. Remembering the true objective to get to our own particular IMRs, it ought to be mixed before securing in cloud. Still there are a couple of troubles, for instance, trustworthiness, security, adaptability which needs to overcome by any capable structure. In this paper, we propose a novel patient-driven framework for data get the opportunity to control to IMRs set away in semi-confided in Blynk servers. To achieve our goal of most secure and versatile structure we are accepting credit-based encryption to encode patient's record. In our structure, we have concentrated on multi-characteristic records from different substances having a place with different spaces. Patient's data security is kept up by using multi-quality records in secure regions. This will similarly give on demand customer credit revocation to emergency staff in veritable conditions. Moreover, we are endeavoring to make the structure affirmation in disconnected condition.

2 Proposed Work

In the proposed system, body sensors been connected to the patient's body. Using Arduino, data can be collected from the patient's body. A Wi-Fi module is used to transmit the data to the application from which the doctors and the patients can access the particular data. For the framework segments to work, we are utilizing a microcontroller called Arduino to control the wearable body sensor and the Wi-Fi module called ESP8266. The Wi-Fi module is utilized to associate the framework to the Internet and send the notification and the data to the client. At the point when the conditions of the sensor sense the data, it will flag the microcontroller which will thus instate the Wi-Fi module. We have utilized the Blynk application as an extension between the Wi-Fi module and the Internet. The API given by the Blynk application sends the information gathered from the client to the client. The Wi-Fi module likewise can acknowledge charges from the Blynk application which can be utilized to send the data on or remotely by utilizing the Blynk cell phone application.

3 Materials and Methodology

Hardware apparatus required for this venture of idea are Arduino UNO, Temperature sensor, Smoke sensor, Wi-Fi module [ESP8266], a breadboard and few jumping wires. Likewise software required to get an output from the PC, Arduino IDE is an open source software used to upload the standard code of the sensors and the Arduino connected to the PC with the help of USB cable. Apart from the Arduino IDE, Blynk application is used to get the data from the sensors that are sensed from the human body. Blynk is a Platform with iOS and Android applications to control Arduino, Raspberry Pi and the inclinations over the Internet. It is a propelled dashboard where you can amass a sensible interface for your wander by basically moving devices. It is really simple to set everything up and you will start tinkering in less than 5 min. Blynk will set you up on the web and for the Internet of Things.

To implement this IoT concept, myself using Blynk libraries that takes information from the microcontroller and sends the information to the host (Blynk application) by utilizing the implicit capacities and methodology of the Blynk libraries. The application acts as a virtual controller for our Arduino microcontroller which can get information from the framework and send summons to it utilizing the Wi-Fi module as a channel. The application creates a validation id for each new venture which is utilized by the microcontroller to speak with the Blynk application over the web.

It is all around perceived that the IoT innovation has been picking up energy and is being coordinated in ordinary things, for example, cars, electrical machines, and so forth. A zone where IoT is being considered as one of the urgent advancements is for security purposes. Healthcare system is an important area of concern for all the doctors and the patients whose data can be retrieving through the concept of IoT. This concept is made for security reasons to store the patient record in an effective

manner so that the third party cannot access the data without the permission of the particular patient.

4 System Architecture

Architecture diagram shows that the Arduino UNO leading the process by allowing the sensors to connect in it. Arduino UNO been connected to PC by using the USB cable. ESP8266 (Wi-Fi module) also connected to the Arduino, it will transmit the sensed data to the Blynk server from which user will get in the Blynk application. Engineering is connected to comprehend the usefulness of the venture. Architecture clarifies the availability procedure between all sensors to microcontroller to Wi-Fi module to Blynk server to Blynk application. Architecture likewise shows the stream of correspondence between the parts and the different qualities in an effectively justifiable organization (Fig. 1).

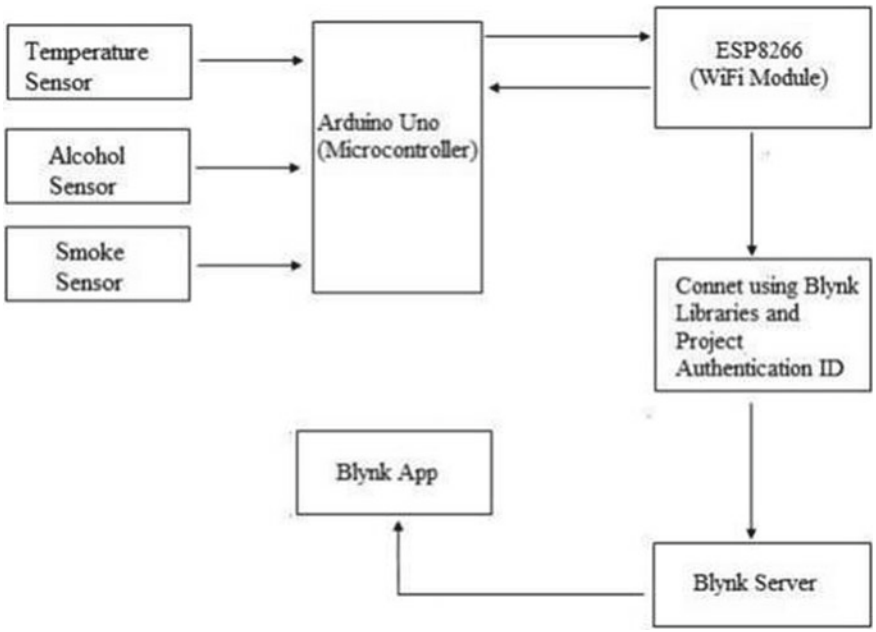

Fig. 1 Architecture diagram

5 System Implementation

5.1 Setting up ESP8266

Before we start associating the equipment, we need to get the ESP8266 set up by blazing the most recent rendition of the firmware accessible for the module. This is on the grounds that the chip accompanies a more seasoned form of the AT summon firmware pre-introduced out of the crate which cannot speak with the Blynk libraries productively and will give a mistake with our code. In this way before we start, download the ESP8266 flasher instrument and the most recent firmware from the web which would be in the receptacle arrangement and set up the ESP8266 to the Arduino Uno (Fig. 2).

5.2 Hardware Configuration

Once the ESP8266 has been flashed with the most recent firmware, we are prepared to amass our venture parts together. For this we will require a breadboard to associate the microcontroller, reed sensor, signal and the ESP8266 utilizing the jumper wires. The breadboard is utilized to interface between the different segments accessible. It additionally makes it simple to associate different contributions to a solitary stick on the Arduino board. The stick setup for all parts and configuration draw taking after the real circuits.

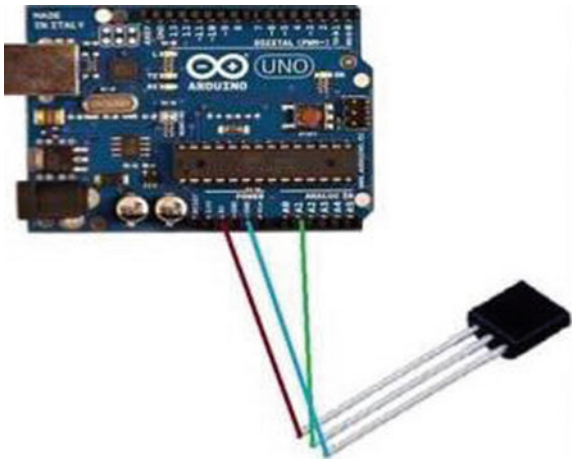

Fig. 2 Circuit diagram (design check)

5.3 Circuit Diagram

Taking after portray which has been developed utilizing the Fritzing programming demonstrates how the segments should be associated together utilizing the bread-board and the jumper wires. The last arrangement requires not be indistinguishable to the given outline, despite the fact that the pins on every gadget should be associated with the same comparing pins on the Arduino Uno board.

5.4 Configure the Blynk Application

Creating an account

- After installing the Blynk app on either android or the iOS devices, you need to create an account to access the services. Initially it will ask for Log-in or Create new account. Opt for Create new account as a new user.
- After the entering the email and password, click on the Sign Up button. It will create the account and user will sign in automatically.

Creating Project

- Once the user have logged in, user can click on the Create new project. This will take the user to Project design screen wherein the client needs to pick the title of the venture, the sort of gadget which the application will speak with and the method of the correspondence.
- For our venture, we select Arduino Uno as our gadget and Wi-Fi as the association sort. Client can likewise choose the choice to pick among dim and light subject according to their inclination which will just change the presence of the application and not influence with any venture alternatives.

Authentication Code

- After you have made the venture, the Blynk App will create an Authentication Token for your venture. Keep in mind that each venture has an alternate Authentication Token so that Blynk servers can recognize them thus that your code transferred to your gadget knows which venture to convey to. The confirmation token is sent to the email-id utilized while joining and can likewise be seen inside the venture settings screen.

Adding Widgets to the Project

- To interface with our segments, we have to add Widgets to our venture. To include Widgets tap the "+" catch, this will draw out the gadgets sheet from the correct corner of the screen which contains the rundown of all gadgets accessible. Simply tap on the gadget you have to add it to your venture.
- According to our prerequisites, we include a Notification gadget and a Button gadget to our venture. The notice gadget is activated when the tell() technique is called from the program and is utilized to show Push warnings on iOS gadgets. The catch is added to control the conduct of the ringer and will be utilized to stop or begin the signal remotely from inside the application.

6 Result/Output

6.1 Upload the Code

The code need to be compiled once it done, upload it to the Arduino UNO board by connecting the board to the computer using USB cable.

6.2 Running the Program

Subsequent to transferring the program, tap on "Serial Monitor" to begin running the code. Once the code begins to run, the principal thing it will do is to attempt and interface the ESP8266 to the Access Point pre-characterized in the code. On the o chance that the ESP8266 interfaces with the Access Point with web abilities, it will associate with the venture by means of the Blynk Servers by sending a ping message.

6.3 Getting Data/Output

The user will get the temperature in the Blynk application which is retrieved from the temperature sensor via Arduino.

7 Conclusion and Future Scope

7.1 Conclusion

The hardware and software both works perfectly as they were expected to with no errors. From sensing it from the patient body to the retrieving the circumstances and sending it to the Blynk application so that the doctors and medical stuff can view it. Even the patient also can view it using their smartphone. Another imperative part of the venture is the availability between the ESP8266 (Wi-Fi module) and the Blynk server. The framework effectively associated with the Blynk server utilizing the confirmation token and the Blynk libraries. Subsequently, we could get the warning on our cell phones when there was any adjustment in the status of the reed module sensor. Likewise the extra capacity to control the alert remotely is exceptionally useful and can be extremely valuable in some unexpected conditions. It was additionally watched that the Blynk application worked easily and done all correspondence between the equipment and the application precisely. In the wake of testing the framework ceaselessly at an interim of 2 h for a time of 10 h, amid which the equipment was not turned off even once, yielded similar outcomes which was that every one of the functionalities were working splendidly in sync. This was done to test the perseverance of the equipment and to test the reliance of the product. The test was furnished with every one of the suppositions being valid for the entire length of time which implies that the cell phone and get to point don't lose the web association and the power supply to the Arduino Uno load up is not cut off.

7.2 Future Scope

The medical Internet of things will play a major role in the medical world. In future we improvise our venture with the help of ready message can be send to specialist when a parameter achieves an unusual esteem. And this proposed framework can be utilized by the healing facility of clinical range to enormous doctor's facility condition to utilize the cloud administrations like as web administrations.

References

1. Ibraimi, L., Asim, M., Petkovic, M.: Secure management of personal health records by applying attribute-based encryption. In: Wearable Micro and Nano Technologies for Personalized Health (pHealth), pp. 71–74 (2009)
2. Li, M., Yu, S., Cao, N., Lou, W.: Authorized private keyword search over encrypted data in cloud computing. In: International Conference on Distributed Computing Systems, pp. 383–392 (2011)

3. Lai, C.-C., Lee, R.-G., Hsiao, C.-C., Liu, H.-S., Chen, C.-C.: A H-QoS-demand personalized home physiological monitoring system over a wireless multi-hop relay network for mobile home healthcare applications. J. Netw. Comput. Appl. **32**, 1229–1241 (2009)
4. Li, M., Yu, S., Ren, K., Lou, W.: Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings. SecureComm. **10**, 89–106 (2010)
5. Lohr, H., Sadeghi, A.-R., Winandy, M.: Securing the e-health cloud. In: International Health Informatics Symposium, pp. 220–229 (2010)
6. Mandl, K.D., Markwell, D., MacDonald, R., Szolovits, P., Kohane, I.S.: Public standards and patients' control: how to keep electronic medical records accessible but privateMedical information: access and privacy Doctrines for developing electronic medical records desirable characteristics of electronic medical records challenges and limitations for electronic medical record-s conclusions commentary: open approaches to electronic patient records commentary: a patient's viewpoint. Bmj **322**, 283–287 (2001)
7. Benaloh, J., Chase, M., Horvitz, E., Lauter, K.: Patient controlled encryption: ensuring privacy of electronic medical records. In: ACM Work-shop on Cloud Computing Security, pp. 103–114 (2009)
8. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and ne-grained data access control in cloud computing. Infocom, pp. 1–9 (2010)
9. Dong, C., Russello, G., Dulay, N.: Shared and searchable encrypted data for untrusted servers. J. Comput. Secur. **19**, 367–397 (2011)
10. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for ne-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
11. Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wireless Commun. **17** (2010)
12. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based en-cryption with e cient revocation. In: ACM Conference on Computer and Communications Security, pp. 417–426 (2008)
13. Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., Jonker, W.: Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes. Technical Report, Centre for Telematics and Information Technology, University of Twente (2009)
14. Yu, S., Wang, C., Ren, K., Lou, W.: Attribute based data sharing with attribute revocation. In: ACM Symposium on Information, Computer and Communications Security, pp. 261–270 (2010)
15. Narayan, S., Gagne, M., Safavi-Naini, R.: Privacy preserving EHR system using attribute-based infrastructure. In: ACM Workshop on Cloud Computing Security Workshop, pp. 47–52 (2010)
16. Liang, X.-H., Lu, R.-X., Lin, X.-D., Shen, X.S.: Patient self-controllable access policy on phi in ehealthcare systems. AHIC, pp. 1–5 (2010)
17. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. Security and Privacy, pp. 321–334 (2007)
18. Akinyele, J.A., Pagano, M.W., Green, M.D., Lehmann, C.U., Peterson, Z.N.J., Rubin, A.D.: Securing electronic medical records using attribute-based encryption on mobile devices. In: ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 75–86 (2011)
19. Darwish, A., Hassanien, A.E.: Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors **11**, 5561–5595 (2011)
20. Kumar, R., ManjupPriya, S.: Cloud based M-Healthcare emergency using SPOC. In: Advanced Computing (ICoAC), pp. 286–292 (2013)