TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

Protection of Patient Information Records Monitoring System through USB-HID and PIC Microcontroller PPIRMS

Ali Hassan, Rosilah Hassan, Mohammed Dauwed and Azizah Ya'acob

Article Info
Volume 83
Page Number: 1725 – 1735
Publication Issue:
May - June 2020

Article History
Article Received*: 11August 2019*
Revised*: 18November 2019*
Accepted*: 23January 2020*
Publication*: 10 May2020*

Abstract:

Several wearable devices have been suggested by the healthcare to assemble and display the patient information. Unfortunately, the privacy nor the reliability of the recorded data are met since many people can use the same device, and not necessarily with prior knowledge. The main objective of this project is to design a new system for patient information recording to ensure both privacy and relevance of the data. This new Protection of Patient Information Records monitoring system (PPIRMS) system can monitor the data in total privacy using USB-HID. The system will send the recorderd data using USB-HID connection which will ensure both security and privacy. The system implementation consists of many simulations. This PPIRMS system avoids the misuse of the wearable devices since reliability and privacy of recorded information are met. Benchmarking has been performed as well to fill in the research gap with previous studies and the highest value obtained was 71%. This study is enabled to create a system of high reliability, privacy, and security to record and monitor the patient's information.

Keywords: *PPIRMS, patient information, reliability and privacy.*

I. INTRODUCTION

Nowadays, recording patient information has become a fundamental action in the health care area and will persist so. The recorded data helps in the synthesis of the health care and contributes in planning the health care facilities development. The Patient health information represents a health procedure in which a complete report of all the patient's daily status is to be provided [1]. The record system for patient information is beneficial for the health institutions and patients since this new service can record all the available information through a device accessible at any time and everywhere [2]. Under medical supervises, the recorded information can be reviewed to guarantee an improved healthcare service. Recording information about patients helps the professionals and the medical team to diagnose illnesses which can cause any health risk. Hence, reliability, privacy, and security of the information record are necessary for a advanced levels identification [3].

Lately, modern technology became significant to record patients' information by any type of system, especially if the patients represent the elderly who are enabled to leave their domiciles. It represents a collective information and a means of communication with related mechanisms through a local network [4].

Devices for information record are significantly advantageous especially in the medical area as it highly contributed in the well curing process of many diseases such as diabetes [5] and cancer [6]. Though, there are difficulties encountered by some users. First of all, they are misused. For example, many patients do not necessarily suffer from any illness. Nevertheless, they use these devices for spotting the data. Besides, if one of the same device is used by more than a person, the data may be mixed up. Therefore, privacy is not met, and the data is irrelevant. Besides, numerous patients if not all of them dislike having their personal information public [7], which shows the lack of security.

Internet of Things -IoT- is a new growing method used in diverse applications including smart environments, houses, personal health care, and others. It is a smart notion for Internet where everything around is related to Internet and can organize data, exchange information, and work adequately. Many studies have been conducted regarding IoT technologies to maintain the need in developing platforms for this technology [8]. Several

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

smart nodes are connected together to acquire information without human interference [9]. Internet, in other words, is a technological growth for an easier life by advancing the global economy. Health monitoring applications have also been considerably marked by Internet [10].

In the medical area, IoT is called Internet Medical Stuff (IoMT) [11]. This is a system of arrangement about the medical applications aiming to ensure an improved and healthier care service. IoMT is nowadays at its maximum for its precious potentials amongst all other IoT applications [12]. Medical IoT is cautious about the recent products including magnetic resonance imaging (MRI), the ultrasound devices, and the wearable devices to make most health procedures easier along with illness diagnosis and inaccessible patient tracking. For IoMT, medical information is exchanged between entities through a wireless intermediate. Consequently, there are very high chances that another entity interrupts during the communications through number of attacks.

Hence, security and privacy are the most important components for an IoT-based health care system[13]. The development of IoMT is crucial for healthcare sources by bringing out numerous challenges including device movement support, secure node communication, timely data connectivity, and power management. Implementing IoMT without ensuring the confidentiality and the security of the patient's information will permit the medical information spotting when they are transferred through the wireless devices. Thus, significant information may be exposed to illegal usage [14].

Nowadays, wearable devices are conventional in healthcare monitoring and technology. The main concern is the fact that it is used by people who might be unknowledgeable about this technology. Devices inappropriately used causes an information overlapping, making it irrelevant for usage. This leads to an erroneous diagnosis which could be fatal in healthcare. Reliability, privacy, and security are the main challenges in this new medical system, since the information recording demand is increasing to provide an improved healthcare quality. This smart technology ensures the patient's data collection and monitoring. Thus, it is essential to guarantee reliability and privacy of the information, and security of their transfer for a safer and accurate diagnosis.

II. METHODOLOGY

This study evaluates a new system for medical devices which ensures privacy and reliability in patients' information recording, and security while transmission and saving. The objective of this study is to solve two major problems: the misuse of medical devices and the overlap of the recorded data. This system consists principally of designing a circuit made of a PIC microprocessor, a sensor, a keypad and an USB-HID. The circuit is connected to the medical devices carried by the patients to record his/her information.

A. Design of a new system of reliability

The purpose of this work is to develop a new system that provides reliability to the relevant records of patient health information in order to ensure the accuracy of the recorded data. The system is implanted into wearable devices to facilitate data recording and make it safe and reliable. The system requires an identifier (ID) for each patient once the device is connected and is ready to record data. The device interprets the patient's condition and saves information under their respective date. Due to the limitations on obtaining information necessary for the real implementation and lack of patients, the system is implemented by simulation through the program Proteus 8 Professional.

Technologies Used in the PPIRMS.

Several technologies have been used in advanced healthcare systems to answer surveillance issues such as the use of IoT. Previous studies showed that reliability, privacy and security were not always met. This study proposes a system regrouping the three major properties placed into portable devices using IoMT.

The system components.

The proposed system is made of various electronic components. The PIC Microcontroller is the main component of the circuit. The one used for this system is PIC18F4550, and it is the most renowned PIC Microcontroller used in nearly all fields. It is a 40-Pin and 8-bit PIC Microcontroller belonging to the PIC18 Family with a 32KB Program Memory, a 2048Bytes RAM, EEPROM, a 256Bytes Memory, a CPU Speed of 12MIPS, and supports USB port, as shown in Figure 1.

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

USB-HID is the connection between the proposed system added on the wearable devices with the computer. This type of USB-HID is used to transfer data from the system to the computer in a wired manner by connecting the system to the USB ports on the computers available in the health care centers in a secure manner through the transport protocols. The purpose is to ensure that data is transferred in the most secure way possible.

Due to the possible circumstances, sensors have been added in the system and therefore to tell the effectiveness of the system, especially implemented through simulation and not a real system.

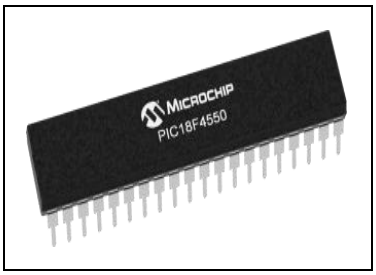

Fig. 1. PIC Microcontroller (PIC 18F4550)

The sensor is also part of the proposed system. In fact, it is used to detect initials such as temperature, blood pressure and heart rate and transfer them to the controller when opening and closing. The 16×2 LCD screen is used for input status displaying and monitoring as shown in Figure 2.

Fig. 2. 16×2 LCD Screen

A 4X4 Keypad interfacing has also been used in this system. The keyboard represents a gadget of information to check the key entered and prepared by the client. It comprises four lines and segments, and the keys are set between the lines and sections. The push keys are an association between the lines and segments of each two connecting switches as in Figure 3. The keypad enables the patient to enter the password so that the system can start working.

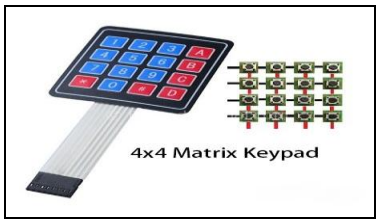

Fig. 3. 4X4 Keypad Interfacing

Moreover, a 1K byte Dual Port RAM + 1K byte GP RAM is included. The memory contributes storing the signals transmitted while the circuit is operating.

The Internal Pull Up resistors (D+/D-) are included in circuits to guarantee that the contributions to the Arduino and PIC are stable at the normal balanced stages in case the external gadgets are not connected, or if the obstruction is extremely low.

Reliability System design

This system is perfectly arranged to register patient data and simultaneously avoid any possible overlap or misuse of the wearable medical devices. It is smart system using attachable device to the patients and monitoring them to be able to collect each one's information including blood pressure and temperature sensors. The objective of this PPIRMS system is to make the recorded information relevant and to provide validation that it is used by one same person to avoid any overlying of the registers.

This system is designed with a PIC 18F4550 microcontroller for regulation and management of the information records of each patient. The sensors are included in the devices to detect any activity that should be taken into consideration. The main sensor is a Buckle used to feel the activity of the user when the device is operating or not. It can send signals to the microcontroller for the key code request before the registration starts. This is to guarantee that a unique person uses the device. The Keypad interfacing of the device permits the user to enter the key code and the status of the device is shown in the LCD screen.

The diagram of Figure 4 represents the system components mechanism to be implemented, the ones of which are listed in the system requirements section in detail.

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

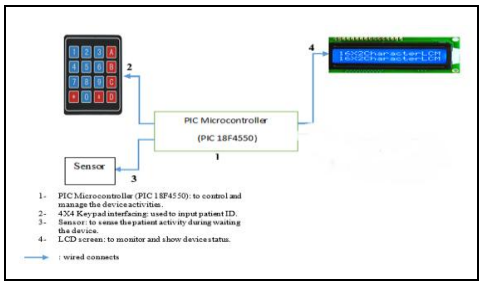

Fig. 4. System Design of PPIRMS

When the patient uses the medical device, a signal is sent by the sensor to the microcontroller. Once received, the microcontroller shows an interface on the LCD screen requiring from the patient to enter her/his ID. The device records the information and saves it under the identifier's numbers entered by the patient. This prevents data overlapping and therefore solves the reliability problem. Figure 5 summarizes the system's work.

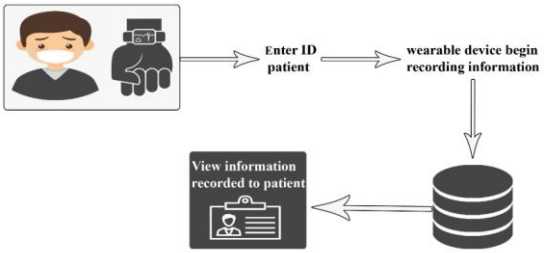

Fig. 5. System Work of PPIRMS

Programming Language

Programming is necessary at this phase of the study. Choosing the right programming language is essential to achieve the expected outcomes. The system is entirely programed by simulation using Proteus 8 Professional and mikroC PRO for PIC. Besides, C programming language is used to program the processor (PIC) and command control.

B. Protection Patient Information Records System

Protecting the recorded information is fundamental for the wee functioning of this system as it is an essential objective that needs to be achieved to gain the patient's trust and avoid any possible doubt that the recorded data by this system may be known. Nowadays, any system providing privacy along with protection are the ones that are the most favorized by the patients.

This system not only guarantees the record privacy, but also ensures a better protection of data while they are being transferred from the device to the health care center.Privacy and security have been achieved by adding a USB-HID to the system described above and setting a login feature with a username and a password once the device is connected to the computer for data reading.

Components

The previous system has been extended in this part of the study by adding a USB-HID. The Human Interface Device (HID) allows architects to create applications and gadgets based on a USB without any obligation for custom driver development. USB gadgets are easily connected with computers. Creating a USB interface among an implanted framework and a computer has been achieved.

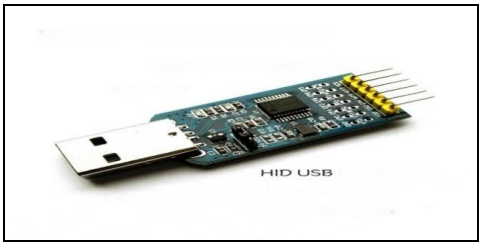

Fig. 6. USB-HID

New Design of the system

The USB-HID was added to the system to ensure security when the data is being transferred to the computers in the health care centers through a direct connection between the system and the computer. Therefore, it was essential to program a graphical interface to allow the username and password to be entered, allowing the health institutions to recognize every data stored in the device belonging to the individual. To retrieve the recorded information, the same USB-HID which was used connected to the device is connected to the computer. Thus, patients can make sure that the health professionals are the ones accessing the records and consulting them. Moreover, they are sure that no loss or interference will occurr as it may have happened in cases of any other wireless transfer. The patient username and password are not required to allow the chosen organization to retrieve the patient information. A C # application is elaborated to show the patient's data records to health professionals. As a result, the misuse of patient's information is avoided, and patient privacy is maintained. Simulations have been performed through Proteus 8 Professional software and Mikro C PRO for PIC. Figure 7 summarizes the mechanism followed for the system implementation.

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

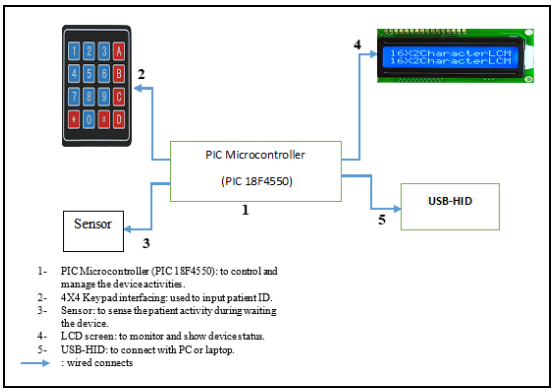

Fig. 7. System Design

III. RESULTS AND DISCUSSION

A. Proposed system

PPIRMS as for Reliability and Privacy of Patient Information Monitoring System is suggested to help monitor patients by guaranteeing secure approaches to transfer data reliably and securely. This system is composed of three major units which are the input, the output and lastly, the processing as shown in Figure 8. Each unit may be separated into sub-parts categorized by the devices used for the system application and the work performed. The Inputs in the PPIRMS system involves two types, the identifier which is reinforced by a password required to authorize the access to the system, and the user system definition. When the management of the identifiers in the C Sharp interfaces started in the system, traffic was created by the system administrator. The password is the key allowing the system to recognize the user and to start operating on perceiving information. Proteus software helps in performing the simulations necessary for the system implementation. The password was entered in the 4x4 keypad in the electronic circuit.

The processing level starts with a password checking as long as the system begins operating. The following entry was the patient's information record in the sensors of the system including blood pressure and temperature sensors and the sensitivity of the proportion of oxygen. This information is considered as an input for the system and is to be processed in the second part of the system. The processing phase is significant for the system life cycle and is performed in three steps. The first step consists of data recording before reading it. A processing step is essential to verify if the password entered is correct or not. A message is then displayed on the LCD screen used in the simulation asking to start the recording process.

The data recording in the PPIRMS system will be done through sensors detecting and registering temperature, blood pressure, and oxygen level. Signals are sent and then, received by PIC18F4550 and the sensors. The data processing unit in the PIC18F4550 will be in charge of issuing directives on whether to start or to stop registering. Once the information recording has begun, the programming stage starts with the data transfer to prepare for recording. The data is processed as long as it was received from sensors. Whilst the data is being registered, the patient will be added throughout the processor PIC18F4550.

Once the previous steps are completed, the information is stored in the PIC18F4550 memory for the final phase of the system processing representing output stage. The final stage is when the output and outcomes are extracted from the system after the two first phases. The output consists of displating the data received after recording during the input step, which is also controlled as structured tables comprising the patient's identifier and information. In fact, the system related to C Sharp interfaces through a USB-HID link will guarantee a secure way to link the system with the computer.

Patient monitoring is done thanks to the information displayed to enable the medics to track the information registered for each patient. All over the recorded information, doctors may realize if the diagnosis primarily made was correct or not. Patient identifier management represents the phase of adding the patient's ID to the device and has appointed a password to access the system while operating. The patient IDs previously used by the system may easily be deleted.

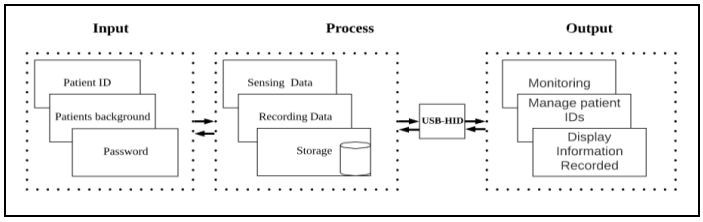

Fig. 8. Proposed System

B. Structure of PPIRMS

The structure represents the principal part of the system application. This procedure was performed through numerous steps. Figure 9 illustrates the PPIRMS structure. The device has to be in direct contact with the body of the patient. This option is applied to avoid any eventual misuse. Recording cannot begin with any data only if the device is related

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

directly to the patient's body. Once the device is connected to the body, a "do not seek" note is shown, which unables the patient to enter his/her password. If the apparatus was not in contact with the body, it would have required the password which has been assigned to the patient by the health organization.

When the password entered was incorrect, patients are asked to return the password over. Nevertheless, when it is correct, the information recording shall begun. The information is then stored in the device. The information will be retrieved using the USB-HID technology. It is connected to transfer the obtained data in a secure manner to the computer of the health centers. Besides, a password should be inserted prior the recorded information display. The privacy of patient information apparatus is able to record information of more than a patient and save it under each identifier. Hence, recorded data is secured, verified, and reliable.

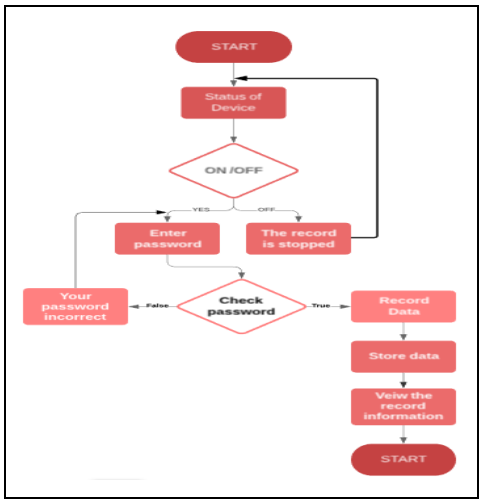

Fig. 9. Structure of PPIRMS System

C. System simulation

The system implementation was performed through many simulations with Proteus 8 Professional program software. This software provided numerous features and was characherized by its flexibility in use. The simulation was the best method to cover the impossible real-world system implementation since it is required to obtain some confidentatial information from health organizations. The simulation and implementation of the system is a basic method to obtain the intended results. The C programming language is favorized among other programming languages for the PPIRMS coding. The circuit of the system adopted is shown in Figure 10.

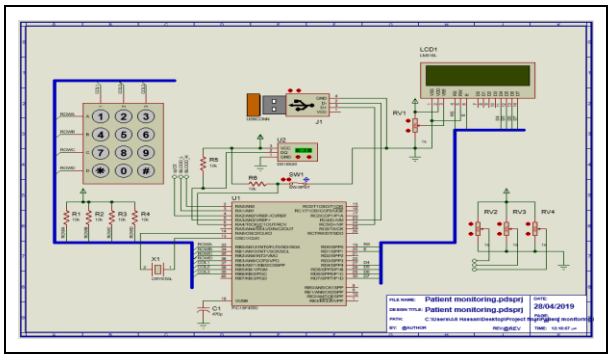

Fig.10. Model Simulation System PPIRMS

Software: Proteus 8 Professional.

Proteus represents an electronic program for circuit simulation adopted to design electronic circuits and to obtain the outcome of a method for creating a circuit on the ground. It also divulges the possible errors that may happen in electronic circuits, and there are various versions of this program improved over the past years such as the program Proteus of Software which is fundamental in the electronic circuits simulation. Version 8.7 of Proteus is the one used in this study.

PIC 18F4550.

Among the most famous PIC microcontrollers is the PIC 18F4550, which is used in nearly every electronics field, and contains 40 pins with few supplementary features. Chip technology is a huge of an implanted system. Every year, it manufactures a different product for several applications from the Beginner Training Group to superior applications including medical and robotic devices. It can be easily exchanged by a PIC18F2550 microcontroller with a simple coding modification. Moreover, the PIC 18F4550 maintains the USB-HID which represents the most relevant controller to add USB. The main purpose of using this controller in this system is the fact that it is characterized by a high-speed USB 2.0 interface (12 Mbps), a dual-access random memory, and a full speed during sending and receiving information. Figure 11 shows the structure of PIC18F4550.

The role of the PIC 18F4550 in this circuit is to control the process of the system from transferring the signals to other units in the system such as the sensors for blood pressure and temperature, the Keypad interfacing, the LCD screen, the USB-HID and the switch.

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

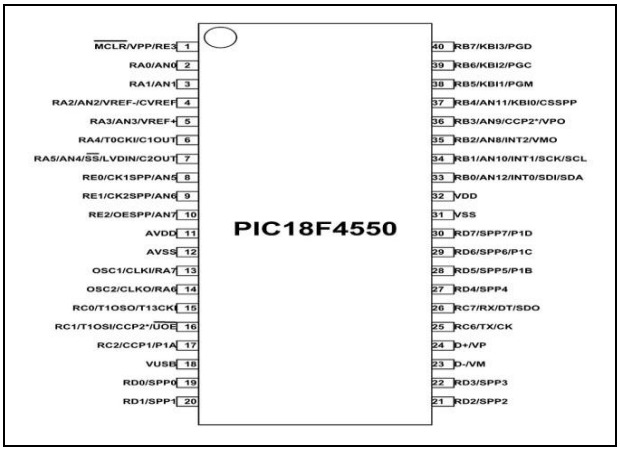

Fig. 11. Structure PIC18F4550

Temperature Sensor.

Temperature sensor interferes to determine the temperature of the patient's body once he turns the device on and place it in direct contact with his body. Once inserting the password, the sensor sends a signal to the microcontroller PIC 18F4550 to save what has been analyzed in the memory of the device.

Blood Pressure Sensor.

Blood Pressure Sensor is essential since it determines the patient's blood pressure necessary for every diagnosis, even the simplest ones. The sensor starts operating when the patient turns on the device placed in contact with his body and once the password is inserted, it then records the patient's blood pressure. The blood pressure will be saved; the sensor then sends the signal to the microcontroller to save the reading with the time spent reading in the device memory.

16 x 2 LCD Screen.

The purpose of the LCD screen in this system is to display explanatory messages to the user to illustrate the status of the system in every moment during the usage, from the operating to the shutdown steps. Among the messages shown were the welcoming message at the beginning of the system followed by the message asking the user to insert his/her password. Once the password is recognized by the system, another message appears to inform the patient that the process started.

USB-HID.

The Human Interface Device class requirement enables the inventers to design new types of devices furnished with a USB, which solves the necessity in developing a custom driver. Advanced chip integration and strong USB interfaces made of the silicon microcontrollers are the best hardware workshops for HID designs. USB-HID is essential to connect devices and applications with the computer. It is used for data transfer from the system to the computer in the most secure possible way through transport protocols. The advantage of the USB human interface device in this system is to transmit the registered information in the microcontroller to the computers of the health centers in a secure manner to avoid any loss or damage of the data. Hence, the data is protected, and privacy is guaranteed.

These devices are connected to the computers as shown in Figure 12, through the creation of certain contact points along with a USB interface between computer and the host machine met with a code for the subsystems: the device firmware, the operating system drivers, and the host-side PC application.

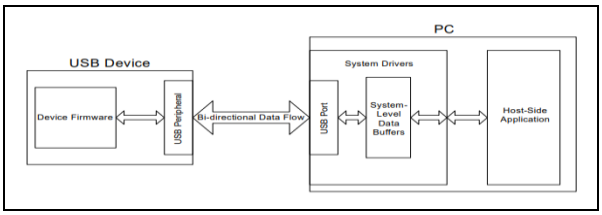

Fig. 12. USB Interface Between a PC

Switch

The switch tool is fundamental in this system since it is the one allowing the signal to be sent to the microcontroller throughout the transferred signal. The processor detects whether the device is in direct contact with the patient's body or not. If the switch is on its ON mode, the signal is sent to PIC18f4550 microcontroller to show the password entry message. If it is in its OFF mode, the processor displays a new message informing that the recording is stopped.

D. Simulation Results

The results of the PPIRMS system simulation are explained below in arrangement with each level and function. The simulation results are divided into two major parts: the first consists of the simulation through proteus program, and the second part is about recorded information at the C Sharp interface level.

Simulation in Software Proteus

The first part of the simulation is done with Proteus software. The electronic circuit is designed as a state in the simulation process and the coding is written in C programming language. The first stage of the implementation consists of loading the code on the microcontroller once converted to the hex file, and then starts the execution. Figure 13 demonstrates the first step of the system implementation.

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

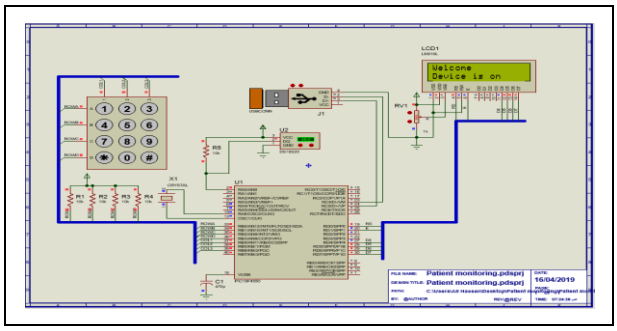

Fig. 13. Implement PPIRMS System Simulation

Once the code file converted, another file is uploaded on the microcontroller PIC18F4550, and the simulation can then start. The "welcome" message is displayed on the system's screen. 10 seconds following the operation, the processor, which is the PIC18F4550 microcontroller displays a new message to the patient, requesting him/her to insert his/her password as shown in Figure 14.

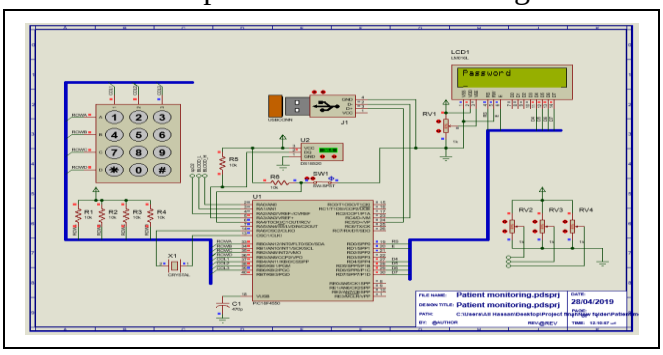

Fig. 14. Interface of Entering Password through Simulation

The new interface is then displayed; the patient can insert his/her password which is checked by the microcontroller. If the password is correct, a signal will be sent to the sensors to start the recording of the information from the patient, and a message will appear on the screen, informing the individual that the record is happening as shown in Figure 15.

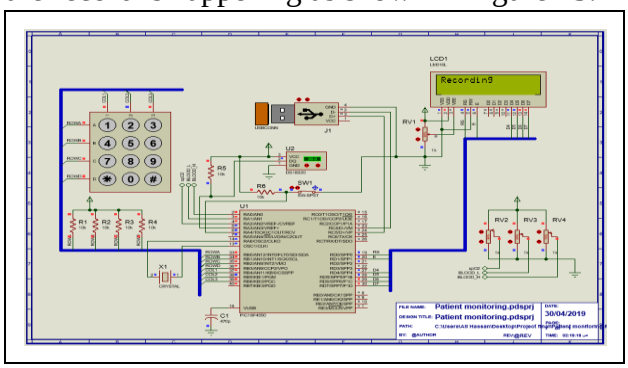

Fig. 15. Interface of Recording Information

However, if the password is incorrect, the patient will be required to re-insert the password and the same previous process will be repeated until the correct password is received by the system.

The switch has two states which can be either in ON or OFF mode to decide whether the system can operate or not. If it is in its ON mode, the system process operates as programmed. If it is OFF, the process will be interrupted, and the system will stop. If the process is still in the step of entering the password, or if it has reached the recording data phase while the switch sends the signal to the microcontroller, it means that the switch is OFF. Thus, the microcontroller-PIC18F4550- interrupts the system until it switches to ON mode again. The purpose of this switch is to know whether the device is in contact with the patient's body or not so that it stops working in case of no contact.

The above figures shows the stages of the system implementation process through simulation. After the simulation, the main objectives of the proposed system will be achieved. First, we protect the device from misuse and the reliability of the data recorded. This is achieved by adding an identifier ID to the system and password for each patient. That is, the patient cannot use the device if he does not have his own password. Second, transferring data safely and quickly using USB-HID and connecting the device to the USB port on the computer will ensure that it is possible to achieve data transfer in a way that cannot be penetrated when the device is connected to the computer wired. As in Figure 16, it shows the data received output by the computer from the wearable device.

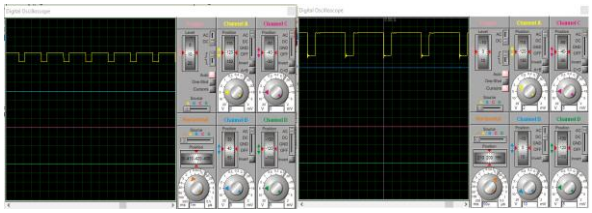

Fig. 16. Received output

E. C Sharp Interfaces Application

The second part of the implementation consists of the elaboration of an application using C Sharp. This application permits to go through the patient data registered during the first level of the PPIRMS system. The application involves three interfaces; to insert the password for application opening, to insert the patient ID, and to show all the records.

The system is related to the C Sharp application through the USB-HID used for this circuit, which represents the interface between the C Sharp interface

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

and the external system through which makes it possible to create a secure path for the data to transfer from the system to the output interface through which the patient information will be recorded within the system and then can be viewed. The data recorded is protected in a way that only authorized persons can access the system, and even this should be done only after providing the password to the system administrator.

The C Sharp application has three interfaces as previously mentioned. The first one appears when the application is run and once the USB-HID is connected. This interface is reserved to the password input field. Each user in the system has a unique identifier (ID) which is provided to him by the health institution to enable him to consult and use the system through that password which should be activated when it is inserted in the box allocated to it. Passwords are provided by the system administrator to patients if they apply for them to use the system to monitor their situations. The password is a patient's number in the system enabling the patients to insert a specific key to the system to store all the information registered by the sensors of the system with the word through which the system was entered as shown in Figure 17.

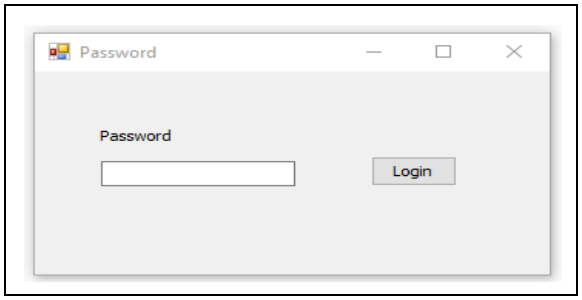

Fig. 17. Interface for Entering Password

After the insertion of the password in the first interface of the application, the second interface will be automatically displayed. This one is designed for the input field of each patient identifier which has been previously added in the same process before the recording of the patient information begins. It also comprises a label representing the status of the system which is linked with the Offline Connection C Sharp interface prompted through the installation of the USB-HID definition in the computer. The communication between the system and the interface is arranged to allow the system integration. Every patient choosing this system has a unique ID under which the recorded data is stored. All in all, the complete information retrieved including the body temperature and the blood pressure are recorded and saved under each of the patient's ID. The same identifier previously attributed to the patient can be used by the same patient to consult the system as shown in Figure 18.

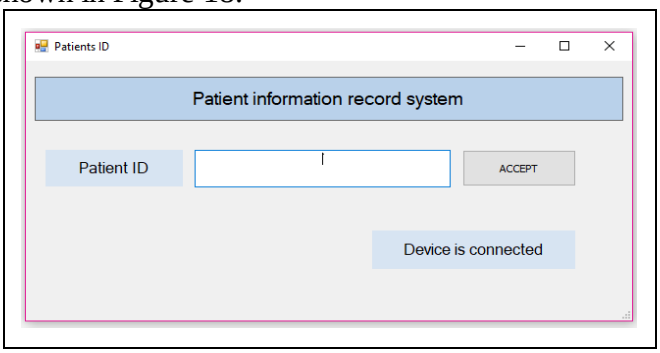

Fig. 18. Interface for Entering Patients ID

The last interface is designed to display all the data recorded. Once the identifier is provided to the system, it will be possible to show the data that has been recorded in the first phase. When the patient's ID is inserted, the result of the patient can be retrieved from all the available readings recorded by the system for other patients as shown in Figure 19.

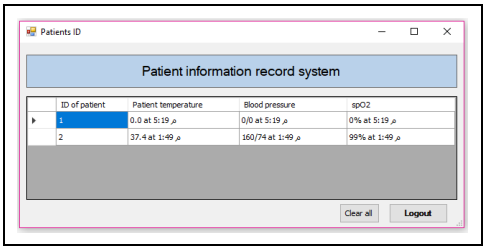

Fig. 19. Interface for Data Recorded

An additional button is available to enable clearing all the data recorded earlier by the system and cleans all the readings. This action makes the system work faster as the old data fills the processor memory storage space. Thus, when more space is available in the memory, the faster the performance will be. Once the process is complete and the data is retrieved, the user logs out and the application is ready to be shut down as shown in Figure 20.

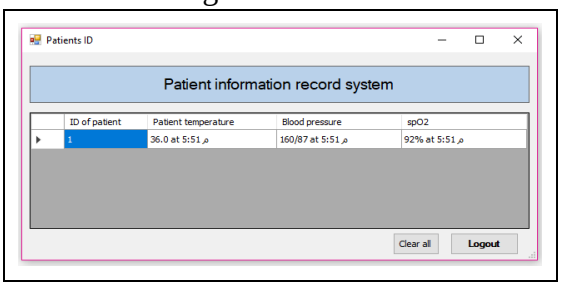

Fig. 20. Show the Clear Bottom

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

F. Comparative Benchmarking

The benchmarking is a procedure by which the actual PPIRMS functioning has been compared to previous systems. The similarities and differences have been highlighted in this comparison. Table 1 summarizes the evaluation between this system in terms of the components used and the techniques followed to design the PPIRMS system USB-HID, password, C # application, patient authentication, patient concern, abuse of patient device and interference log represent the benchmarking points.

Table I. Benchmarking Comparative with Literature Review

Component and Technology	Sandeep Resource	Jia-Wei Jhuang	Abel N.Kho	Zhe Yang	Azra Hazwanie Azizulkarim
USB-HID					
Password	√		√		
Interface GUI					√
Patient Authentication		√	√		√
Patient Concern	√	√	√	√	√
Misuse and Patient Device		√	√		√
Overlapping	√	√		√	√
Rate	42%	57%	57%	28%	71%

Component and Technology	Sebastian Winkler	Cavalleri	Proposed System	Rate
USB-HID			√	12%
Password			√	37%
Interface GUI			√	25%
Patient Authentication	√		√	62%
Patient Concern	√	√	√	100%
Misuse and Patient Device		√	√	62%
Overlapping	√	√	√	87%
Rate	42%	42%	100%	

It can be concluded from this benchmarking that the highest match value was 71% regarding the PPIRMS system components and technologies used to reach the reliability, privacy, and security of the patient information record system. Figure 21 summarizes the use from previous studies of the components and technologies favorited in this PPIRMS.

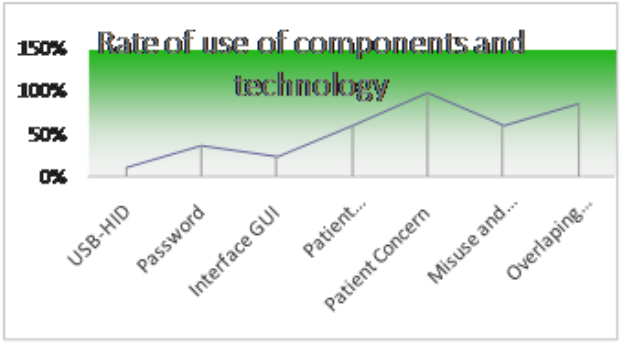

Fig. 21. Rate of use of Components and Technology

IV. CONCLUSION

Monitoring the condition of patients from competent health institutions, especially patients with chronic diseases is a significant approach, since it is a matter of saving time and information. Therefore, there are numerous devices designed to monitor those information including the smallest wearable ones. These devices are suggested to ease the healthcare patient information collection and monitoring. Unfortunately, patient records are not always relevent or trustworthy since those devices may be used by the patient himself without receiving any assistance from a professional.

This misuse makes the data recording irrelevant since the devices since anyone can use them. Besides, the patients are very concerned about the privacy of their information. Therefore, the proposed system is controlled with microcontroller (PIC) adressed to the health data monitoring in a secure way through a reliable system. The system is secured with the addition of the identifier (ID) feature. This feature restricts that every patient desiring to use the PPIRMS should have a unique and private ID to access the and record the information. This system significantly contributes to healthcare technology improvement by restricting the exploitation of wearable devices through sensor technology and is compatible for information record in the safest possible manner. The actual PPIRMS system comprises several features that distinguish it from existing ones. It combines reliability, privacy, and security all together. These features are one of the most vital ones for every patient. By delivering a password and with the flexible graphical interface that was programmed in C Sharp, and throughout which the registered data can be retrieved, the suggested system may be successful to ensuring reliability and granting security and privacy of the records.

This system is designed to solve the problem of medical devices misuse. The benchmarking showed that the highest match with previous studies was only 71%, making this system a unique one.

ACKNOWLEDGMENT

We would like to express our gratitude to the Network and Communication Technology (NCT) Lab, Cyber Security research group for the support and assistance they have provided for the well-functioning of this study, and the Faculty of Information Science and Technology (FTSM).

May – June 2020
ISSN: 0193-4120 Page No. 1725 - 1735

Supported from Universiti Kebangsaan Malaysia (UKM) under code grant PP-FTSM-2019 and DIP-2018-040, for granting facilities during the research.

REFERENCES

[1] Demlo, L.K., Campbell, P.M. & Brown, S.S., "Reliability of information abstracted from patients' medical records. Medical Care," vol. 16, no. 12, p. 995–1005, 1978.

[2] Cavalleri, M., Morstabilini, R. & Reni, G., " A wearable device for a fully automated in-hospital staff and patient identification.," in The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society 4, 2004.

[3] Vreugdenhil, M.M.T., Kool, R.B., Van Boven, K., Assendelft, W.J.J. & Kremer, J.A.M. , " Use and effects of patient access to medical records in general practice through a personal health record in the netherlands: Protocol for a mixed-methods study.," Journal of Medical Internet Research, vol. 20, no. 9, 2018..

[4] Kamaruzaman F. M., Hamid R., Mutalib A. A., and Rasul M. S.,, " Conceptual framework for the development of 4IR skills for engineering graduates," Global Journal of Engineering Education, vol. 21, no. 1, pp. 54-61, 2019.

[5] K.Vidhya and R.Shanmugalakshmi, "Improved Diabetic Data Analytic Model for Complication Prediction," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no. 6S, pp. 224-230, 2019

[6] T.Siva Prasanna and P.Jagadeesh, "Automated Detection of White Blood Cells Cancer Diseases," International Journal of Engineering and Advanced Technology, vol. 8, no. 6S, pp. 366-369, 2019.

[7] Cheek, P., Nikpour, L. & Nowlin, H.D., "Aging well with smart technology," Nursing Administration Quarterly, vol. 29, no. 4, p. 329–338, 2005.

[8] Hassan R., Nori S. S., Othman N. O., Arba'iah Inn, "The improvement of the protection for 6LoWPAN in IoT through non-causal hash function scheme," in ECTI-CON 2018 - 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Chiang Rai, 2018.

[9] Pirbhulal, S., Shang, P., Wu, W. & Kumar, A., "Fuzzy vault-based biometric security method for tele-health.," Computers and Electrical Engineering, vol. 71, p. 546–557., 2018.

[10] Sodhro, A.H., Pirbhulal, S. & Sangaiah, A.K., "5G-Based Transmission Power Control Mechanism in Fog Computing for Internet of Things Devices," p. 1–17, 2018.

[11] Puthal, B.D., Malik, N., Mohanty, S.P., Kougianos, E. & Yang, C. , "The Blockchain as a Decentralized Security Framework," p. 8–11, 2008.

[12] Islam M. S., Islam M. T., Almutairi A. F., Beng G. K., Misran N., and Amin N., "Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system," Applied Sciences, vol. 9, no. 9, 2019.

[13] Pirbhulal, S., Zhang, H. and Wu, W., "A Comparative Study of Fuzzy Vault based Security Methods for Wirless Body Sensor Networks," 2016.

[14] Dauwed, M. A., Yahaya, J., Mansor, Z. and Hamdan, A. R.,, "Determinants of internet of things services utilization in health information exchange," Journal of Engineering and Applied Sciences, vol. 13, no. 24, pp. 10490-10501, 2018.