I.J. Information Technology and Computer Science, **2024, 3, 22-35**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2024.03.03

Information Security based on IoT for e-Health Care Using RFID Technology and Steganography

Bahubali Akiwate*
K.L.E. College of Engineering & Technology/Department of Computer Science and Engineering, Chikodi, 591201, India
E-mail: bahubalimakiwate@gmail.com
ORCID iD: https://orcid.org/0000-0001-8331-423X
*Corresponding author

Sanjay Ankali
K.L.E. College of Engineering & Technology/Department of Computer Science and Engineering, Chikodi, 591201, India
E-mail: sanjayankali123@gmail.com
ORCID iD: https://orcid.org/0000-0001-8892-0976

Shantappa Gollagi
K.L.E. College of Engineering & Technology/Department of Computer Science and Engineering, Chikodi, 591201, India
E-mail: shantesh1973@rediffmail.com
ORCID iD: https://orcid.org/0000-0002-2912-4598

Norjihan Abdul Ghani
Universiti Malaya/Department of Information System, Kuala Lumpur, 50603, Malaysia
E-mail: norjihan@um.edu.my
ORCID iD: https://orcid.org/0000-0002-0804-3916

Received: 07 September 2023; Revised: 05 November 2023; Accepted: 22 December 2023; Published: 08 June 2024

Abstract: The Internet of Things (IoT) allows you to connect a broad spectrum of smart devices through the Internet. Incorporating IoT sensors for remote health monitoring is a game-changer for the medical industry, especially in limited spaces. Environmental sensors can be installed in small rooms to monitor an individual's health. Through low-cost sensors, as the core of the IoT physical layer, the RF (Radio Frequency) identification technique is advanced enough to facilitate personal healthcare. Recently, RFID technology has been utilized in the healthcare sector to enhance accurate data collection through various software systems. Steganography is a method that makes user data more secure than it has ever been before. The necessity of upholding secrecy in the widely used healthcare system will be covered in this solution. Health monitoring sensors are a crucial tool for analyzing real-time data and developing the medical box, an innovative solution that provides patients with access to medical assistance. By monitoring patients remotely, healthcare professionals can provide prompt medical attention whenever needed while ensuring patients' privacy and personal information are protected.

Index Terms: Internet of Things (IoT), Smart Healthcare, Steganography, RFID, Sensors.

1. Introduction

With a staggering number of approximately 421 million hospitalizations occurring every year, safety and health must become the utmost priority. The Internet of Things (IoT) has enabled wireless and continuous data collection in the healthcare sector through numerous research studies. The IoT is a term used to describe modern quantitative technology for healthcare services as well as mobile or computer-based medical sensors. In recent years, platforms for social media have increasingly incorporated remote surveillance. As a method of automating and gathering data, RFID has grown in favor recently. Although RFID technology is utilized and processed in a range of industries, including retail and logistical, it is unconnected to these. To medical equipment, the IoT and the proliferation of moderate medical

sensors such as wearable, atmospheric, and embedded sensors are examples of technological innovations that can handle and produce medical knowledge. Recent research has focused on extracting physical quantities of tags from electrical radiation received, obtaining spatial quantities of tags from wireless fields received. The utilization of RFID technology proves to be highly effective in facilitating interaction with the surrounding environment in the realm of Internet of Things (IoT). Its ability to provide accurate and real-time data allows for seamless integration and communication between various devices, leading to enhanced operational efficiency and convenience. A wearable technology of the IoT gadget will be an RFID system with rechargeable batteries surroundings that will support aid services via a reader network. The study refers to the current state of RFID technology from an IoT approach. This work's purpose is to develop an Internet - of - things healthcare information system that incorporates an RFID system.

The devices with an Ultra High-Frequency medium range of 10-13.56 GHz that might be used to combine sensors for environmental and health monitoring will be the focus of this research. The IoT (Internet of Things) is a highly advanced tool used in manufacturing, commerce, and home construction. Its main function is to enable remote monitoring, analysis, and assessment of RFID-powered data. This tool is particularly useful in observation and personal healthcare as it reduces the need for human involvement. Embedded RFID systems for personal healthcare have been developed using the IoT at a high cost; however, due to user security issues and the placement of RFID tags in the human body, these systems are not yet recommended as an appropriate framework for IoT-based technology in the home is still absent. The majority of individuals were apprehensive of embedded devices, according to the survey. In healthcare monitoring systems that incorporate RFID, which is currently a contentious topic, the user's health and privacy are still inadequate. Various studies on IoT technology for remote healthcare monitoring have yielded unsatisfactory results. Patient identification can be aided by RFID technology, although these systems currently lack efficiency and user safety features.

The current systems in use do not have all of the patient's conditions in one place, which hinders the user experience. The technology uses GSR to measure heart rate, oxygen saturation, body temperature, humidity, air quality, and sweat production. Its implementation holds the promise of enhancing operational efficiency and overall efficacy. Most RFID-based managed services are effective. Effectively, address the aspects that are of concern. The RFID technology used in this scheme will act as a safe way of protecting healthcare system users. A wearable electronic device or medical box with consistent and tangible health data is more viable. This study aims to create an IoT-based personal healthcare system that utilizes RFID technology. The two-level secured platform ensures improved health analysis and privacy. Steganography is used to store the collected records. For instance, environmental and portable equipment can support the development of the medical paradigm.

Remote health support and monitoring are both made possible by the RFID smart healthcare system. The environment is being made intelligent by using inexpensive, energy-free, and disposable sensors. RFID technology used in IoT-assisted personal healthcare is beneficial for critical advancement. As well as monitoring other aspects of health like heart rate and blood pressure, sensors are employed to keep an eye on the quality of the air and prevent breathing anesthetic substances.

1.1. Major Research Objectives

The proposed research work aims to achieve the following objectives:

- Registering patients using RFID tags and acquiring their health readings through sensors. Transmitting this information, along with the patient's RFID tag, to a patient database via a mobile device and web application.
- Ensuring the patient health records are transmitted securely between the system and approved parties.
- Reading, storing, and accessing environmental and patient sensor data using Steganography and RFID technology.
- Implementing a sensor module to measure the user's health data.
- Use Steganography to store the sensor data collected and stored in the database to increase security.

1.2. Problem to be Solved in this Article

Our goal is to develop a secure healthcare system that employs IoT, RFID, and Steganography for health analysis and security enhancement. We have successfully programmed the proposed design on a Wi-Fi-based python Raspberry Pi, which allows for data to be securely hidden behind images using Steganography. Patients and their designated doctors will receive alert messages through their registered email addresses for added convenience and peace of mind.

2. Related Works

The purpose of studying related works is to investigate existing methodologies, identify issues, and determine the limitations of the present research to define the problem accurately.

R. Mitra and R. Ganiga proposed healthcare monitoring to track a patients temperature using the ZigBee mesh protocol for 24-hour care records monitoring. Records from hospitals are kept on the cloud. By continually monitoring and gathering data, reducing the cost of care, and analyzing the data, IoT-enabled devices enhance the quality of care [1]. An exposition of a health monitoring Internet of Things (IoT) system tailored for emergency medical services was

presented by A. Rghioui and A. Oumnad. This approach proves to be highly effective in reducing the overall expenses incurred in medical treatment while also addressing the anxieties and worries of patients regarding their health conditions. There is less need for patients to visit the doctor because data streams are collected, recorded, analyzed, and shared on the Internet. Doctors should routinely check health indicators like blood pressure, temperature, and heart rate [2].

It is important to explore the development of health systems for the senior population and address the concerns of patients regarding their chronic diseases [3]. Researchers like M. Gouveia, N. Da Costa, L. P. Eusébio, M. Ramiro, S. Machado, and others have emphasized the significance of effective measures that can help reduce the expenses associated with medical treatments. They went over wearable technology in depth for a remote health care system [4]. Modern medicine planning and the healthcare system must make efficient and secure use of healthcare technology, as discussed by S. Tyagi, A. Agarwal, and P. Maheshwari.

Medical equipment maintenance worries have been brought up. The development of the healthcare system must be addressed. This document highlights significant advancements in the adoption of healthcare policies. Also noted is the need for preventative efforts to raise the standard of healthcare, as well as the lack of safety regulations for medical equipment [5-7]. Li, Xu, and Wang conducted a thorough investigation into the potential benefits of compressed sensing for enhancing data acquisition in the context of both IoT and wireless sensor networks [8-10]. Through their research, they were able to gain a deeper understanding of how this technique could effectively optimize data collection and processing, ultimately leading to improved performance and more efficient operations within these systems [11-14]. Table 1 presents the existing solutions along with their respective limitations.

Table 1. Existing solutions

Authors/Year	Remarks	Limitations
Rishabh Mitra and Raghavendra Ganiga (2019)	Implementing this system can expedite processes and decrease the duration needed for sensor development.	Need to define and implement standardized protocols.
Sapna Tyagi, A. Agarwal, P. Maheshwari. (2016)	This strategy centers on utilizing an IoT cloud-based healthcare system to effectively track and monitor patient health.	This solution functions optimally exclusively in a cloud-based environment.
Cui, Lei, Zonghua Zhang, Nan Gao, Zhaozong Meng, and Zhen Li. (2019)	The extensive use of RFID sensing technology has facilitated innovative solutions in different domains.	(1) The efficiency of RF frontend energy harvesting, and power conversion limits some applications of miniature sensors. (2) To simplify the use of various types of antennas, RFID ICs, applications, and sensor data reading protocols in industry, standardization or guidelines are required.
Prosanta Gope, Youcef Gheraibia, Sohag Kabir, and Biplab Sikdar (2021)	The foundation of IoT is established on extending and applying existing protocols. This approach introduces a fault-tolerant decision-making plan for IoT-driven healthcare.	Implementing a decision-making process that can handle faults may result in increased computation overhead.

3. Information Security based on IoT for e-Health Care Using RFID Technology and Steganography

We presented this smart medical health analysis to solve some of the limits and drawbacks of existing equipment's. Both software and hardware are combined in the suggested system. It consists of an intelligent Wi-Fi-based application. In the sphere of medicine, this system provides automation. It allows doctors to keep track of their patients' health from a far. In this scheme:

- Sensors are used to extract data or readings from a patient's medical records, which are then transformed into signals.
- The Raspberry Pi, which seems to be the IoT module, receives these signals and processes. The Raspberry Pi then displays the data on a display unit and saves it to the cloud. The doctor can use his phone or laptop to acquire the ways of gathering it.

In this section, we will learn how sensors can measure heart rate and SpO2 levels in the body. The sensor is capable of detecting the user's heart rate and SpO2 level and can be programmed using software written in the Python programming language. The intelligent medical box for monitoring health utilized a Node MCU microcontroller in programming its sensor, which was able to send data to the Blynk application through Wi-Fi. In order to guarantee the precision of the sensor's readings, several tests were carried out and compared with the measurements obtained from a Samsung S10 mobile phone. In order to guarantee the reliability and efficiency of the medical box, the mean heart rate was established as the benchmark using the Samsung S10. Nonetheless, upon reviewing the data provided on the Samsung website, it was discovered that the device's readings were not entirely precise. Nevertheless, it was deemed satisfactory to proceed with this method.

The data collected by the Samsung S10 for smart health monitoring was found to be more dependable than the data collected by a medical box due to the insufficient accuracy of its sensors. In order to improve accuracy, a Sensor MQ

135 was used to track respiratory parameters and detect CO in the air. A threshold was set to identify gases using the same sensor. The Raspberry Pi was connected to the sensor's voltage output and programmed using its software. The data was measured in parts per trillion and processed using the smoke programming language. Proportion detection with a threshold was used for statistical analysis, and a notification sign was displayed on the Blynk mobile app when the proportion crossed the threshold. It's important to note that this experiment did not take an average of samples as CO content in the air varies rapidly and is not stable.

In this experiment, ten samples were taken to measure the amount of CO and smoke in the air. Normal CO levels range from 450 to 550 PPM (parts per minute) while the typical smoke concentration in a room is between 60 to 80%. When cigarette smoke is detected, the sensor triggers an alarm on the mobile app and indicates danger in the user's surroundings with a CO measurement of 755 PPM. The data is then plotted on a graph to show the change in smoke detection over time. Once the smoke clears, the air quality improves and rises above the usual level of 450-580 PPM. The sensor detects this and records it. PPM levels increase with higher amounts of smoke in the air, which can be harmful to the user's health.

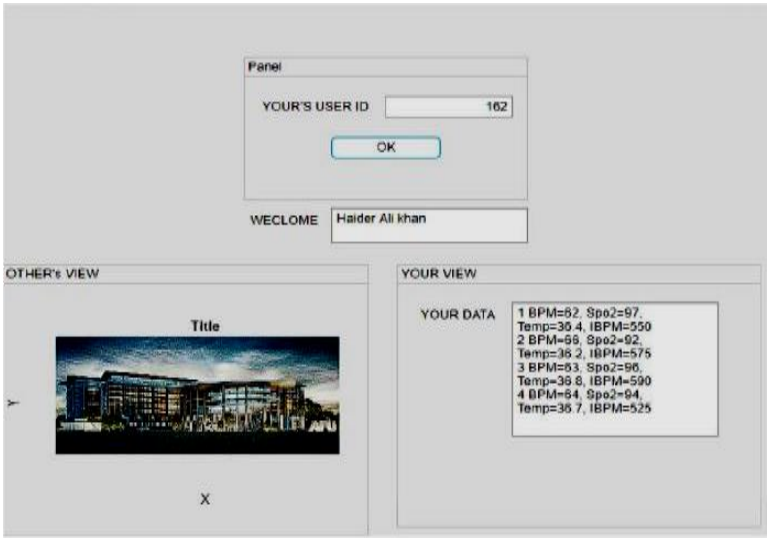


Fig.1. Steganography technology

After thorough examination of the information provided on the Samsung website, it is evident that the data is highly reliable. While there was a 17% discrepancy in the projected value of 98 BPM from the smart healthcare box during the same period, the recorded average heart rate was an impressive 83.5 BPM (Beats Per Minute). Although the sensor had to capture data outside of an industrial setting, the results obtained from the connected health box were satisfactory, with potential for further improvement. The blood oxygen level, or SpO2, was measured using two different devices with a maximum of 11 sample data collected. The collected data from the devices varied, but we calculated the mean and analyzed the overall data on the IoT platform. The smart healthcare medical box showed that the GSR sensors on fingers can measure the galvanic skin response. This is an important tool for detecting changes in emotional states based on sweat accumulation when the user moves their fingers. The technology used in this approach is Steganography, as depicted in Figure 1. After a legitimate user log in, they can access the corresponding medical data. The data is only visible to the person who logged in, while it remains hidden behind an image for others. Figure 2 illustrates the Steganography process utilized in the data security mechanism for personal healthcare based on IoT and RFID technology.

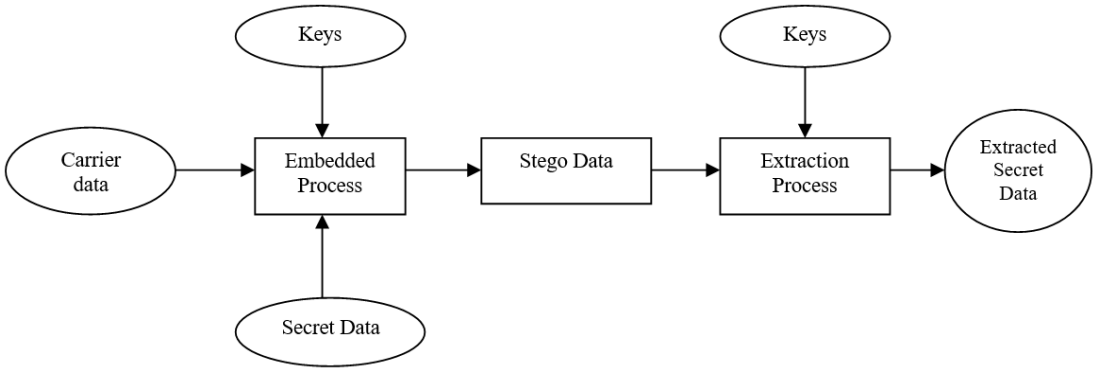


Fig.2. Steganography process

The GSR (Galvanic Skin Response) graph shows the user's regular emotion and the change in feeling just by moving their finger. There are two lines on the graph - the white line depicts the shift in mood when the person places their finger, while the red line represents their usual emotion. Once the perspiration level surpasses the predetermined threshold of 60, the graph's white line will begin to intersect with the red line for a specific period. The graph provides real-time monitoring of the user's mental well-being and can maintain data for up to three months. The smoke control alarm has two operational settings: "Normal" and "Alert". As time progresses, the smoke detection sensors transmit information to the application, which presents the smoke concentration in the vicinity.

To keep track of the body's heart rate and blood oxygen levels, a pulse sensor is utilized. This sensor is capable of measuring up to a maximum value and can be easily operated using a single finger. Apart from measuring the pulse, the sensor can also record the interbeat time or the time duration between each heartbeat. This test is conducted on patients with varying levels of physical activity, both while they are at rest and during exercise. To ensure the accuracy of the results, data was collected from five individuals and their real-time interbeat results were compared and contrasted to obtain precise readings.

3.1. Algorithm

Step 1: Import all the necessary Python modules.

Step 2: In order to encode and decode the secret data and the pixel values, we must first define a function that can convert any kind of data into binary.

Step 3: Defining a different function that alters the Least Significant Bit (LSB) of the image to conceal a hidden message.

Step 4: Writing a function to extract the Steganographic image's secret message.

Step 5: An additional method should be created that takes a user-supplied secret message and picture name and calls the hideData() function to encrypt it.

Step 6: A function is defined to ask the user for an image name and return the decoded message using the show_Data() function.

Step 7: Describing the Main method.

To determine the effectiveness of Steganography, one can compare the cover image to the Steganography image and consider various factors. These include:

Robustness: This refers to embedded data remaining intact despite stego-picture changes.

Imperceptibility: It is a Steganography algorithm's ability to remain invisible to the human eye. Therefore, imperceptibility is the most important criterion to consider.

Error Rate in Bits: The communication channel must be able to successfully recover secret information. Errors can occur when attempting to retrieve hidden information, which is measured by the Bit Error Rate (BER). The BER is the ratio of the number of faults found in an image to the total number of bits delivered.

Error in the Mean Square: Calculating the Error in the Mean Square involves a byte-by-byte comparison of the cover image and stego image. This calculation provides insight into the degree to which the image has been altered.

Signal-to-Noise Ratio: When using Steganography to embed content in an image, it is crucial to maintain high image quality. The Peak Signal-to-Noise Ratio (PSNR) is a widely accepted metric for evaluating the quality of lossy compression reconstruction. A higher PSNR value indicates superior image quality and less distortion.

3.2. Methodology

A system consisting of Raspberry Pi and Node MCU components has been proposed to facilitate data acquisition and transmission. Upon scanning an RFID card and entering the corresponding password, the system proceeds to transmit the acquired data to the IoT cloud via Node MCU. This transmission is facilitated by Raspberry Pi, which serves as an intermediary and receives information from Node MCU. It is worth noting that this process occurs seamlessly and without interruption, allowing for the timely processing and analysis of the acquired data [15, 16]. Figure 3 shows the interconnected blocks in the framework, displaying the system's architectures acting as the main controller with multiple sensors linked to the microcontroller, receiving input data from the user's hand. The system employs a two-step security feature that requires an input password to gain access, with the keypad linked to Raspberry Pi. Blynk software is utilized to display all the necessary data on the IoT platform, which Node MCU transmits via Wi-Fi connection upon successful entry of the passcode. To ensure maximum security, our system employs a two-step verification process through the RFID reader [17]. Firstly, users must place their RFID card on the reader to gain access to the data. Secondly, they must enter their unique security passcode for full access. The IoT database stores each individual's passcode, user ID, RFID tag ID, and user data received from the sensors in an array for easy analysis. This data is systematically stored in a table, allowing us to determine if a patient requires immediate medical attention. If data falls below the threshold value, our closed and automated system uses SMS technology to promptly notify both authorities and family members.

The smart healthcare medical box is equipped with an LCD system that enables users to access their healthcare data and parameters [18, 19]. Raspberry Pi processes the sensor readings from the patient's health records, converting them into signals and storing them in the cloud [20, 21]. Doctors can access this information via their phone or computer. The MQ135 sensor is used to measure CO2 and identify gases, with the voltage output connected to Arduino

mega. The Arduino IDE and Python programming language are used to analyze the data, and the serial monitor shows the results. When the percentage of detected smoke exceeds the threshold of 102, an alarm is delivered to the Blynk mobile app. Smoke detection is displayed as a percentage. Because CO2 levels in the air fluctuate quickly, an average of the samples was not taken for the experiment. The CO detection test is shown in Figure 3. Smoke detection causes the air quality to rise above the typical threshold of 450–580 PPM; the amount of smoke in the air determines the PPM and has an impact on human health [22, 23].

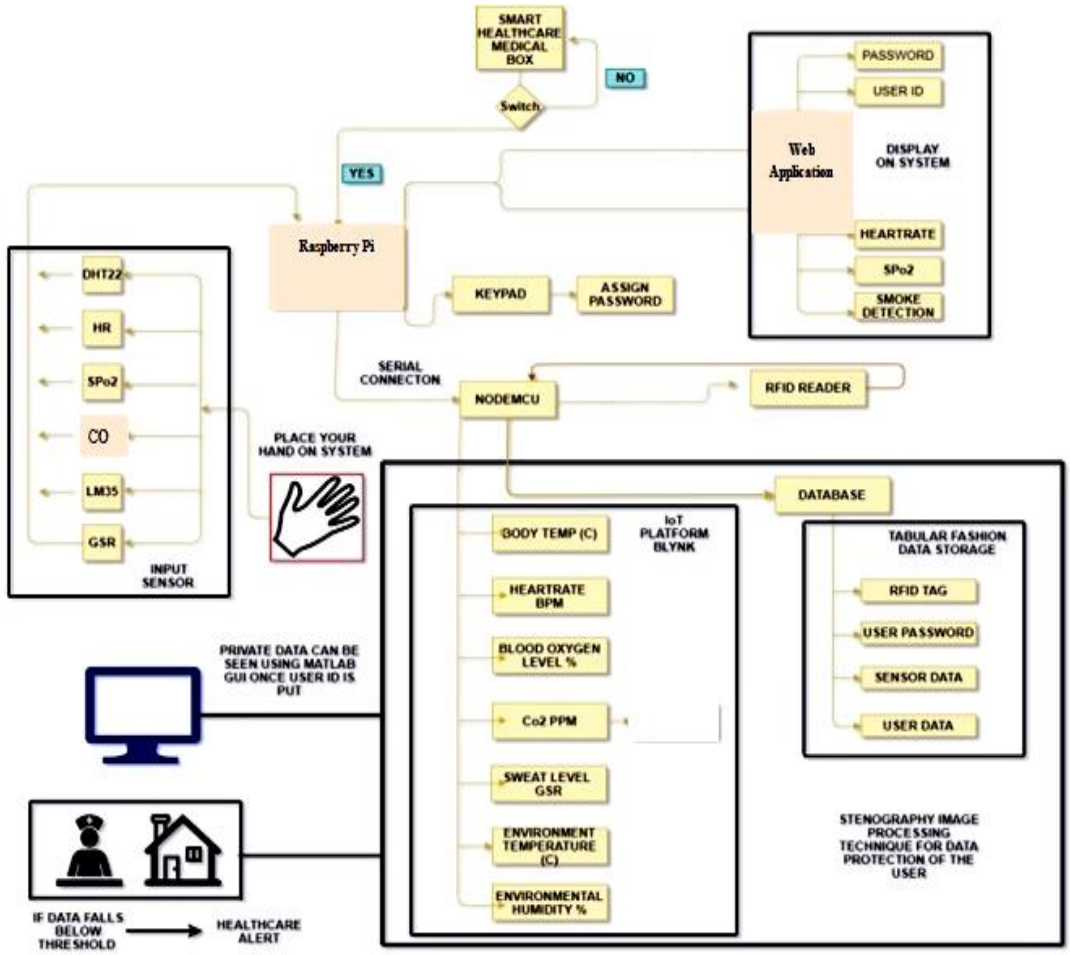


Fig.3. The system architecture

3.3. Functional Flow Diagram

The proposed work is presented in a Figure 4 flow diagram. To access the system, users are required to select the "user" button and subsequently input their unique passcode. Once authenticated, a picture will appear on the left-hand side of the screen, accompanied by a text box displaying the data stored in the database on the right. The data is strictly viewable by the authenticated user, while the image on the left is visible to all [24]. The system utilizes Steganography, a data hiding technique, to ensure user data remains secure. To initiate the system, an N.O. switch, as depicted in Figure 4, is to be utilized. Once turned on, every linked part, including the Node MCU and Raspberry Pi, which are in charge of gathering and sending data, will function. Heart rate, air quality, smoke detector, GSR, body temperature, digital humidity and temperature sensors are among the sensors incorporated inside the system's main microcontroller, the Raspberry Pi [25-27]. The OLED and LCD screens serve as the system's display unit, showcasing the patient's information.

3.4. Advancing Features of the Proposed Research Case

The scope of our proposed system will be reflected in the following points.

- This work intends to build and implement a secure personal healthcare system built on the IoT that employs RFID technology and steganography to improve patient health security and evaluation [28].
- We plan to program the proposed design on a Raspberry Pi using Python. We will integrate sensors and implement two-step security through the use of Raspberry Pi.
- The RFID system will ensure that only authorized persons can access data by scanning their card [29]. The

information will then be stored in a database and connected to the Internet of Things.

- Because the system will be recommended to be faster than the current system and may have a greater accuracy rate, issues relating to information dependability may arise during the concealment of confidential data.

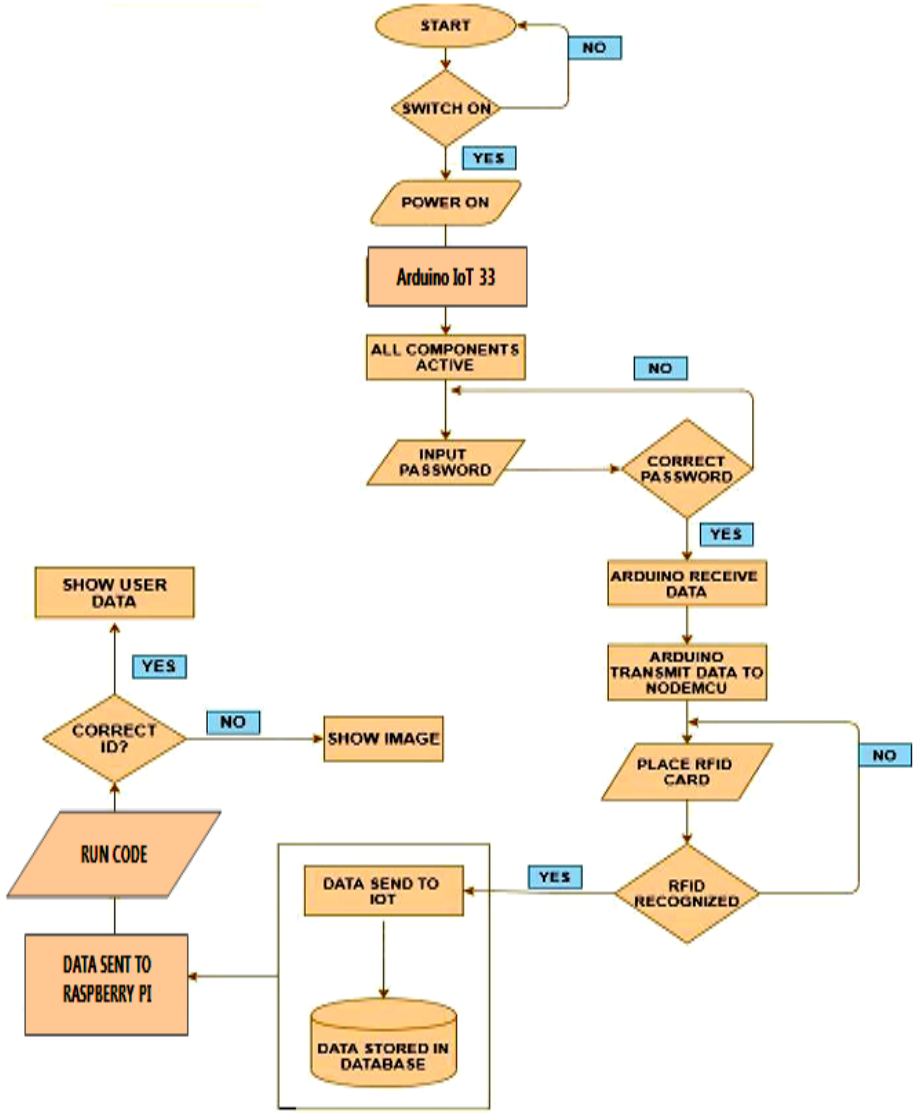


Fig.4. Flow diagram

4. Results and Discussions

Running on a Debian-based GNU/Linux operating system, Raspberry Pi OS powers the Raspberry Pi single board computer. It is also capable of running other operating systems. The Raspberry Pi 4 is an excellent platform for creating embedded systems, as shown in Figure 5. This tiny computer features an ARM V8 processor, two USB ports, an Ethernet connector, a bootable SD card slot, an HDMI and RCA display port, a 3.5mm audio input, and general-purpose I/O pins. It also includes two gigabytes of RAM. It can do anything a standard desktop computer can do, including word processing, databases, web browsing, programming, and gaming. It operates on 5 volts and features an ARM processor and the Linux Debian operating system, along with all application programs libraries. The Raspberry Pi 3, powered by the BCM2837 SoC CPU, has nearly all the same components as second-generation processors, including a set amount of RAM that can be expanded using a micro-SD card.

The proposed system utilizes an RFID module, as displayed in Figure 6. This module consists of a portable or fixed reader that connects to the network, emitting radio wave signals to activate the tag. Once activated, the tag sends a wave to the antenna, which is converted into information. Table 2, shown below, presents the average values for Actual Interbeat time, measured in milliseconds, along with Detected Interbeat time, Error Difference, and Accuracy.

To retrieve data, it is as simple as placing a single finger on the pulse sensor. From there, the system will automatically calculate the interbeat time, which is the duration required for a single heartbeat to occur. In order to test the system's accuracy, we conducted experiments on various patients who were both at rest and exercising, collecting data from a total of five individuals. This data has been carefully collated and is presented in Tables 2 and 3, allowing

us to analyze any variances between the actual interbeat time and the detected time. It is significant to remember that milliseconds are used to measure interbeat time.

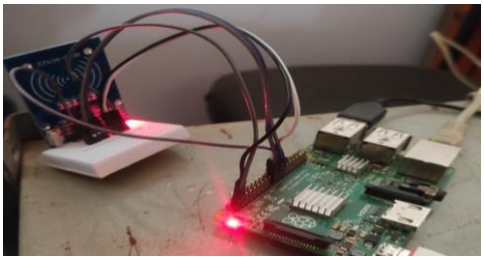


Fig.5. Raspberry Pi

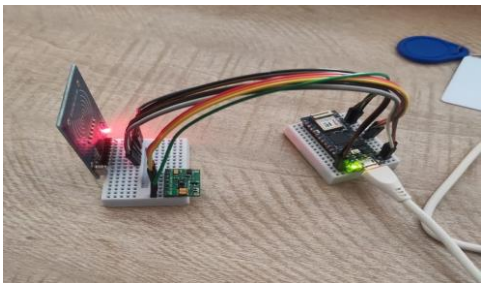


Fig.6. RFID module

Table 2. Average values for actual interbeat time, error difference and precision (when patient is exercising)

No.of People	Actual Interbeat Time [milliseconds]	Detected Interbeat Time [milliseconds]	Error Difference	Precision %
1	731.7	731.7	0.00	100
2	731.7	750	-18.3	97.5
3	652.1	625	27.1	95.8
4	833.3	882.35	-49.05	94.4
5	769.2	750	19.2	97.5

Table 3. Average values for actual interbeat time, error difference and precision (when patient is at rest)

No. of People	Actual Interbeat Time [milliseconds]	Detected Interbeat Time [milliseconds]	Error Difference	Precision %
1	468.7	483.8	-15.1	96.8
2	444.4	428.5	15.9	96.4
3	394.7	379.7	15	96.1
4	454.5	468.7	-14.2	96.9
5	434.7	491.8	-57.1	88.3

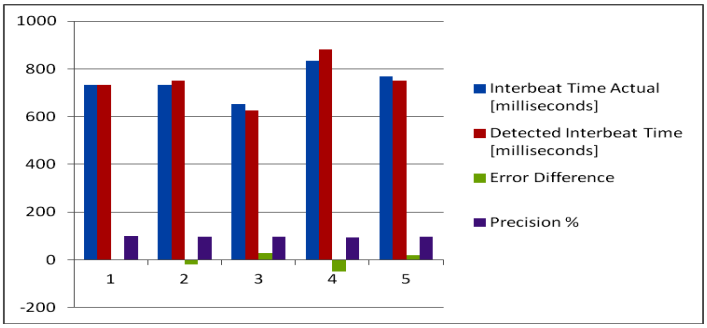


Fig.7. Plotting interbeat time (when patient is exercising)

In Figures 7 and 8, significant data is displayed regarding the time intervals between heartbeats, both during rest and exercise. These metrics provide insight into the accuracy of measurements and performance of patients under varying conditions. This information is valuable for further research and developing treatment options for individuals with similar conditions.

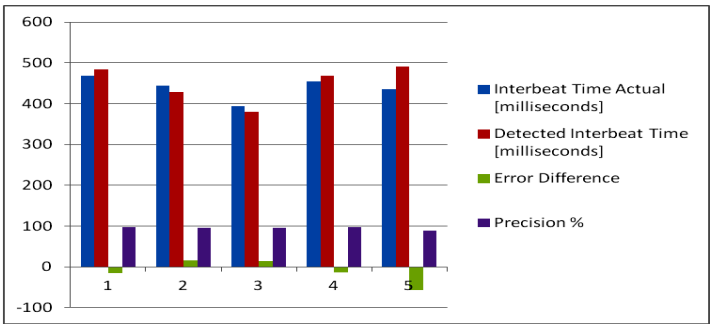


Fig.8. Plotting interbeat time (when patient is at rest)

The GSR finger sensors are user-friendly and measure the galvanic skin response, detecting emotional changes by sensing sweat on the finger. A blue line on the graph represents natural emotion, with emotional changes indicated when the line surpasses a red line for more than 60 seconds. The NodeMCU microcontroller was programmed with RFID reader software. Number_1 determines maximum heart rate; SpO2 measures oxygen levels in the blood, and LM 35 measures body temperature at precisely 36 degrees Celsius. The MQ 135 air quality sensor measures the air quality, and the CO gas concentration is shown in the GUI [30-35].

Data is transmitted when the NodeMCU is connected to Wi-Fi and latency tests predict delays in processing data. Steps can be taken to minimize delays before losing crucial data. Real-time data ranges from 0 to 1.4 seconds, while expected data is from 0 to 0.8 seconds. The system has a delay of approximately 1.7 seconds [36-39]. Figure 9 presents the health records of a specific patient, including Report ID, Patient ID, Name, Age, and Date. Clicking the "View Report" button displays the patient's sensor values during a specific timeline. Figure 10 below illustrates this display.

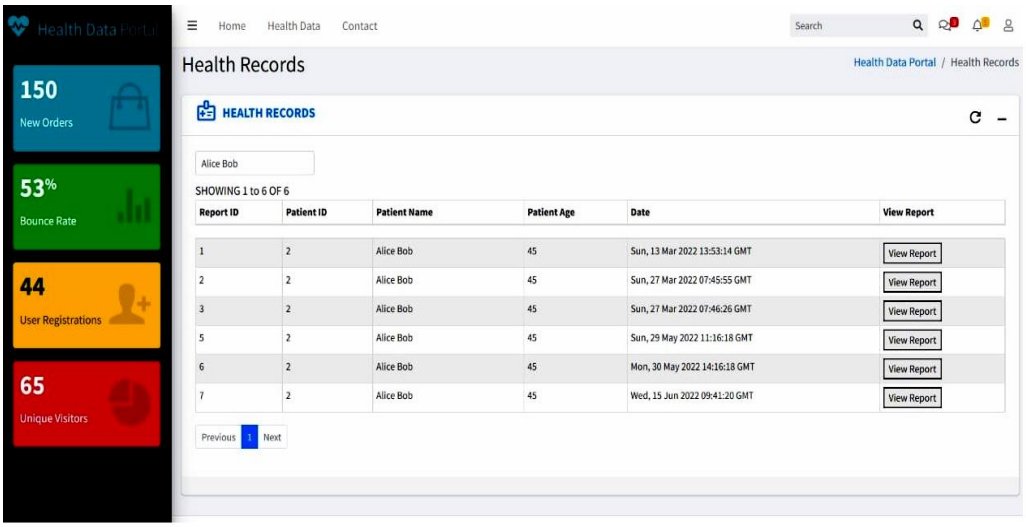


Fig.9. Health records

According to the findings depicted in Figure 11, the blue line remains above the red line for a certain duration when the sweat level surpasses the 60 threshold, as demonstrated in the graph. The prototype was subjected to rigorous testing, with 10 samples gathered and averaged to provide an accurate representation of the system's overall performance [40, 41].

Figure 12 displays the results of the web application's data analysis. GSR sensors on the fingers measure galvanic skin response, which indicates emotional changes through changes in sweat as the user moves their fingers [42-44]. The user's pulse rate and SpO2 level are monitored by max 30102 sensors, while the LM 35 sensor module detects body temperature and displays a precise result of 36 degrees [45, 46]. Additionally, the GUI tracks the amount of CO gas in the atmosphere, requiring user input [47-49]. To transfer data to the IoT platform, users insert an RFID card into the reader, which saves the data locally in a text file. The ARM architecture then stores the data in a text file, concealed within a random image using Steganography applications [50, 51]. Upon running the code, users are presented with a graphical interface (GUI) to log in and view their data by entering their unique password. Only authorized individuals have access to the data, and others can only view a screenshot. The use of Steganography technology is an essential tool in protecting user and family data privacy and security, especially in the healthcare industry.

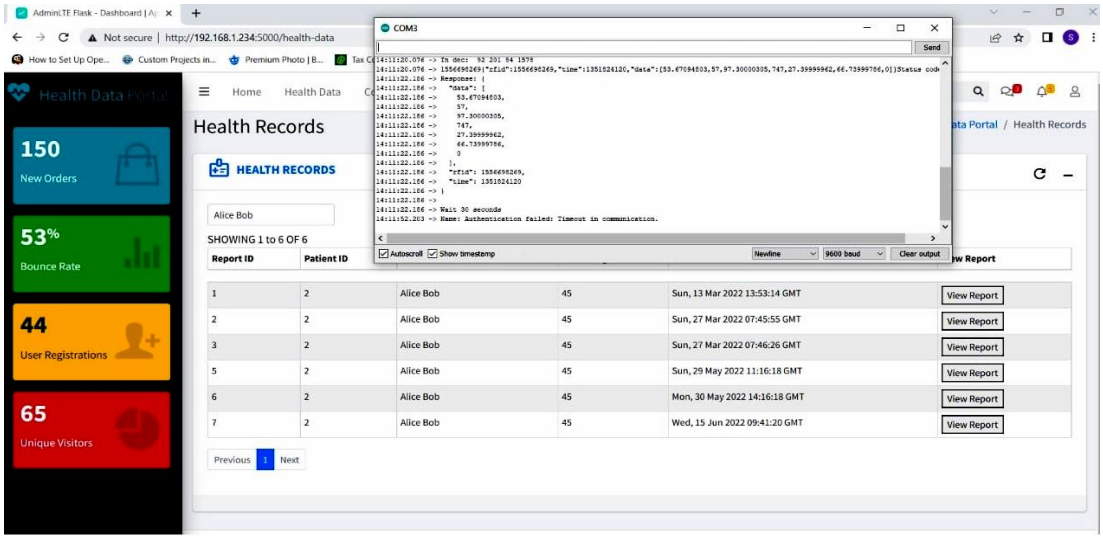


Fig.10. Display the sensor values

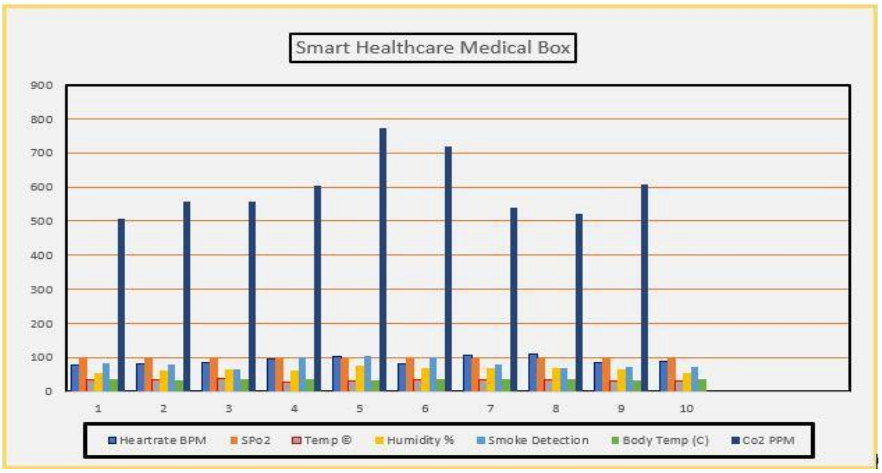


Fig.11. Integrated graphical interface evaluation

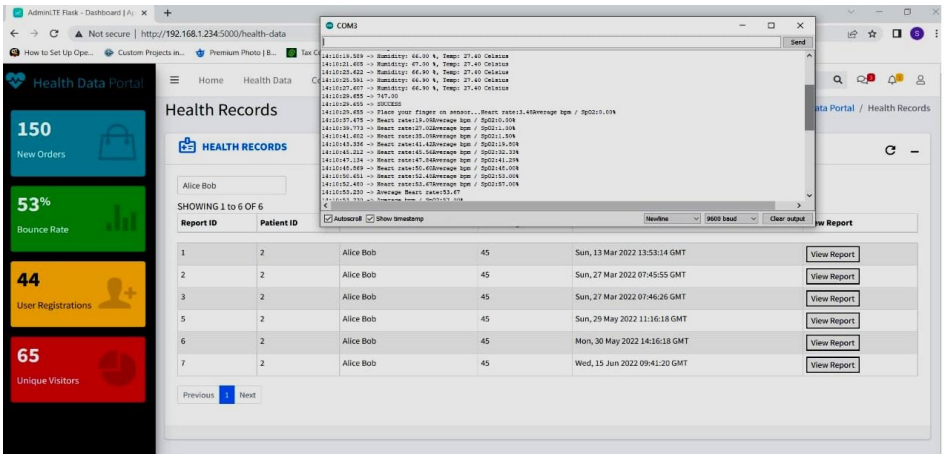
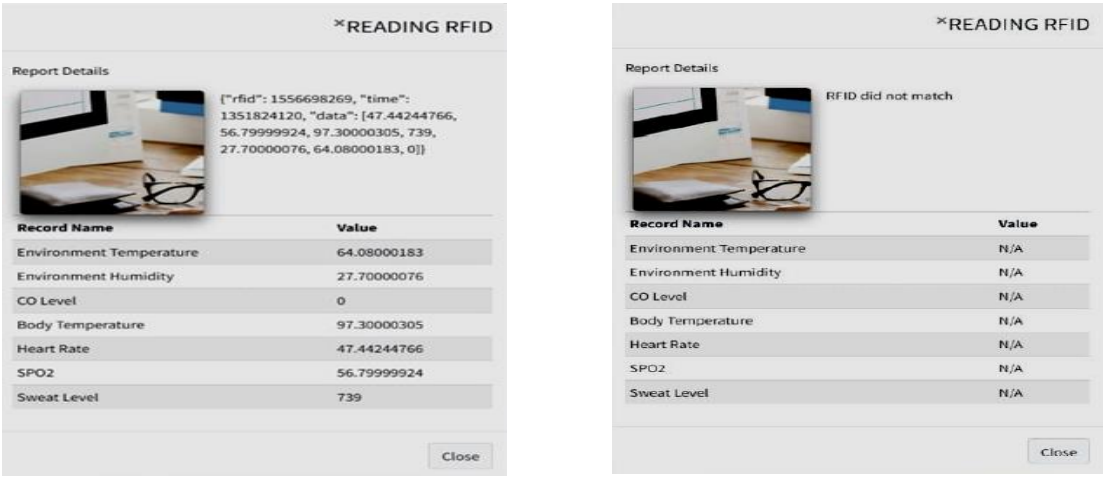


Fig.12. Average sensor data

To better comprehend the disparities between a matched RFID card and a mismatched one, refer to Figure 13. It presents a side-by-side comparison of the information displayed on both cards. The details provided therein will be instrumental in enhancing your understanding of the key differences between the two.



a. Matched RFID Card b. Mismatched RFID Card

Fig.13. RFID card details

Feasibility Study of the Proposed Research Approach

This article explores the use of an algorithm in the healthcare industry and evaluates its feasibility through three distinct studies: Technical, Operational, and Economic.

- Technical feasibility ensures that all necessary technical resources are employed in implementing the proposed model to create an operable system. Components such as Raspberry Pi, LCD Display, Node MCU, various sensors, and RFID Modules are required, and the software is developed using the Python programming language. These resources and technologies are sufficient to establish a smart medical healthcare system.
- Operational feasibility is achieved by monitoring heart rate, blood pressure, and other essential data through IoT healthcare devices. This research can yield important details regarding the patient's current condition, and the suggested design makes it simple to maintain and enhance the product. IoT-enabled healthcare facilitates better data processing and analysis.
- Economic feasibility is achieved by utilizing IoT technology to make healthcare more accessible and efficient, leading to better patient health outcomes. RFID technology offers numerous advantages for hospital asset management and patient safety. It also helps in the development of new equipment that is tailored to the needs of the patient. RFID technology helps hospitals track and manage supplies and equipment more effectively, which lowers costs while enhancing patient safety and experience.

5. Conclusions

Our objective was to develop a healthcare system that makes use of Steganography and RFID technologies to improve security and health analysis using the Internet of Things (IoT). We have successfully designed this system by using Blynk as the user interface for the IoT platform on a Wi-Fi-based Microcontroller Board, along with Python for intelligent data transmission. Additionally, we plan to use the Steganography technique to safeguard data by concealing it behind a picture. Blynk was used to develop the first GUI, while Python was used to make the second. The user's private database is only accessible to their families and doctors, increasing the accuracy and security of medical exams using RFID technology. We accomplished our objectives by implementing two-step security and connecting sensors to a Raspberry Pi. The IoT and the RFID were designed so that users cannot access data until their card has been scanned by the RFID reader, which then records the data.

Our proposed health monitoring system uses an array of sensors to gather patient data. This data is processed and transmitted through a Raspberry Pi device, which acts as both a data aggregator and processor, and can be monitored, by patients and doctors via their respective devices. Doctors can leverage the collected sensor data to improve emergency healthcare situations. During testing, the system calculated an average of 83.5 BPM (Beats Per Minute). However, a non-industrial sensor in the smart healthcare box recorded an average value of 98 BPM with a 15.5% error rate, indicating a need for increased accuracy. To ensure safer and more reliable health assessments, a separate database equipped with RFID technology was provided to consumers, accessible only to doctors and the patient's family. By integrating sensors with Raspberry Pi and implementing two-step security with RFID technology, users can access the data only after utilizing their card on the reader, which stores it in a secure database and IoT platform.

Acknowledgment

This work was supported by the UM International Collaboration Grant, under University Grant IMG005-2023

titled A Framework for Secure Health Information Exchange in Smart Healthcare Environments.

References

[1] Rishabh Mitra, Raghavendra Ganiga, “A novel approach to sensor implementation for healthcare systems using internet of things” International Journal of Electrical and Computer Engineering (IJECE), Vol. 9, No. 6, pp. 5031–5045, 2019.

[2] Selvaraj S., Sundaravaradhan S., “Challenges and opportunities in IoT healthcare systems: a systematic review”, SN Appl. Sci. 2, 139 (2020). DOI: https://doi.org/10.1007/s42452-019-1925-y.

[3] Murugan A., Chechare T., Muruganantham B., Kumar S. G., “Healthcare information exchange using block chain technology”, International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 1, pp. 421–426, 2020. DOI: 10.11591/ijece.v10i1.pp421-426.

[4] F. Fernandez. G. C. Pallis, "Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective", 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), Athens, Greece, 2014, pp. 263-266. DOI: 10.1109/MOBIHEALTH.2014.7015961.

[5] Tyagi S., Agarwal A., Maheshwari P., “A conceptual framework for IoT-based healthcare system using cloud computing”, in 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Jan. 2016, pp. 503–507. DOI: 10.1109/CONFLUENCE.2016.7508172.

[6] Cui, Lei, Zonghua Zhang, Nan Gao, Zhaozong Meng, Zhen Li., "Radio Frequency Identification and Sensing Techniques and Their Applications—A Review of the State-of-the-Art", Sensors 19, No. 18: 4012. DOI: https://doi.org/10.3390/s19184012.

[7] Alrowaily MA, “Utilizing beacon technology for the development of a smart attendance system”, International Journal of Advanced and Applied Sciences, 9(6): 26-35.

[8] Eldemerdash T., Abdulla R., Jayapal V., Nataraj C., Abbas M. K., “IoT Based Smart Helmet for Mining Industry Application”, Int. Journal of Advanced Science and Technology, Vol. 29, No. 1, pp. 373–387, 2020.

[9] G. Sushanth and S. Sujatha, "IOT Based Smart Agriculture System," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2018, pp. 1-4, DOI: 10.1109/WiSPNET.2018.8538702.

[10] A. A. Khan, A. I. E. Yakzan, M. Ali, "Radio Frequency Identification (RFID) Based Toll Collection System", 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, Indonesia, 2011, pp. 103-107. DOI: 10.1109/CICSyN.2011.33.

[11] Lakshmanan R., Djama, M. Selvaperumal S. K., Abdulla R., “Automated smart hydroponics system using internet of things,” International Journal of Electrical and Computer Engineering (IJECE), vol. 10, No. 6, pp. 6389–6398, 2020. DOI: 10.11591/ijece.v10i6.pp6389-6398.

[12] Aziz, A., Osamy, W., Khedr, A.M., Salim, A., “Chain-routing scheme with compressive sensing-based data acquisition for Internet of Things-based wireless sensor networks”, IET Netw, 10: 43-58. DOI: https://doi.org/10.1049/ntw2.12002.

[13] Nupur Agrekar, Nilesh P.Bodne, “An Insight on RFID technology and Future challenges”, Int. J S Res Sci. Tech. 2018 May-June; 4(8) : 225-231.

[14] Shivangi Pandey, “RFID Technology for IoT Based Personal Healthcare in Smart Spaces”, International Journal of Scientific & Engineering Research, Volume 7, Issue 8, August-2016.

[15] C.E.Turcu and C. O. Turku, “Internet of Things as Key Enabler for Sustainable Healthcare Delivery”, Procedia - Social and Behavioral Sciences, Vol. 73, pp. 251–256, 2013.

[16] Muhammad Nadeem Akhtar, Muhammad Adrees, Muhammad Mukhtar Qureshi, Zulfiqar Ali, “Ethical Issues of Radio Frequency Identification Chips Implanted in Human Bodies: A Review”, Indian Journal of Science and Technology, January 2020, Vol 13(03), 269–276, DOI: 10.17485/ijst/2020/v13i03/147192.

[17] A.G. Sampoornam, “An Efficient Healthcare System in IoT Platform Using RFID System”, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 5, No. 2, pp. 421–424, 2020.

[18] K. Natarajan, B. Prasath, P. Kokila, “Smart Health Care System Using Internet of Things”, Journal of Network Communications and Emerging Technologies, Volume 6, Issue 3, March (2016).

[19] Firouzi, F., Rahmani A. M., Mankodiya K., Badaroglu M., Merrett, G. V., Wong P., Farahani B., “Internetof-Things and Big Data for Smarter Healthcare: From Device to Architecture, Applications, and Analytics”, Future Generation. Compute. Syst., Vol. 78, pp. 583–586, Jan. 2018. DOI: 10.1016/j.future.2017.09.016.

[20] E.Radhamma, Mr.P.Lachi Reddy, Mr.A.SravanKumar, “Smart Farm Monitoring Using Raspberry Pi and Arduino”, International Journal of Scientific Development and Research, Volume 1, Issue 9, 2016.

[21] Prosanta Gope, Youcef Gheraibia, Sohag Kabir, Biplab Sikdar, “A Secure IoT-based Modern Healthcare System with Faulttolerant Decision Making Process”, IEEE Journal of Biomedical and Health Informatics, 2020. DOI: 10.1109/JBHI.2020.3007488.

[22] M., Gómez-Inhiesto, E., Acaiturri-Ayesta, M.T., “Implementation and Evaluation of a RFID Smart Cabinet to Improve Traceability and the Efficient Consumption of High Cost Medical Supplies in a Large Hospital”, Journal of Med. Syst. 43, 178 (2019). DOI: https://doi.org/10.1007/s10916-019-1269-6

[23] Pramod Kumar, "An Overview of IoT-Aware Architecture for Smart Healthcare Systems", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 9, page no.38-42, September 2018.

[24] Mohammed Imtyaz Ahmed, Govindaraj Kannan, “Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring”, Journal of King Saud University – Computer and Information Sciences 34 (2022) 6895–6908, Volume 34, Issue 9, October 2022.

[25] T. Kellomaki, “On-body performance of a wearable single-layer RFID tag”, IEEE Antennas Wireless Propag. Lett. Vol. 11, pp. 73– 76, Jan. 2018.

[26] C. Occhiuzzi, S. Cippitelli, G. Marrocco, “Modeling, design and experimentation of wearable RFID sensor tag,” IEEE Trans. Antennas Propag., Vol. 58, No. 8, pp. 2490–2498, Aug. 2016.

[27] S. Manzari, C. Occhiuzzi, G. Marrocco, “Feasibility of body-centric passive RFID systems by using textile tags”, IEEE Antennas Propag. Mag., Vol. 54, No. 4, pp. 49–62, Aug. 2017.
[28] C. Storni, “Report in the reassembling health workshop: Exploring the role of the Internet of Things”, J. Particip. Med. Conf., Vol. 2, Sep. 2018.
[29] E. Di Giampaolo, F. Fornì, G. Marrocco, “RFID network planning by particle swarm optimization”, Appl. Compute. Electromagnets. Soc. J., Vol. 25, No. 3, pp. 263–272, Mar. 2015.
[30] C. Occhiuzzi, A. Rida, G. Marrocco, and M. Tentzeris, “RFID passive gas sensor integrating carbon nanotubes”, IEEE Trans. Microw. Theory Techn., Vol. 59, No. 10, pp. 2674–2684, Oct. 2019.
[31] S. Manzari, C. Occhiuzzi, S. Newell, A. Catini, C. Di Natale, G. Marrocco, “Humidity sensing by polymer-loaded UHF RFID antennas”, IEEE Sens. J., Vol. 12, No. 9, pp. 2851–2858, Sep. 2018.
[32] Teh, H.Y., Kempa-Liehr, A.W., Wang, K., “Sensor data quality: a systematic review”, J Big Data 7, 11 (2020). DOI: https://doi.org/10.1186/s40537-020-0285-1.
[33] Krishnamurthi, Rajalakshmi, Adarsh Kumar, Dhanalekshmi Gopinathan, Anand Nayyar, Basit Qureshi. 2020. "An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques", Sensors 20, No. 21: 6076. DOI: https://doi.org/10.3390/s20216076.
[34] Khan, Muhammad Adnan, Intisar Ali Sajjad, Mustanser Tahir, Abdul Haseeb, "IOT Application for Energy Management in Smart Homes", Engineering Proceedings 20, No. 1: 43. DOI: https://doi.org/10.3390/engproc2022020043.
[35] Uras Panahi, “Enabling secure data transmission for wireless sensor networks based IoT applications”, Ain Shams Engineering Journal, Volume 14, Issue 2, March 2023, 101866, DOI: https://doi.org/10.1016/j.asej.2022.101866.
[36] Mena, Alma Rosa, Hector G. Ceballos, Joanna Alvarado-Uribe, "Measuring Indoor Occupancy through Environmental Sensors: A Systematic Review on Sensor Deployment", Sensors 22, No. 10: 3770. DOI: https://doi.org/10.3390/s22103770.
[37] Wong, Chun Man Victor, Rosanna Yuen-Yan Chan, Yen Na Yum, Kangzhong Wang, "Internet of Things (IoT)-Enhanced Applied Behavior Analysis (ABA) for Special Education Needs", Sensors 21, No. 19: 6693. DOI: https://doi.org/10.3390/s21196693.
[38] Miyazaki, Yusuke, Kohei Shoda, Koji Kitamura, Yoshifumi Nishida, "Assessing Handrail-Use Behavior during Stair Ascent or Descent Using Ambient Sensing Technology", Sensors 23, No. 4: 2236. DOI: https://doi.org/10.3390/s23042236.
[39] Fereira, Rolden, Chathurika Ranaweera, Kevin Lee, and Jean-Guy Schneider., "Energy Efficient Node Selection in Edge-Fog-Cloud Layered IoT Architecture", Sensors 23, No. 13: 6039. DOI: https://doi.org/10.3390/s23136039.
[40] V. Shankar, Sunethra Kandagatla, Kumar Dorthi, V. Chandra Shekhar Rao, Praveen Ankam, N. Swathi, "Smart farming using IOT", AIP Publishing, 2022.
[41] “Advances in Manufacturing and Industrial Engineering", Springer Science and Business Media LLC, 2021.
[42] Osama Zaid Salah, Sathish Kumar Selvaperumal, Raed Abdulla. "Accelerometer based elderly fall detection system using edge artificial intelligence architecture", International Journal of Electrical and Computer Engineering (IJECE), 2022.
[43] Shruti, Monika Singh. "Intelligent HealthCare System using Raspberry Pi", 2021 International Conference on Technological Advancements and Innovations (ICTAI), 2021
[44] V. Lokeswara Reddy, "Improved Secure Data Transfer Using Video Steganographic Technique", International Journal of Rough Sets and Data Analysis, 2017.
[45] S.C. Shiralashetti, A.B. Deshi, P.B. Mutalik Desai, "Haar wavelet collocation method for the numerical solution of singular initial value problems", Ain Shams Engineering Journal, 2016.
[46] "The semiconductor device technology and its societal impact", Nano-Scaled Semiconductor Devices Physics Modelling Characterisation and Societal Impact, 2016.
[47] Apeksha Thorat, Sangeeta Kumari, Nandakishor D. Valakunde, "An IoT based smart solution for leaf disease detection", 2017 International Conference on Big Data, IoT and Data Science (BID), 2017.
[48] Gemma Bird, Davide Schmid, "Humanitarianism and the ‘Migration Fix’: On the Implication of NGOs in Racial Capitalism and the Management of Relative Surplus Populations", Geopolitics, 2021.
[49] Nicolás Gaggion, Federico Ariel, Vladimir Daric, Éric Lambert, "ChronoRoot: High throughput phenotyping by deep segmentation networks reveals novel temporal parameters of plant root system architecture", Cold Spring Harbor Laboratory, 2020.
[50] Abhinav Agarwal, Sandeep Malik. "A Brief Review on Various Aspects of Steganography Followed by Cryptographic Analysis", 2022 IEEE 7th International conference for Convergence in Technology (I2CT), 2022.
[51] E. N. GANESH, "Health Monitoring System using Raspberry Pi and IOT", Oriental journal of computer science and technology, 2019.

Authors’ Profiles

Dr. Bahubali M. Akiwate is an Associate Professor in the Department of Computer Science and Engineering at KLE College of Engineering and Technology in Chikodi, Karnataka, India. He has over 12 years of experience in teaching and research. He holds a Bachelor of Engineering degree in Computer Science and Engineering, an M.Tech. in Digital Communication and Networking, and a Ph.D. in Computer and Information Science from Visvesvaraya Technological University, Belagavi. His research interests include Cryptography, Information Security, and Networking. You can reach him at his email address: bahubalimakiwate@gmail.com.

Dr. Sanjay B. Ankali is an Associate Professor in the Department of Computer Science and Engineering at the College of Engineering and Technology, Chikodi, Karnataka, India. He has 12 years of teaching experience and 7 years of research experience. He received his bachelor's degree in computer science and engineering, M.Tech. in Computer Networking, and Ph.D. in Computer and Information Science from VTU, Belagavi. His research interests include software engineering, software clone detection, and code plagiarism detection. If you wish to contact him, you can reach out via email at sanjay.ankali@yahoo.com.

Dr. Shantappa G. Gollagi is a Professor in the Department of Computer Science and Engineering at KLE College of Engineering and Technology in Chikodi, India. He has 24 years of teaching experience and 7 years of research experience. Dr. Gollagi earned his bachelor's degree in computer science and engineering from BVB College of Engineering and Technology in Hubli, his M.Tech. in Computer Engineering from COEP in Pune, and his Ph.D. in Computer and Information Science from VTU in Belagavi, India. His research interests include software security, image processing, and pervasive computing. He can be contacted via email at shantesh1973@rediffmail.com.

Dr. Norjihan Abdul Ghani is an Associate Professor and Head of Department at Department of Information Systems, Faculty of Computer Science & Information Technology. Her PhD in Computer Science from Universiti Teknologi Malaysia (2013), and her master's in information technology (2000) from Universiti Kebangsaan Malaysia and she obtained her bachelor's degree in information technology from Universiti Utara Malaysia (2000). Currently, she is the Head of Department for Information Systems since 7 October 2019. Her research interest is in the areas of information security which she focuses more on information privacy, data security and data protection. Norjihan managed to secure various research grants from internal and external funds as Principal Investigator, and a co-researcher for many grants.

How to cite this paper: Bahubali Akiwate, Sanjay Ankali, Shantappa Gollagi, Norjihan Abdul Ghani, "Information Security based on IoT for e-Health Care Using RFID Technology and Steganography", International Journal of Information Technology and Computer Science(IJITCS), Vol.16, No.3, pp.22-35, 2024. DOI:10.5815/ijitcs.2024.03.03