Babylonian Journal of Internet of Things
Vol.2024, **pp**. 126–136
DOI: https://doi.org/10.58496/BJIoT/2024/015; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

IoT of Healthcare Innovation Solutions for Predictable Virus Detection

Sara Salman Qasim[1,*],

[1] *College of Computing & Informatics (CCI), University Tenaga Nasional (UNITEN), Putrajaya Campus, Malaysia.*

ARTICLE INFO

Article History

Received 29 Jul 2024
Revised: 28 Sep 2024
Accepted 29 Oct 2024
Published 15 Nov 2024

Keywords

Quick Response
Internet of Thing
One-Time Password
Arduino
healthcare system

ABSTRACT

The evolution of health care systems from old models to more personalized frameworks facilitates easier diagnosis, treatment, and monitoring of patients, benefiting numerous individuals. Individuals receive remote treatment and care, which is essential for some during the global crisis exemplified by Predictable Virus Detection. This manuscript, A medical platform features an architecture reliant on middleware and database support for individuals with Coronavirus, primarily serving three user categories. The administrator is categorized into two user groups: doctors and patients. The doctor has an app that questions through the patient so he knows the patient that is being visited and extracts the health identity from him, and he questions the patient for sending him an OTP in the event that the patient does not have a mobile screen or an Internet connection. Alternatively, if QR inquires whether his laptop is intelligent and connected to the Internet. The individual will gain access to the system subsequent to the doctor's examination. The patient will conduct a self-examination using his equipment and present the results to his doctor. The physician is able to provide a prescription each time he transmits new readings. If the prescription is accurate, retain it and escalate the dosage; do not incorporate an additional dose. Physicians will utilize the prescription interface to transmit the prescription for cloud authentication and acquire an encrypted QR code, which will subsequently be provided to the medication receiver. The patient is afforded the opportunity to examine medicine information through the recipient's application. The entitlement to access QR protected cloud data is perpetual. The pharmacy can dispense the medication just as prescribed until the QR code's expiration date. The initiative aims to enhance access to healthcare facilities for patients and physicians, while adhering to GDPR regulations.

1. INTRODUCTION

In light of the Internet's success in connecting individuals globally, it is now the time for the objects in our environment to integrate into the global intelligence network referred to as "the Internet." [1] The Internet of Things The Internet of Things (IoT) refers to a collection of interconnected devices that can communicate with one another (machine-to-machine) or with humans (machine-to-human) throughout the day [2].

The word initially emerged in the twentieth century, namely in 1999 AD, introduced by British scientist Kevin Ashton, who proposed the concept of interconnecting various gadgets in our environment, such as electrical and residential appliances, to monitor their state [3].

Managing the ratios of lighting, temperature, and humidity within the home through self-regulation and remote management of various devices. In addition to assessing human health by observing potential signs and predicting diseases, particularly those that could result in severe health complications. Besides its diverse industrial applications, it serves as a monitoring device and equipment in factories, forecasts potential defects, mitigates losses, and facilitates the timely availability of spare parts [4].

The healthcare industry has gained advantages from digital transformation and contemporary communication technologies, and their use is expected to increase significantly. In the forthcoming years, the trends of the Internet of Smart Things will be influenced by the ongoing advancements in communication systems and artificial intelligence technologies, which have facilitated the development of creative methodologies that enhance healthcare services.[5].

*Corresponding author. Email: it@gmail.com

The Internet of Things is swiftly emerging as a vital technology in healthcare monitoring due to its ability to cut costs, enhance service efficiency, and provide sophisticated consumer interfaces. The Internet of Things is anticipated to proliferate in healthcare owing to its substantial capabilities, encompassing mapping, recognition, verification, and data collection.[6].

Following the 1918 influenza pandemic, COVID-19 has emerged as the most significant worldwide public health epidemic. As per the latest study by the World Health Organization (WHO), verified COVID-19 cases exceeded 31 million as of September 2020, with around 960,000 fatalities. Fever, cough, and nausea are influenza-like symptoms that must be identified to facilitate early diagnosis of the illness [7-10]. The incubation period for COVID-19 ranges from 1 to 14 days. Unexpectedly, a patient may transmit the COVID-19 virus to others despite exhibiting no symptoms. Isolation of these persons is necessary at this juncture [10].

The recovery duration for this disease varies based on the patient's age, underlying conditions, and other circumstances, ranging from 6 to 41 days in total [11]. Despite this disease's significant potential for rapid transmission compared to other coronaviruses, numerous efforts and trials are underway to curtail the virus's spread. IoT technology has demonstrated its efficacy and security in addressing the COVID-19 pandemic in this context [12].

2. RELATED WORK

Previous studies in medical science have utilized the Internet of Things to monitor patient health. Which systems exert the greatest influence on the healthcare monitoring model for IoT, and which can be circumvented in its design. Table (1) presents many studies on IoT applications in healthcare monitoring.

TABLE I. IOT APPLICATIONS IN HEALTHCARE MONITORING.

Ref.	**Methodology**	**Independent**	**Dependent**
[13]	Model of Technology Acceptance	Device sensor	The study relied on daily health assessments, measuring bodily indicators, and reporting findings to medical professionals, with information about the outcomes provided through a web application.
[14]	A mobile computer regulated Arduino-based health parameter monitoring.	Avoid utilizing alternative devices for the transfer process and employ a Bluetooth device with limited range.	Analog values are converted into digital data using Bluetooth, while physical attributes are transmitted to the existing system.
[15]	Ethernet Wi-Fi Arduino	Do not utilize other gadgets, as several sensors cannot be adequately managed.	The DS18B20 sensor was used to measure body temperature and pulse rate, while the Wi-Fi module and Ethernet shield enabled data transfer from Arduino to the cloud.
[16]	The ARDUINO-UNO module functions as a microcontroller in conjunction with cloud computing.	No specific performance measures are mentioned for any subject.	The Arduino-UNO was used as the processing unit, capturing data from various sensors such as heartbeat, SpO2, temperature, and eyeblink.
[17]	Wireless Local Area Network, Liquid Crystal Display, wireless communication.	----	Sensors monitored body temperature, heart rate, and humidity, which were displayed on an LCD and transmitted to a medical server via wireless communication.
[18]	BP sensor ECG sensor raspberry pi.	The primary limitation of the system is the absence of built interfaces for data visualization.	Sensor data from various devices, including Raspberry Pi, temperature, blood pressure, pulse, and ECG sensors, was collected and processed before returning to the Internet of Things network.

3. BACKGROUND THEORY

1. The GDPR, which stands for the General Data Protection Regulation

The GDPR stands for General Data Protection Regulation and is the data protection and privacy regulation law governing in the EU and the EEA. It does not only relate to processing the personal data but also relates to either transmission of such data outside the Union or to any third country. As it was mentioned earlier, the GDPR is considered as the most significant amendment to the data protection legislation over the last twenty years up to the time of the occurrence of the current application of the global ones, which collect and process personal data.

In general the main purpose of the GDPR is to make individual control over the personal information the key purpose. This regulation also aims at providing a more structured legal framework for international operations with reference to the business entity itself and the liberalised data transfer across borders while, at the same, time maintaining a very high level of data protection.

Thus for those who discharge the Duty of managing the online user Authentication the GDPR provides them the roadmap and procedures to follow more so the regulation attaches prominence to the principle of security and consent of the user. Consequently, the GDPR can be qualified as a major advancement in the question of privacy rights and individuals' decisional freedom for the Information Society [19].

2. One-Time Password (OTP)

In digital interfaces, a password that is only operational for a single session or the login transaction is recognized as the one-time password (OTP). It can also be referred to as single use PIN, one time password, one time personal identification number (PIN), dynamic password, or comfortable password. OTPs overcome various problems which are attributed to the use of conventional static password system.

Almost every application of two factor authentication includes the use of a one time password along with what a user has (like a hardware token, smart card, or a specific mobile device) and what a user knows (such as a personal identification number).

Also, the production of OTPs depends on algorithms that employ either pseudo random or random factors, and therefore it becomes very difficult for the attackers to guess subsequent OTPs. Further, perhaps use may be made of a cryptographic hash function in deriving other values from the OTPs, which cannot actually be reverse-engineered. This security measure is very important because the attacker can easily guess the future OTPs in case he or she gets the previous ones.

Fig1. The One Time Password massages.

3. Quick Response (QR)

Since it is possible for them to encode more information, short matrix codes, including Quick Response (QR) codes, are seen to have the capability to be deployed at larger scales than that of one-dimensional codes. The QR code was first designed in 1994 by the Denso-Wave Company in Japan and now has been officially standardized by the International Organization for Standardization (ISO) [1]. Normally, QR codes can be used in different aspects in people's daily life including data collection, connection building, tracking, verification, and authentication. Furthermore, since QR codes offer info transmission without contact, an appealing new trend has developed with the mode of QR codes that can be utilized offline. 1. For instance, the segmental loss and symbol effect are associated with barcodes, but a QR code is not sensitive to such. The details that is encoded in a QR codes is open knowledge for any hoodlum, thus this is not reasonable as a method of storing sensitive data. The last year has shown a number of efforts to embed messages into QR codes and to secure them [21]

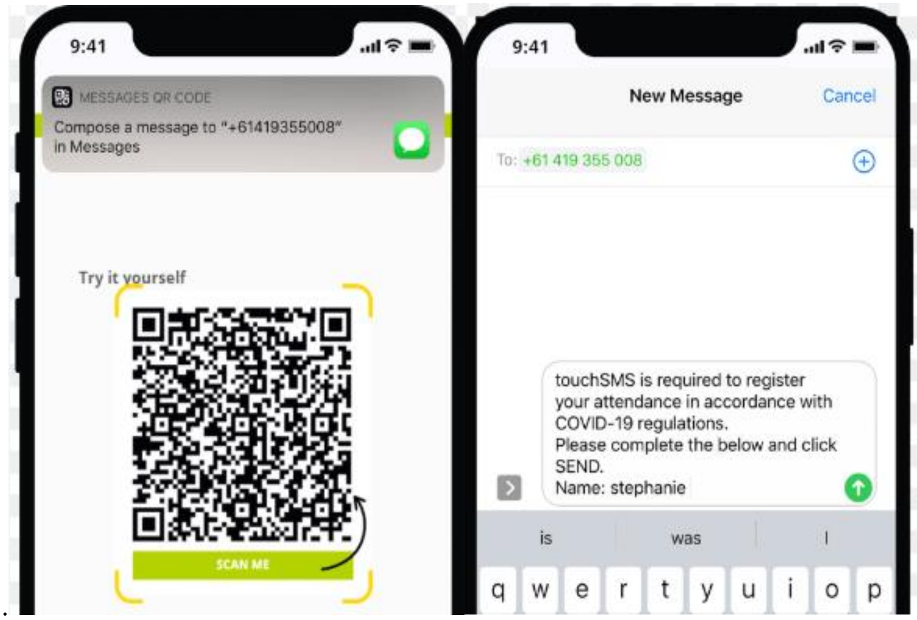

Fig. 2. Quick Response message

4. METHODOLOGY

The system that is being proposed is comprised of two phases: the hardware phase and the software phase. The hardware element of the system is comprised of the devices that are utilized in this system to evaluate the individual who has Covid 19, including the sensors that measure heartbeats, temperature, and oxygen rate. The name of the device is Raspberry Pi4, and it is the most powerful and feature-rich Raspberry Pi that has ever been launched. It is a remarkable upgrade over the boards that came before it. There are three phases that make up the software component. These phases reflect the interface that is utilized through the mobile, frontend, and backend facets. All of the components that were utilized will be discussed in the following paragraphs. Within the software phase, the suggested system was depicted in Figure (3)(4).

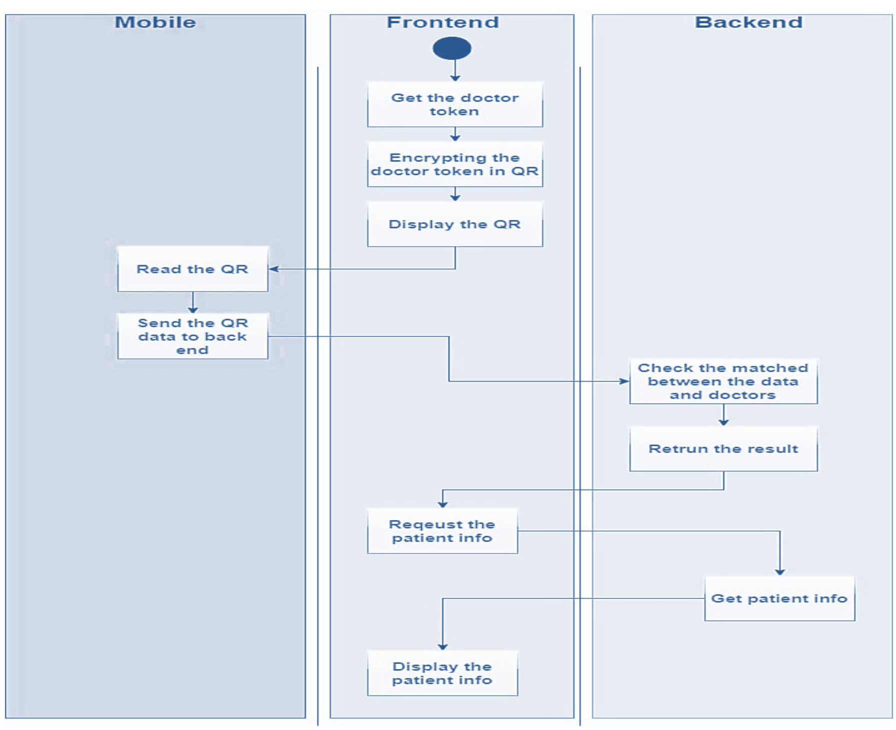

Fig.3. Conceptualization of a QR-based patient assistance system.

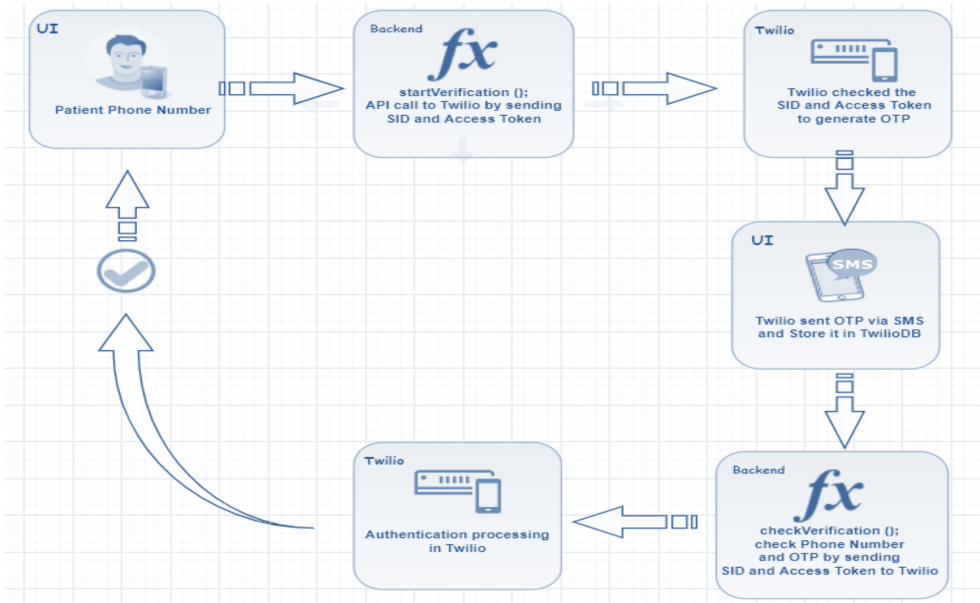

Fig. 4. System of Proposal for the Support of Patients using OTP

A. Hardware phase

The several kinds of medical equipment that were utilized by the healthcare system in order to assess a patient who was infected with the coronavirus will be discussed in this section.

1. Sensors

Two types of sensors were used as shown below:

• The GY-906 MLX90614ESF is a contactless temperature sensor module configuration.

The GY-906 MLX90614ESF Contactless Temperature Sensor Module is an infrared thermometer compatible with Arduino and other microcontrollers with an I2C device. It comes with a breakout board and two pin types, but has not been soldered. The solder jumpers may require soldering depending on the application

Fig.5 .The GY-906 MLX90614ESF is a contactless temperature sensor module configuration.

• This is an open-source hardware development sensor for the microcontroller that measures the heart rate (pulse).

The Pulse Sensor Amped is a microcontroller open-source hardware development sensor that helps determine heart rate, which is crucial for various purposes like exercise routine design, fitness analysis, and synchronizing shirt blinking with heartbeat.

Fig.6. open-source hardware development sensor for the microcontroller that measures the heart rate (pulse).

• Pulse Oximeter (SPO2) Heart-Rate Sensor Module MAX30100

The MAX30100 sensor, featuring pulse oximetry and heart rate monitoring, uses LEDs, photodetector, calibrated optics, and low-noise analog signal processing. It uses 1.8V and 3.3V power supplies and can be turned down with minimal standby current.

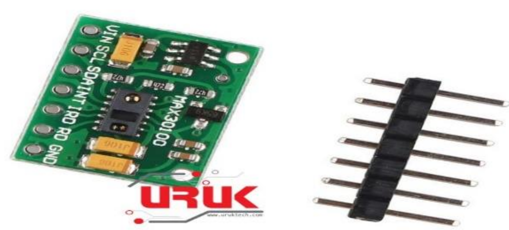

Fig. 7. The MAX30100 Heart-Rate Sensor Module is a Pulse Oxmeter (SPO2).

2. Software Phase

A central token issuance system is incorporated into the system. This system is responsible for issuing and verifying encrypted tokens, which are the foundation of this plan to secure prescription data that facilitates the treatment of a patient with Covid 19. Prescriptions are kept in the cloud as document objects, and the one-of-a-kind identifier that is generated by the cloud storage is encrypted and encoded into a mapping QR code that has some degree of authenticity.

- **Platform**

When it comes to managing users (including adding users and altering rights), the platform has three different categories of customers. The system administrator is the most powerful of these customers, and they have the maximum privileges. Additionally, they have access to a comprehensive dashboard that contains statistics for all medical centers.

From the perspective of the physician, his privileges are restricted to the addition of a new visit only after receiving the patient's consent (this is the second development of the letter), and he also possesses a dashboard that is specialized in the statistics of his own patients.

Last but not least, the subscriber to the medical platform who possesses the ability to approve the doctor through the mobile application by means of the QR code or the OTP, as well as the customers and references, includes all of the relevant information.

Although the doctor has the ability to detect and add the therapy, the patient must be authorized to view the data in order to protect the patient's privacy. This is necessary in order to ensure that the data is kept confidential. The provision of this method is accomplished by first utilizing an encrypted QR code to verify the existence of the physician within the system, and then subsequently granting him access to the data. Twilio's One-Time Password (OTP) will be utilized in the event that the phone is either not connected to the network or is not an intelligent smart device. In order to illustrate this point, the following Flow diagram (8) and (9) will be used.

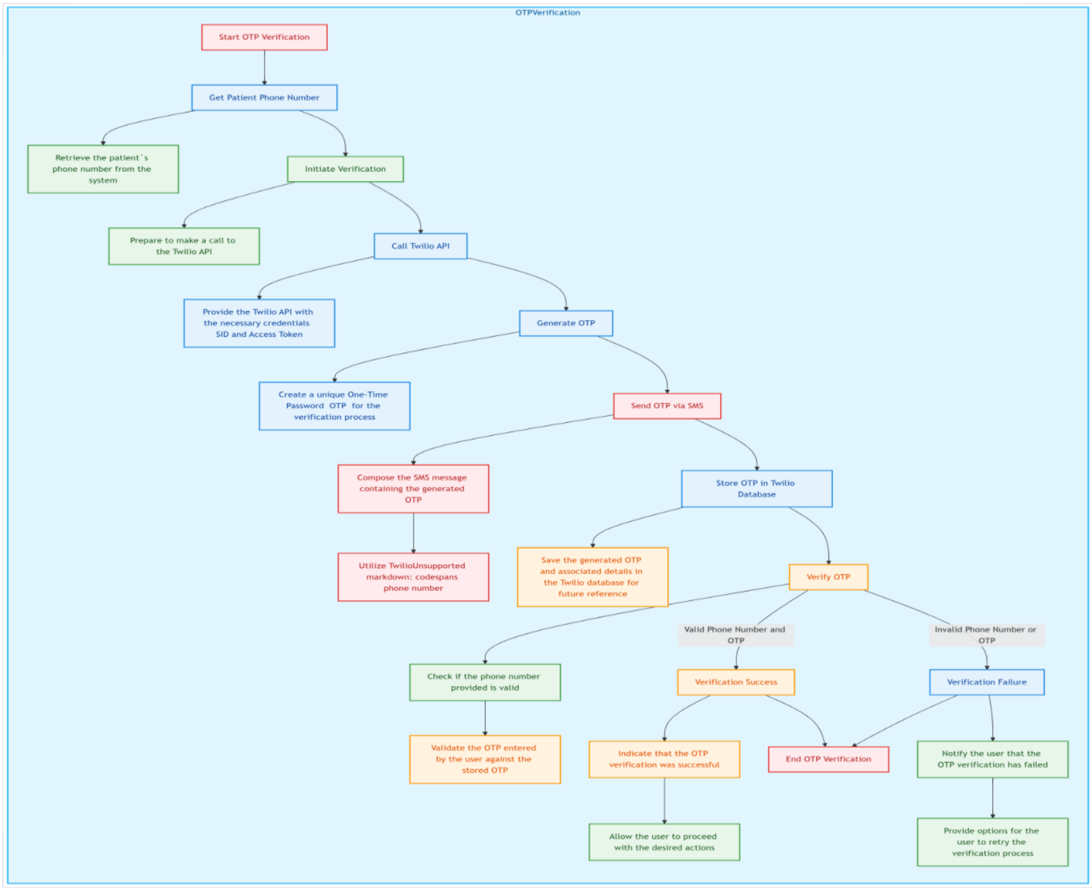

Fig. 8. one time password

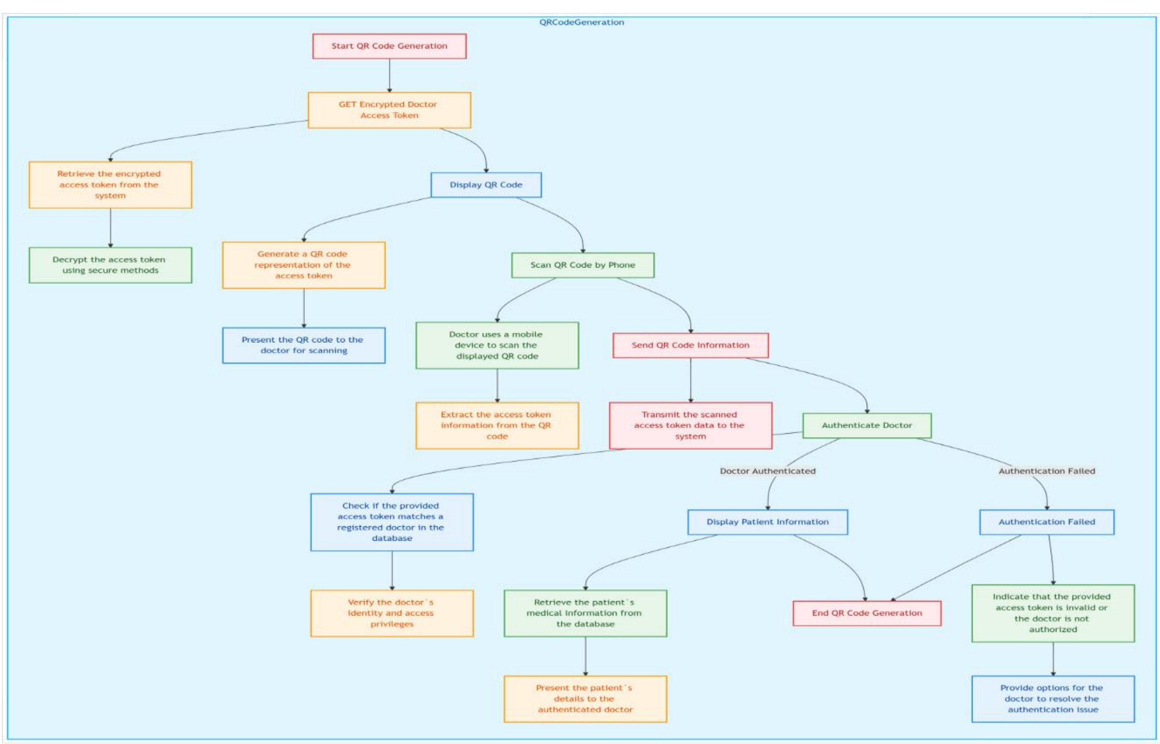

Fig.9. Quick Response

- **Front-layer design**

As stated in the second chapter, the first component, the "Raspberry Pi 4," is in charge of sending data via the medical sensors that are linked inside of it. The next paragraph will cover the specifics of the data transfer where it transmits data to databases as a last step. Regarding the second component of the front layer, which is mobile and web, as stated in the previous paragraph, only the user has access to his or her readings and the doctor's authorization on mobile devices.

- **Back-end layer**

There are three steps of processing that take place within the backend layer. The first stage begins with the authorization of all individuals who are authorized to enter the system by depending on a token that is produced by the system. The second stage is focused with dealing with the process, which involves validation and verification, and it is at this level that the data is ready to be analyzed and visualized.
The final component encrypts the data before storing it using the algorithm that was proposed (the first development of the research).

- **Exparmental Result**

Beginning with the system interface that the administrator uses and progressing all the way down to the patient interfaces, this section will provide an explanation of the interfaces that may be accessed through the medical platform, as well as instructions on how to deal with these interfaces.

The most significant front-end solution designed for the doctor is the customizable and typically managed dashboard with full control and monitoring of the IoT-based COVID-19 detection system. This single window puts together all the vital data and calls through which necessary patient tracking and disease control occur.

The dashboard is workful and has a perfect organization of the materials; the sections are divided perfectly, plus there is no confusion in directing oneself around here. From a bird's eye perspective, the doctor acquires instantaneous information on the patients' status through connected IoT devices, the symptoms, results and more. Sophisticated query tools, like impulse and non-impulse world/graphic charting systems, help the doctor to spot trends and variations early and obtain a head start on intervention.

The interface also allows for linkage to the hospital's electronic health record system, where the docotor can directly view full patient history and medical records all at the dashboard of the interface. Its integration makes it possible to obtain a comprehensive view of each patient's state and make the right decisions.

Multi-media communication and collaboration capabilities are front-end-enabled as the doctor can safely share patient info, discuss cases, and organize patient care with other care givers. Computer directed alarms and notification systems guarantee the timely notification of the doctor especially on difficult emergent or developing circumstances.
In general, the main interface is a powerful tool to control the situation, the distribution of the load between hospitals, and make decisions to increase the effectiveness of the treatment of COVID-19 cases, as well as protect the health of doctors and the population, and improve the efficiency of the healthcare system.

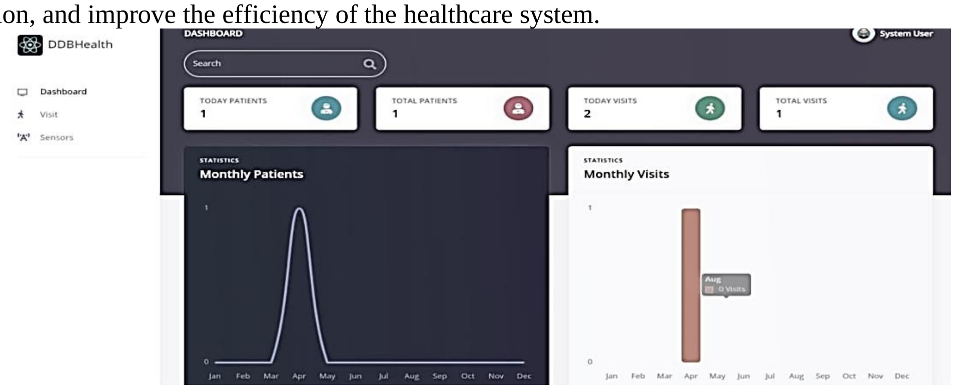

Fig. 10. Display of the Doctor's Dashboard

B. The Patient’s Interface for the IoT based COVID-19 detection system is an easy and efficient means for the doctor to save and get information from/to the patient irrespective of the internet connectivity and the capabilities of the device used by the patient.
For patients with internet-connected and smart devices:
Through the patent interface, there is an option of QR code for identifying the patient and for sharing information. Whenever the doctor requires data from the patient, the screen generates a one-time Use of QR codes Patients can provide information to the doctor using the interface by scanning a unique QR code displayed on the screen. This way, the patient can merely aim the smartphone’s camera at this QR code and securely link the patient’s device to the system so that the doctor should be able to view the necessary information, including temperature, symptoms, and tests. Using a QR code eliminates high risk, time consuming data entry and user friendly, allows for easy set up & secures the patient’s privacy.
For patients without internet connectivity or smart devices:
Caring for the fact that the patients may not have access to internet connected or possibly an advanced device, the patient interface allows for one time password authentication. ‘’In this scenario when the doctor require information entry from the patient the interface will show an OTP that the patient can relay to the doctor via phone call etc.” Once the OTP has been generated, the doctor can input that OTP into the system and the patient can be safely authenticated while the doctor can access patient files that are relevant for the particular service.
Since the patients will need to authenticate their account on the IoT-based COVID-19 detection system, this work adopts two authentication methods, namely QR code and OTP, to accommodate the patients with different technological literacy levels and number of internet-connected devices. With this flexibility, it becomes possible to accommodate all patients into the remote monitoring and data sharing process and make the system as effective as it is in meeting the aims of the healthcare solution. Figure (11) shows the patient's interface after.

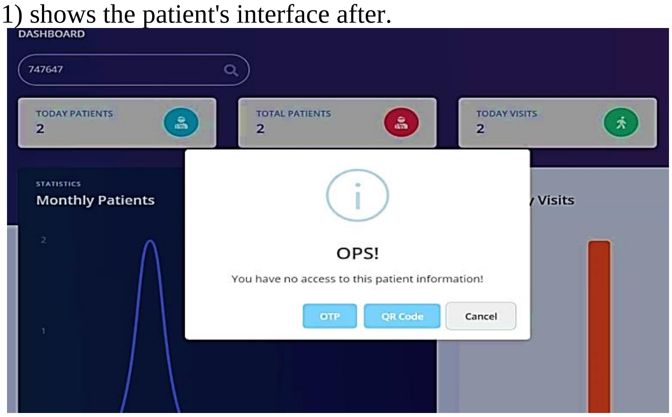

Fig.11. Authentication of the Patients

C. Recording a patient's visit by a doctor, including the patient's examination and medications, through a specific interface. Here are some points that may help clarify the idea:
Steps to record a patient's visit
Record basic information:
Patient's name
Date of visit
Patient's age
Recording a clinical examination:
Notes on symptoms
Results of a clinical examination (such as blood pressure, pulse, etc.)
Initial diagnosis
Recording medications:
Names of prescribed medications
Doses
Duration of treatment
Special instructions (such as appropriate times to take the medication)
Recording additional notes:
Any advice or instructions to the patient shown in the figure below (11).

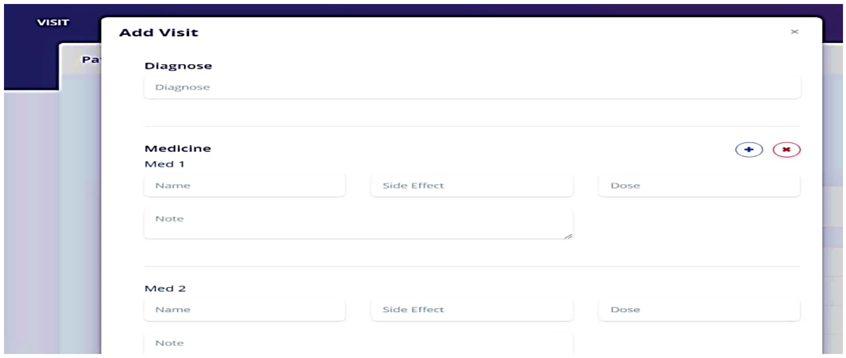

Fig.12. Adding a New Visit

d. A form that allows the patient to fill in certain details on their visit as shown in figure (12).

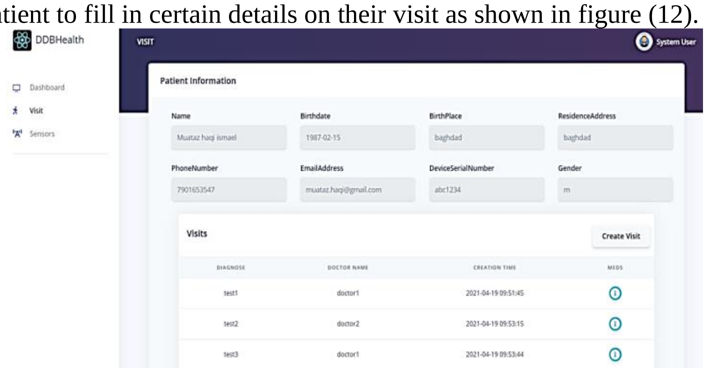

Fig.13. The text suggests retrying all previous visits.

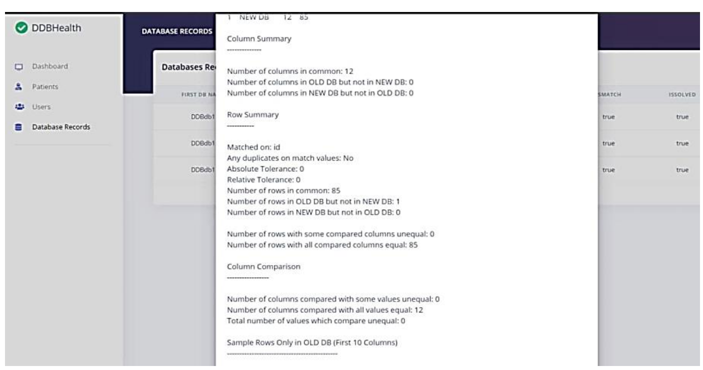

Fig. 14. Log File Showing Data Comparison With Each Database

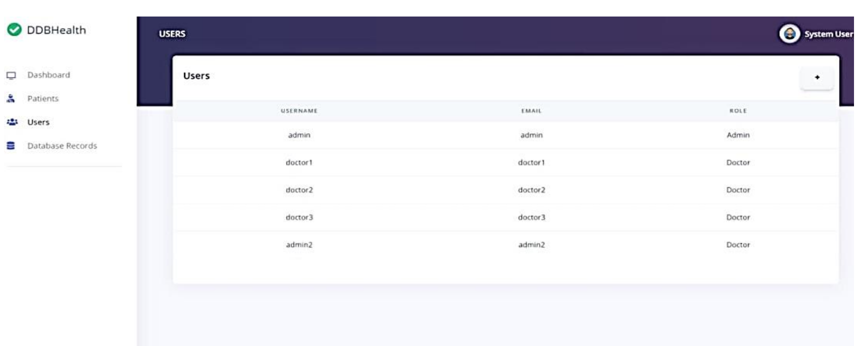

Fig.15.panel to add user (admin or doctor)

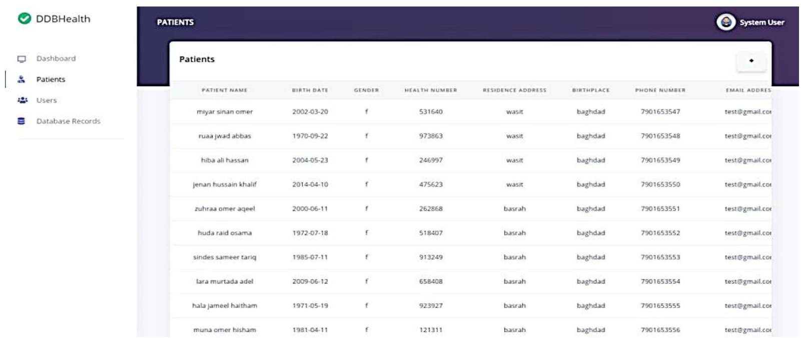

Fig.16.patient user panel

5.CONCLUSION

As a result of Predictable Virus Detection epidemic around the world, many countries faced problems like the scarcity of health facilities and problems related to treatment of patients. This situation clearly called for a solution to be devised. As a result, a medical system on the basis of the Internet of Things (IoT) appeared.

This system incorporates various devices that make one to check on their health status with aspects such as temperature, pulse rate and blood pressure. If any of these readings are out of range, the data goes to the physicians like doctors for uninterrupted follow-up of the patient’s condition. For security purposes, the system comes with the QR code features, thus patient info is secure.

Also, if prescriptions’ management is digitized and the application of limits is introduced by QR codes, the above-mentioned goal to eliminate deception and unsafe actions, particularly the unlawful use of prescriptions, is to be achieved. Those who use the Android app can also get information on the available medication types via this platform.

In general, this kind of innovative system characterizes a social revolution of prescriptions, departing from another approach and improving effectiveness and safety of health care.

Funding

No institutional affiliations or sponsorship agreements are mentioned in the paper, indicating a lack of external funding.

Conflicts Of Interest

The author's affiliations, financial relationships, or personal interests do not present any conflicts in the research.

Acknowledgment

The author acknowledges the institution for the intellectual resources and academic guidance that significantly enriched this research.

References

[1] A. Shukla et al., "Air pollution associated epigenetic modifications," Science of the Total Environment, vol. 656, pp. 760-777, 2019.
[2] W. Zhang et al., "The relationship between particulate matter and lung function," Environmental Pollution, p. 119735, 2022.
[3] S. E. Bibri and J. Krogstie, "Smart sustainable cities of the future," Sustainable Cities and Society, vol. 31, pp. 183-212, 2017.
[4] B. N. Silva et al., "Towards sustainable smart cities," Sustainable Cities and Society, vol. 38, pp. 697-713, 2018.
[5] W. A. Jabbar et al., "LoRaWAN-based IoT system implementation," Internet of Things, vol. 19, p. 100540, 2022.
[6] N. Pacheco Rocha et al., "Systematic literature review of context-awareness applications," SN Applied Sciences, vol. 4, no. 4, p. 90, 2022.
[7] S. Mahajan, "Internet of environmental things: A human-centered approach," in Proceedings of Mobisys Ph.D. Forum, pp. 11-12, 2018.
[8] J. Stübinger and L. Schneider, "Understanding smart city—A data-driven literature review," Sustainability, vol. 12, no. 20, p. 8460, 2020.
[9] S. Polymeni et al., "IoT-based prediction models in the environmental context," Internet of Things, p. 100612, 2022.
[10] A. B. Siddique et al., "Intelligent and secure air quality monitoring system," IETE Journal of Research, pp. 1-14, 2022.