Measurement: Sensors 24 (2022) 100499

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Design and implementation of Internet of Medical Things (IoMT) using artificial intelligent for mobile-healthcare

Ahmad Abdullah Aljabr [*], Kailash Kumar

College of Computing and Informatics, Saudi Electronic University, Riyadh, 11673, Saudi Arabia

ARTICLE INFO

Keywords:
m-Health
Internet of things
Internet of medical things
Chronic disease management
Wireless network

ABSTRACT

The newest phase of the Internet of Things is the Internet of Medical Things (IoMT), which has applications for smart healthcare systems. In a pandemic, healthcare workers face many issues while treating patients. IoMT equipment keeps tabs on the patient's wellbeing. The initial safety measures can be implemented individually based on the outcome. The healthcare sector is heavily relying on it to boost the precision, dependability, and effectiveness of electronic instruments. IoMT can link actual, physical objects in the physical environment for communication and information exchange. It also guarantees the standard of service. To diagnose, simple communication protocols are utilized to track biological signals. The IoMT will assist doctors, nurses, public health officials, and patients in monitoring, identifying, educating, and directing them to receive the proper medical care as well as ensuring the quick and accurate dissemination of data in a controlled situation.

1. Introduction

A subset of Internet of Things (IoT) technology known as the Internet of Medical Things (IoMT) comprises medical equipment interconnected through networks to monitor patient health. IoMT devices, also known as healthcare IoT, integrate automation, interlayer sensors, and artificial intelligence based on machine learning to provide healthcare monitoring without human involvement. Through the use of medical devices, IoMT technology links patients and physicians, enabling remote access for the collection, processing, and transmission of medical data across a secured network. IoMT technologies enable wireless surveillance of health parameters, which reduces unneeded hospital stays and, consequently, the related health expenses. The point-of-care (POC) devices used in hospitals or clinical settings as well as wearable and in-home real-time health monitoring devices are all included in the IoMT medical technology segment. IoMT wearable's can keep an eye on elderly people's unintentional falls. Although older people may inevitably fall, their environment can be watched and accidents can be avoided to prevent chronic injury. Conventional medical monitoring is changing dramatically, and digital healthcare puts online storage goods and automated detection technologies in the hands of consumers. With the help of this digital change, patients, doctors, and residents of rural areas may now easily access high-quality healthcare services. POC equipment that include Internet access and cloud storage capabilities, such as ultrasonography, thermometers, glucose meters, and ECG readers, enable users to monitor their health. The advancements in these technology are essential for improvised healthcare since they allow for the adjustment of insulin dosages and direct patient-clinician communication. Modern healthcare facilities have begun implementing the "smart bed" idea, which could adjust the bed's positioning and angle based on the patient's resting position. Conventional home healthcare solutions are being transformed by IoMT-enabled devices. A people's clinical history is automatically uploaded to the cloud via the intelligent dispensing system, for instance. It notifies clinicians when a patient also isn't taking medication, as well as doctors and patients, about the necessary medication to be taken. Demands on the healthcare system are rising as a result of technological development, industrial adaption, and urbanization. The focus of this paper is on how the development of IoMT-integrated devices with cellphones, sensors, as well as actuators can enable regular healthcare monitoring.

2. Literature review

Over the next ten years, IoT and health technologies may completely transform the healthcare sector, profoundly affecting the healthcare system. The recent research on digital health systems that leverage IoT, cloud computing, and big data technologies that are intended to seamlessly connect patients and clinicians across various healthcare systems

[*] Corresponding author.
E-mail addresses: a.aljabr@seu.edu.sa (A.A. Aljabr), k.kumar@seu.edu.sa (K. Kumar).

https://doi.org/10.1016/j.measen.2022.100499
Received 27 August 2022; Received in revised form 18 September 2022; Accepted 21 September 2022
Available online 2 October 2022

is presented in the current section. The ability of medical care providers to provide patients with evidence-based therapies and repeat treatments will rise with the ease with which patients' medical information may be accessed through simultaneous announcement and checking via connected devices. The IoT now mostly consists of sensors, diagnostic imaging equipment, and the majority of medical devices. The practical and competent usage of these devices is still constrained by issues with data volume and performance, device diversity and interoperability, hacking and illegal use, and acceptance and adoption hurdles [1]. In essence, the IoT ensures the optimum use of resources while providing the greatest number of patients, allowing for efficient scheduling of scarce resources. The clinical workforce can use this variety of precise health information to support decisions that reduce clinical errors. The primary security concerns, issues, and drawbacks of IoMT were outlined and examined in this study, which also underlined the necessity of a strong security plan for the several wireless communication protocols employed by the IoMT system to maintain it safe, private, dependable, and accurate [2]. In essence, the IoT ensures the optimum use of resources while providing the greatest number of patients, allowing for efficient scheduling of scarce resources. The clinical staff can use this variety of precise wellness data to inform decisions that reduce healthcare errors. The viability of implementing smart city healthcare the practical analysis's major objective was to propose novel and engaging ideas. The applications that were thought to be the most appropriate for deployment were active aging, population monitoring, healthy lifestyles, socialization, care service organization, and emergency response [3]. By swiftly sharing vital information, this data can be utilized to reduce interaction with the sick person. IoT makes its biggest contribution to the pandemic response through efficient data management, superior care, and enhanced diagnostics. The use of intelligent ventilators, masks, and hospital instruments that can self-monitor patients can also be reduced thanks to the Internet of Things. The fall anomaly is the most common, being listed in five primary research. The smart shirt-based anomaly detection system can recognize six different abnormalities, including cardiac arrhythmia, posture, violent attack, vital signs, and ellipsis. The results indicate that IoT technology has assisted healthcare professionals in monitoring and diagnosing various health issues, measuring many health parameters, and providing develop precise at remote locations. Healthcare IoT has enhanced patient safety, reduced medical costs, enhanced accessibility of health care, and increased operational effectiveness in the healthcare industry [4]. IoT AI applications give businesses the ability to reduce unscheduled downtime, create new services or goods, boost operational efficiency, and improve risk management [5].The study focuses on the use of AI in IoT and healthcare systems, including the application of AI approaches across a wide range of healthcare specialties. This research article demonstrates the key applications of AI approach in the fields of medicine, robotic surgery, and tailored treatment [6].

3. Proposed Methodology

The World Health Organization issues various guidelines in the event of a pandemic outbreak. One of the main guide lines is that 6 feet of social distancing is to be maintained. The usage of a passive infrared sensor (PIR) sensor allows for the identification of nearby targets (6 feet). PIR sensors are electronic devices that detect the infrared (IR) light that objects in their range of view emit. Most frequently, they are utilized in PIR-based motion sensors. PIR sensors are frequently utilized in autonomous lighting and security alarm systems. The Arduino Uno board's PIR sensor, which is installed, detects the breach of social distance. By acting as a digital ring, this technology lowers the risk of infection and the spread of disease. Fig. 1 shows the wearable future interface of the devices.

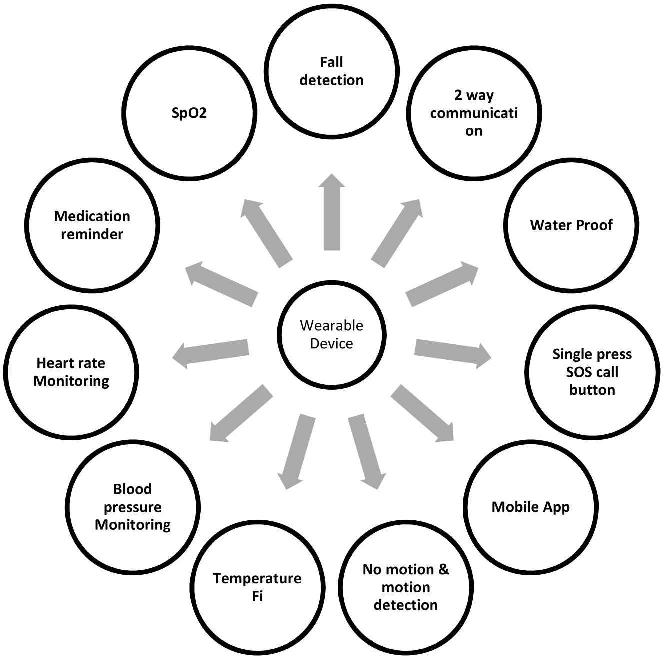


Fig. 1. Wearable future.

3.1. *Internet of Medical Things (IoMT) for remote monitoring*

For patients who are elderly or disabled, remote patient monitoring is crucial. A wearable gadget measures SpO2 levels, heart rate, blood pressure, and body temperature. It is a two-way, waterproof communication tool. Falls may be detected. There are built-in Global Positioning Systems, making it simple to determine the location. Healthcare service providers can better understand the issue thanks to the two-way communication service. There is only one SOS call button available in case of an emergency. A normal level of oxygen is regarded as 95% or above. 90% of patients who suffer from pulmonary disease or sleep apnea may well have normal levels. The percentage of oxygen in the blood is shown by the "SpO2" measurement on a pulse oximeter. A patient should seek medical assistance if their SpO2 measurement is less than 95%. The alarm clock and medicine reminder on this device are integrated. It is easy to find both motion detection and no motion in the neighbourhood and direction of the innovation. These devices are able to pinpoint the patient's location with astounding accuracy thanks to GPS technology. The patient's supporters can view the patient's precise location by just pulling out the map on the smart phone app. Fig. 2 is shown below to demonstrate the connectivity of various sensors.

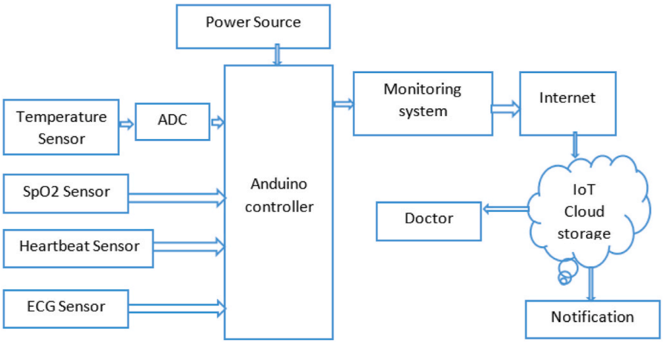


Fig. 2. Sensors connectivity.

3.2. Smartphone-based (GPS tracking) methods for infection detection

The current pandemic condition is indicative of an increase in the occurrence of infectious diseases brought on by microorganisms on a worldwide scale. The total wellbeing of the people and, perhaps, the economy are in danger due to the rapid spread of such diseases in a very short amount of time. A significant obstacle to providing quality medical care is the inadequacy of standard diagnostic tools for labour-intensive and sophisticated laboratory-based diagnosis procedures. The advancement of point-of-care testing (POCT) is required in the modern day for quick diagnosis of infectious diseases as well as "on-site" results that are beneficial in prompt and early action for improved treatment. The value of AI in enhancing the performance of point-of-care (POC) and IoMT devices used in cutting-edge healthcare fields like heart monitoring, cancer diagnosis, and diabetes control is well known [7].

Additionally, POCT devices help to stop the spread of infectious illnesses by providing lab-quality microbiological identification in just a few minutes and real-time testing. The control of infectious illness epidemics is facilitated by prompt diagnosis and improved ongoing treatment. In the area of a IoMT, technical advancement is currently being used to facilitate such POCT. With the help of the IoMT, POCT devices can operate wirelessly and be connected to healthcare professionals and hospitals. With a focus on newly emerging and re-emerging infectious diseases such as malaria, dengue fever, influenza A (H1N1), human papilloma virus (HPV), Ebola virus disease (EVD), Zika virus (ZIKV), and coronavirus, the recently developed POC diagnostics are integrated. The gap among bioinformatics generation, huge fast analysis, and clinical validation can be filled by IoMT-assisted POCT systems. In order to evaluate the development of the disease, make treatment decisions, and assess the effectiveness of recommended therapy, an optimised IoMT-assisted POCT would be helpful. The point of care testing is described in Fig. 3.

3.3. IoT-enabled thermal screening for avoiding the potential spread

IoT Smart Desirable to develop provide thermal imaging solutions, which are automated screening devices that can swiftly and correctly determine an individual's body temperature in high-traffic areas. To fulfill the entry-point requirements of any business, these solutions—flexible sufficient to be installed to one or several of locations—can be simply attached to an entry wall or cart. Automatic screening devices scan onlookers by turning their infrared emissions into a video sequence. An alert with a real-time view of a position of the detection is sent to the necessary parties when an increased body temperatures above a predetermined threshold is discovered. A typical body temperature screening system is shown in Fig. 4.

Connecting the sensors to the microcontroller was the initial step in developing the body temperature system. The Node MCU board has one analog pin and 16 general-purpose input-output (GPIO) digital pins for connecting additional peripherals like sensors and actuators. It is powered by micro-USB. Among the serial communication protocols that the board supports are Inter-integrated circuit (I2C), Serial Peripheral Interface (SPI), and Universal Asynchronous Reception & Transmitting (UART).

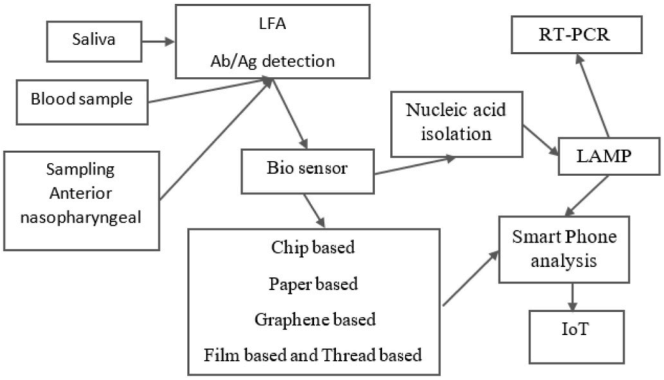


Fig. 3. Point of care testing.

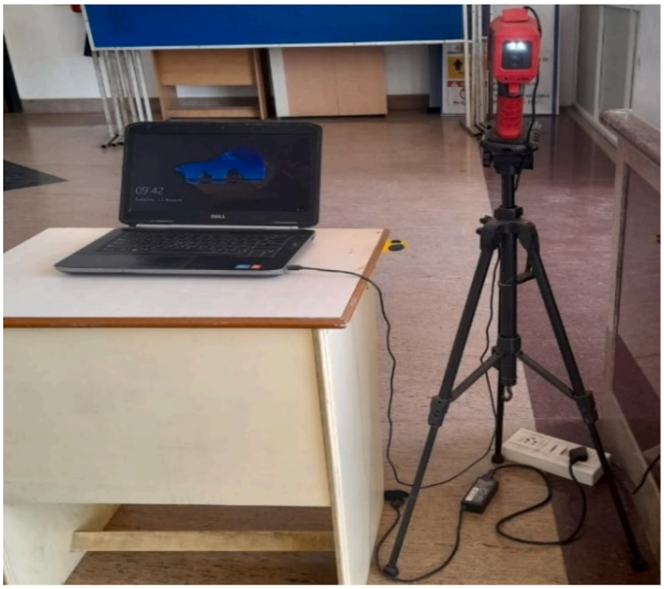


Fig. 4. The body temperature screening system.

The TRIGGER and ECHO pins of the digital ultrasonic sensor HC-SR04 are linked to wires D5 and D6, respectively, in a simple manner. Based on Fig. 3, the I2C protocol, a straightforward, bidirectional synchronous serial bus, is used by the MLX90614 non-contact temperature probe and the OLED display to connect with the microcontroller. I2C uses just two wires to transport data between connected devices: a serial clock line (SCL) for synchronizing transmission and a serial data line (SDA) for sending and receiving bits of data. To open the slave device and start the data bus transmission, the master device generates a clock. The master and slave devices on the bus that send and receive data have varying relationships with one another depending on the current direction of data flow. The MLX90614 sensor serves as the master in this scenario, sending temperature data to the microcontroller and OLED display for additional processing. Pins D1 and D2 are connected to the SCL and SDA ports on both of these components. When a slave wants to connect with another, the master gives that slave a 10-bit location and a read/write bit, which the receiving slave then compares to its own. If the addresses do not match, the slave leaves the SDA line high. If the address matches, the slave returns an acknowledgement (ACK) bit, that changes the SDA line too short for one bit. The master then sends or receives the data frame master. After every data frame has been delivered, the receiving device sends an ACK bit to the transmitter to confirm a successful transmission. In order to terminate the data transmission, the master switches the SDA to a high value before shifting the SCL to high. Last but not least, pin D7 is connected to the buzzer's signal pin. As soon as the active buzzer receives a DC voltage, it will begin to buzz. There can only be a continuous or pulsed audio signal produced because the frequency is fixed. The process of creating an unique robust enclosure to shield the delicate electronic components from of the elements, whether inside or outside, began once all components had been interfaced to the system. The components' measurements were measured, and CAD software called CREO Parametric was used to make.

3.4. Secure handling of the medical data by using encryption algorithms

Encoding data using a keys and a cryptographic algorithm is data encryption. Only those with the proper key to decipher it can read the cipher text that is produced. Both at storage and in movement, data can be encrypted. All information kept on a user's device or in your backend is considered data at rest. Due to the high attack susceptibility of this data, it must be protected using appropriate encryption. The physical disk device is encrypted when using disk-level encryption. This prevents access to your data in the event that the drive is stolen. However, the data is available when the server is active. Database-level encryption involves encrypting the entire database with a single key. Cloud service providers typically offer this. The problem is that all data is vulnerable if only one key is lost. Often regularly see people keeping the key in a plain text configuration file under the admin account.

Application- or record-level encryption entails individually encrypting each database record. In essence, each instance of the application has a key that can be used to encryption the user's own data.

The most secure option, though it does require key management, is when users need to see or process information on the backend. All data contained within the application is encrypted as part of E2e (end-to-end) encryption. The data is completely inaccessible to the backend. Even though it's really safe, one may only use this if you don't need to process the data on the backend.

The optimal strategy is to employ record-level encryption if all users want to do is save the health data in a secure manner. There are a few things to know, though. Implementing record-level encryption is challenging. To manage who has control over the keys, a strong login as well as permissions system is needed. In the database, the data is encrypted. This means that users can't look for it directly. The effects of this on the design of their application must be taken into account. These kind of encrypted databases are never as quick to respond as unencrypted databases. This is something users must keep in mind while user create their application. Ideally, you should keep user information and data records in distinct systems. This provides an extra degree of security. One can also do this to lessen the quantity of data that needs to be encrypted.

Encryption one of each system's most delicate components, from which privacy and security of information depend, is the data encryption process. In this approach, classified information is transmitted as encryption from the database through client apps and is kept in encrypted form. Since the key is the weakest component of each encryption technique, the encryption method using a non-stored key (master key) offers the additional level of protection for classified information systems. Once more, the safety of another key must be considered when storing the keys. Due to this, we have designed a key management procedure that can only be managed by the established system, preventing both external and internal parties from decrypting data.

Encryption Algorithm.

Step 1: Generation of plain text bytes.

Step 2: Compression of plain text bytes.

Step 3: Generation of salt (random bytes) (IV).

Step 4: Concatenation of salt bytes with compressed bytes (IV || compressed plaintext).

Step 5: Generation of record key.

Step 6: Calculation of master key ($R_{key} \oplus C_{key}$).

Step 7: Encryption of concatenated bytes using AES algorithm with master key.

Step 8: Conversion of encrypted bytes to ASCII string format using Base64 encoding.

Step 9: Storing cipher text result in database as ASCII string.

Decryption Only the client program offers the data decryption function, and the master key is created using the client and record keys. The phases of the encryption method are carried out backwards during the decryption procedure.

Decryption Algorithm.

Step 1: Removing salt from record key.

Step 2: Calculating master key ($R_{key} \oplus C_{key}$).

Step 3: Get concatenated bytes from cipher text (ASCII format string).

Step 4: Decryption of concatenated bytes (IV || compressed plaintext) with master key.

Step 5: Removing salt (random bytes) (IV) from compressed bytes.

Organizations frequently need to be able to transfer health information between reliable parties. In this case, having robust authorization, accounting, and authentication controls is crucial. It is employed to manage who has access to the data, what they are permitted to do with it, and to maintain a log of all data accesses and changes. Frequently, just simply need to give the actual health data and not the associated personal information. When the system employs AI to analyze scans and patient observation data, this is typically what happens. When determining which data to encrypt, this is one of the factors that should take into account.

Even when the data is as delicate as medical records, big data still makes headlines. For instance, by analysing and comprehending common patient profiles, pharmaceutical businesses stand to gain significantly. Data anonymization has a role in this. The difficulty in anonymizing health information is a challenge. The remaining data is frequently useless for conducting any meaningful analysis.

4. Result and discussion

4.1. *Secured login page*

The health professional or guardian enters their login information on this screen. The system will display a list of the patients who have been allocated to the specialist when the credentials have been validated. The patient who has to be screened will be chosen by the specialist. Here, the expert or caregiver may basically watch the key readings that the patient's monitoring gadgets have reported. Here, the specialist takes great precautions to preserve sensitive information and uphold patient privacy. Fig. 5 shows the login page of the application.

4.2. *Patient's health monitoring*

Page A professional or guardian can readily view real-time patient health information, such as temperature, heartbeat, ECG, and other measurements, after successfully logging in. Sent data is encrypted while being sent to the database server and is decoded while being transferred on the site page with the ultimate goal of ensuring the security of the patient's information in mind. Fig. 6 shown below describe the web interface of the application.

Providers can gain knowledge from the patient's current readings in picture subheadings if communications with the devices are successful

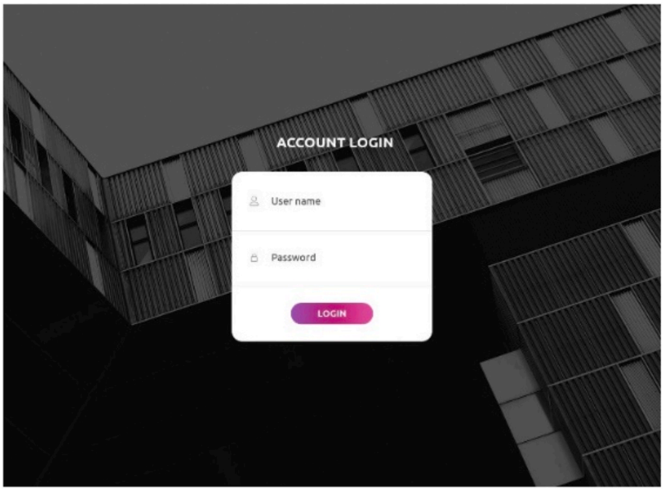
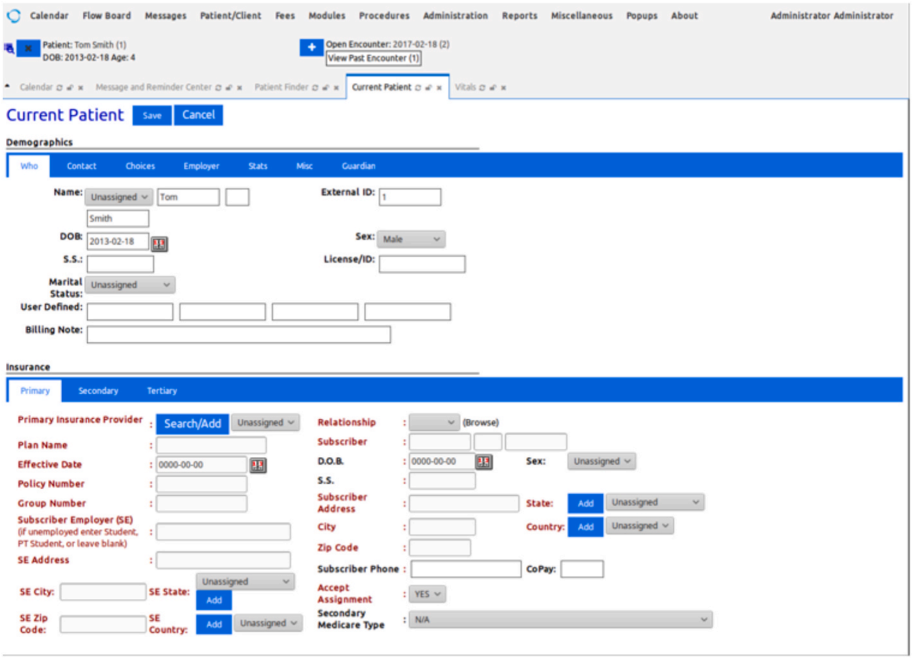


Fig. 5. Login page.



Patient: Tom Smith (1)
DOB: 2013-02-18 Age: 4

Open Encounter: 2017-02-18 (2)
View Past Encounter (1)

Current Patient

Demographics

Name: Unassigned Tom
Smith
External ID: 1
DOB: 2013-02-18
Sex: Male
S.S.:
License/ID:
Marital Status: Unassigned
User Defined:
Billing Note:

Insurance

Primary Insurance Provider : Unassigned
Plan Name :
Effective Date : 0000-00-00
Policy Number :
Group Number :
Subscriber Employer (SE) (if unemployed enter Student, PT Student, or leave blank) :
SE Address :
SE City:
SE State: Unassigned
SE Zip Code:
SE Country: Unassigned
Relationship : (Browse)
Subscriber :
D.O.B. : 0000-00-00
Sex: Unassigned
S.S. :
Subscriber Address :
State: Unassigned
City :
Country: Unassigned
Zip Code :
Subscriber Phone :
CoPay:
Accept Assignment : YES
Secondary Medicare Type : N/A

Fig. 6. Health monitoring interface.

and error-free. All readings would be recorded as zero if the device wasn't connected to the patient or if any of the sensors weren't connected to the patient, preventing an incorrect diagnosis. This page would display a gadget disconnected error in the unlikely event that a device was turned off. The data is then utilized to generate graphs and analyze health reports after being posted into the server from the various sensors.

5. Conclusion and future work

To handle pandemic conditions, an end-to-end IoMT equipped architecture has been suggested. Due to recent developments in the architecture of sensors and communications infrastructure, it has been discovered that IoMT technology promise to meet the needs of pandemic control in a variety of indoor and outdoor locations. The suggested paradigm improves patient engagement in real-time medical observation and decision-making, which aids in real-time treatment in emergency circumstances. It also promotes human connection with the IoMT system. As a result of fewer follow-up visits, the morbidity and cost burden will be reduced. In the case of a medical emergency, the response time will be sped up. Individual citizens, government, and medical professionals should all be able to handle pandemics more successfully with the aid of the suggested architecture for guaranteeing end-to-end social distance while delivering essential supplies.

CRediT authorship contribution statement

Ahmad Abdullah Aljabr: Software, Validation, Writing – review & editing. **Kailash Kumar:** Conceptualization, Methodology, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number 7989.

References

[1] D. Gupta, M.P.S. Bhatia, A. Kumar, Resolving data overload and latency issues in multivariate time-series IoMT data for mental health monitoring, IEEE Sensor. J. 21 (22) (2021) 25421–25428, https://doi.org/10.1109/JSEN.2021.3095853.

[2] R. Hireche, H. Mansouri, A.K. Pathan, Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis, 2022, pp. 640–661.

[3] M. Alshamrani, IoT and artificial intelligence implementations for remote healthcare monitoring systems: a survey, J. King Saud Univ. - Comput. Inf. Sci. 34 (8) (2021) 4687–4701, https://doi.org/10.1016/j.jksuci.2021.06.005.

[4] B. Pradhan, S. Bhattacharyya, K. Pal, IoT-based applications in healthcare devices, J. Healthc. Eng. 2021 (2021), https://doi.org/10.1155/2021/6632599.

[5] S. Mahalakshmi, R. Latha, Artificial intelligence with the internet of things on healthcare systems: a survey, Int. J. Adv. Trends Comput. Sci. Eng. 8 (6) (2019) 2847–2854, https://doi.org/10.30534/ijatcse/2019/27862019.

[6] K. Raj, AI Enabled Internet of Medical Things 9, 2021, pp. 578–602, 12.

[7] P. Manickam, et al., Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare, 2022.