IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

An Secure Information Transmission for Medical Services Applications Internet-Of-Medical-Thing

Subhashini K, P.Pushparani, Dr.M.Malarvizhi

ME Embedded System Technology, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.

Assistant Professor, Department of EEE, ME Embedded System Technology, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.

Professor, Department of EEE, ME Embedded System Technology, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.

ABSTRACT: Tiny sensors, embedded devices, and other "things" with sensing, processing, and communication capabilities are now feasible thanks to the current paradigm of the Internet of Things. The Internet of Things (IoT) and other connected medical technologies have allowed for remote monitoring of patients' vital signs in real time. In the event of a corona-virus pandemic, there would be a dramatic increase in the number of persons seeking medical assistance, making regular patient monitoring essential. Other non-invasive health markers include blood pressure, glucose levels, and respiration rate. Machine learning technology may prove to be an essential part of any healthcare monitoring system due to its potential to increase the rapidity and precision of medical diagnostics. In addition, other tactics can be integrated into this initiative in the event of an emergency, such as when the patient's body produces an irregular signal. Firstly, a SIM800L GSM Module will be integrated into the system, allowing for phone calls and SMS messaging to be made and received from the project to locations such as hospitals, homes, and emergency medical care hubs. NodeMCU has the ability to send urgent emails to specific addresses automatically. Second, in the case of a VF, a DC defibrillator can be worn by the patient and attached to the body in order to automatically give DC shocks (Ventricular Fibrillation). Finally, if the SPO2% falls below 90%, an automatic ventilation system can be introduced to the system to replenish oxygen levels.

KEYWORDS: Internet of Things (IoT), Health Care System, ECG monitoring system, IoT Based ECG

I. INTRODUCTION

Over the past ten years, there has been a revolution on the Internet of Things (IoT) due to developments in networking technologies and protocols. Governments and communities approved IoT applications, because they give users opportunities to have control over their peripherals and assets. The concept of IoT has been expanded to the healthcare industry with this development. To follow the state of individuals suffering from long-term diseases, new networks known as IoMT have been launched. These IoMT networks should be connected to patients and caregivers in order to facilitate routine biomedical measurement exchange and remote access to testing and diagnosis.

Because IoMT networks are susceptible to a wide range of attacks, their security is a vast area of research. During data transmission over IoMT networks, attacks could involve anything from fake users to fake nodes. Furthermore, in ways akin to SQL injection, attackers might be able to breach IoMT networks and manipulate patient data. It is obvious that such actions could endanger the patients' lives, since they will result in inaccurate diagnosis and course of treatment. Answering the query “How is the network accessed by the patients??” is the first step towards ensuring the security of IoMT networks. Patients have the option to base their IoMT network access on biometric-based authentication, according to Xin et al. For the patients to access the IoMT networks, they could use a framework that is based on the combination of facial, fingerprint, and finger vein features.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

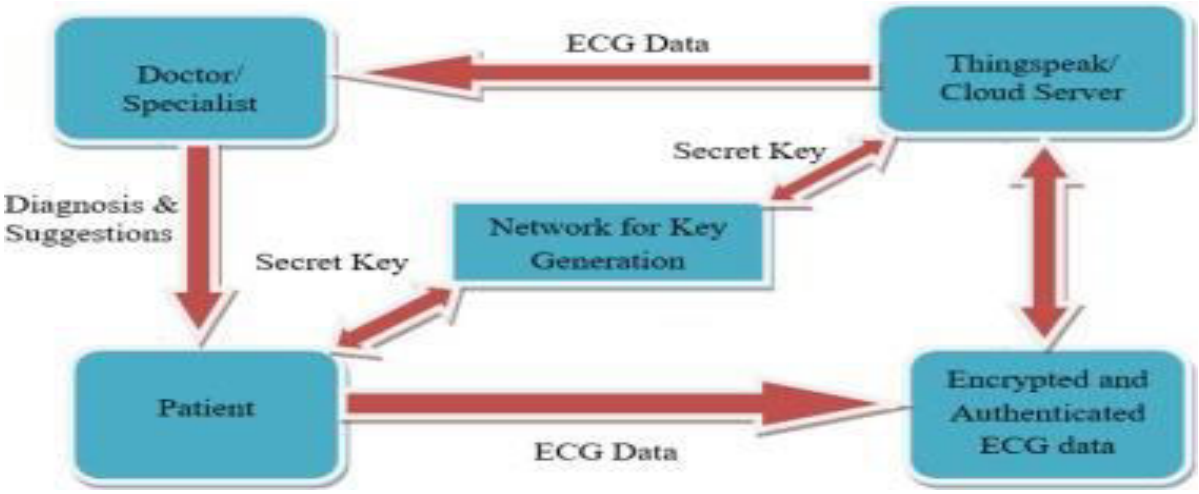

Fig 1: Block Diagram

The IoMT network primary goal is to monitor patient conditions associated with chronic diseases. Consequently, it is advised to use one of the biometrics associated with the ongoing patient measurements in the access process. The ECG is highly recommended for this task. The heart electrical activity is measured with the ECG. Through a combination of parasympathetic and sympathetic mechanisms, the ECG waveform is regulated by the autonomic nervous system. As a result, each instance is unique for each subject. Therefore, ECG signals can be utilized for authentication. With ECG signals used as biometrics, patients will not be required to provide additional biometrics for authentication, and hence the ECG signals are better suited for use in IoMT networks.

To reduce the effects of attacks, many contemporary access control system designers, particularly in the medical sector, place a strong emphasis on biometric authentication in place of passwords, credit cards, or token-based verification systems. Biometric-based authentication systems' ease of use is thought to be beneficial in many important applications. Biometric traits, like voice, electroencephalography (EEG), photoplethysmography (PPG), ECG, face, hand geometry, and ear shape, are distinct for each user, and cannot be replicated. Users can therefore use them with ease in remote access systems. ECG scanning provides the advantage of continuously enabling ECG signals for patients in the context of patient monitoring. As a result, even in situations of fatigue and lack of capacity to provide additional biometric traits, patients can simply rely on ECG signals to connect to the healthcare system. Unfortunately, one of the weakest points in the biometric system is the biometric acquisition, which makes the biometric trait vulnerable to theft and other forms of attacks. It is important to secure the primary biometrics used during the access process to stop attackers from pretending to be other users.

ECG signals adhere to the two primary prerequisites for use of human biometrics in authentication systems: universality and permanence. Given that the ECG signals of all subjects can be continuously monitored, universality is preserved. High permanence of ECG-based authentication systems is guaranteed by the signals' long-term invariance. Furthermore, with ECG signals, there is a continuous guarantee for aliveness detection. ECG signals can be used for biometric authentication over IoMT networks due to all of these features.

Regretfully, databases must hold biometric features or attributes in order for biometric-based authentication systems to operate, effectively. Attacks can occur at any point in a biometric system, from biometric acquisition to decision-making. For this reason, cancellable biometrics have become more popular. Users can use alternative biometric templates made with non-invertible transformations or encryption schemes by creating new cancellable biometric templates. The purpose of cancellable biometrics is to safeguard the original biometric information, while keeping the ability to discriminate between users.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

II. RELATED WORK

For patients, it makes sense to benefit from cancellable biometrics' recent growth in IoMT applications for access control. For patients to deal with IoMT applications, the best biometric traits are the ECG signals, which are continuously monitored. The two main tools for the development of cancellable biometric systems, namely non-invertible transforms and biometric encryption, are not adequate on their own, because they are susceptible to specific kinds of attacks. Combining them can raise the cancellable templates' level of security, as this paper reveals. Avoiding excessive complexity in the combination process is an essential requirement that must be taken into account. For this reason, lightweight encryption is used, and a signal separation algorithm is implemented as a non-invertible transform. The rationale behind the utilization of signal separation is its ability to give two low-correlation signal components from two signals having some sort of correlation. As a result, if we begin operation with an ECG signal and an auxiliary audio signal for the same person, with some sort of correlation of any level, the two resultant signals after separation will be of minimal correlation. In other words, the two resultant signals after separation can be considered as distorted signals that depend in their origin on the ECG signal used. One of these distorted signals can be used as a cancellable template for the user. The combination of lightweight encryption and blind signal separation improves security effectiveness of original cancellable templates.

After an exhaustive review of the existing cancellable biometric systems, we found that encryption-based systems are vulnerable to record multiplicity attacks, and non-invertible transform-based systems are susceptible to brute-force attacks. For brute-force attacks to be prevented, strong encryption techniques with very long keys are required. They might not be appropriate for high-speed biomedical applications. Introducing a hybrid framework for cancellable biometrics that combines a non-invertible transform and a lightweight encryption scheme is a sophisticated solution to this problem. With this approach, we can achieve high authentication accuracy, high speed of operation, and high privacy of users by cascading these two stages.

It is clear that IoMT applications are developing right now. Resilient and efficient access mechanisms are necessary for them. It is not advised to gain access to these applications using raw biometrics, since they are susceptible to hacking attempts. Thus, there is presently a dearth of research into the development of cancellable biometric recognition systems that are particularly well-suited for use in IoMT applications. In the context of IoMT, cancellable biometrics and encryption-based algorithms have not yet been thoroughly investigated, despite being extensively studied in other contexts. As a result, there is a chance that the biometric recognition technologies currently in use in IoMT applications are insufficiently secure to stop misuse and unauthorized access to personal health data. Conventional biometric systems are susceptible to breaches of security and invasions of privacy, because biometric data is kept in a central database. Consequently, a safe and private biometric recognition system is required, one that can be reliably used for authentication, while safeguarding patient data. The proposed cancellable biometric recognition framework is a good candidate to address this problem. It is based on lightweight encryption and a signal separation algorithm to induce distortion in the original ECG signals. However, more investigation is required to confirm the system performance and pinpoint its potential restrictions or disadvantages as well. The efficacy and generalizability of this system have not yet been thoroughly assessed.

III. METHODS

The sensors that will be used in this project and their connections are shown in the image above, which is a connection diagram for the proposed work. The nodemcu is wired to a temperature and humidity sensor (a DHT11) and a pulse rate sensor (an HC-SR04), while the electrocardiogram (ECG) sensor is wired to the Arduino. In this setup, the dht11's data pin was wired to the analogue input on the nodemcu board, and the pulse rate sensor's output pin was wired to the board's fourth GPIO (General purpose input output) port. Connecting an electrocardiogram (ECG) sensor to an Arduino The analogue input pin on the Arduino board is connected to the Lo- and Lo+ pins of the ECG sensor. Once the IN electrode is unplugged, dc leads off detection mode is activated and LO rises, and the condition is reversed once the IN electrode is connected again. The logic one (LO+) in the first stage of a comparator is an important output. In the The above diagram depicts the ECG algorithm for processed ECG data; this programme is uploaded into the Arduino board since our ECG sensor is directly connected to the Arduino board; after capture readings, the data is processed in the Arduino board and then transferred to the nodemcu via serial communication so that it can be updated on the thingspeak web server. Pins 10 and 11 are used as inputs, so they are set to input mode at the outset of the algorithm.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

From there, serial communication is initiated at a baud rate of 9600; if pins 10 and 11 are found to be high, a message is printed to the serial monitor; otherwise, the received reading is transferred to the nodemcu using serial communication.

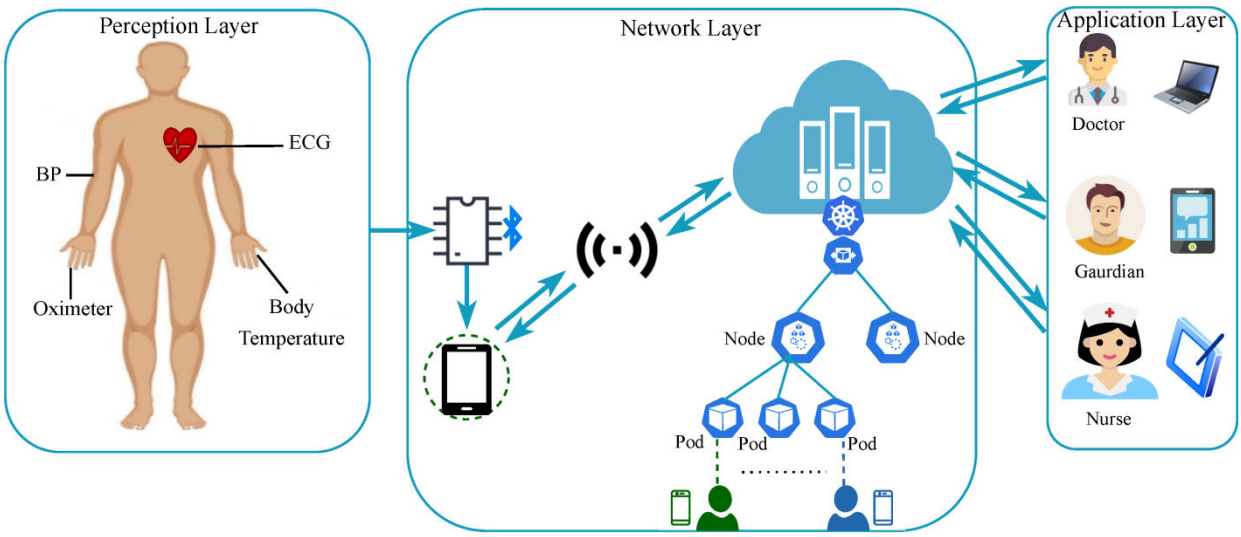

Fig 2: Work Flow

First, the algorithm is run; next, the firebase, wifi, thingspeak, dht11, and pulse sensor libraries are initialized; and last, the firebase host, key, and URL are displayed. At last, the nodemcu's saved wifi SSID and password are shown for use in establishing a secure connection between the router and the device. After initializing firebase data, the following step is to set up the API key, number, and URL for a Thingspeak channel. Once the timing has begun, we will begin taking pulse readings through the pulse wire connected to analogue pin 0 with the maximum ignore value set to 550. One the byte has been received, it is treated as a 0. Data read from the serial port is saved in this Arduino variable. After entering the required information, the nodemcu wifi will begin scanning for networks that match the SSID and password. The cycle starts over every 500 ms and continues until the nodemcu is offline. The serial print port on the nodemcu must be connected to the device's local IP address over WiFi so that firebase and thigspeak may communicate with each other. In this case, Nodemcu's analogue pin 0 will be used to read the information from the pulses. The analysis of heart rate requires the determination of beats per minute. The nodemcu's digital pin 4 is where the output from the dht11 sensor may be read for information on the current temperature and humidity levels. Then, we'll test if there's any new information by looking at the serial RX pin on the nodemcu. If so, then the nodemcu has received data from the arduino through its TX pin. Data is written to the incoming byte variable if all conditions are met. After this is complete, the nodemcu sends the processed data as a byte variable to the firebase server, which then converts the data into strings S1 through S4 according to the data type (temperature, humidity, pulse data, and electrocardiogram). The ECG data uploaded to the thingspeak server can be used to create a graph. Finally, we'll check that the graph was updated correctly by using the condition (x==1000). Serial print channel update is complete when this algorithm returns, and the loop continues until power is restored to the nodemcu.

IV. RESULT ANALYSIS

Firebase provides everything you need to build and manage a website, including hosting, authentication, storage, and more. This project makes use of a hosting service and a real-time database. Instead of managing a server and coordinating deployment and networking, you can use Firebase's hosting service. It's free (but severely limited), straightforward, and convenient. Google's Firebase is a platform for making mobile and web applications. As can be seen in the accompanying picture, once the first line of code is performed, all input/output devices are activated and a WiFi connection is made. The figure also shows the remaining processes that take place during a conversation between an Android app and the Firebase server. When online, the system connects to Firebase and reads sensor readings from there. Whenever you make a modification to a string in Firebase, like when new information is added, the corresponding strings in your mobile app will also be updated.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

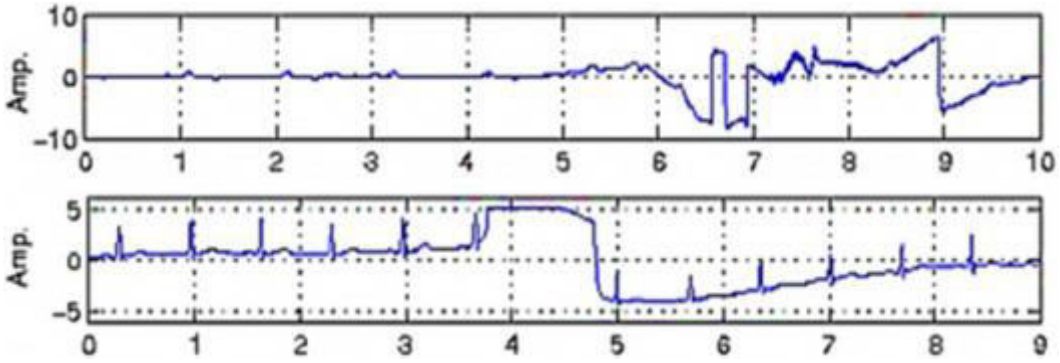

Fig 3: Result analysis

Given the recent worldwide population explosion and the increasing need for health insurance, the rising expense of providing basic medical treatment has emerged as one of the most serious challenges for both individuals and governments. However, a new report from the World Health Organization emphasises the gravity of problems caused by an ageing population. More frequent checks on the health of the elderly are needed, as they will serve as a more public test of current medical structures. Careful planning is required for the diagnosis of human diseases to be quick, accurate, and inexpensive. Detection, processing, and communication capabilities may now be built into the blueprint for sensors, embedded devices, and other "things" thanks to the expanding Internet of Things (IoT) infrastructure. An Internet of Things (IoT)-enabled electrocardiogram (ECG) monitoring system has been created so that a patient's heart health can be monitored continuously.

V. CONCLUSION

This research presented a new cancellable biometric recognition framework that utilizes unique ECG signals to secure the IoMT network access process. The methodology adopted herein combines blind signal separation with lightweight encryption. It guarantees balancing between security demands and operational efficiency. Such a balance is critical in healthcare contexts, where the immediacy of access to medical data must not compromise the integrity and confidentiality of patient information. Moreover, the practicality of our solution, characterized by its adaptability to mobile hardware, paves the way for broader adoption and integration into existing IoMT ecosystems. It underscores the potential for cancellable biometric frameworks to evolve beyond traditional security mechanisms, offering a dual advantage of enhanced security and user-centric design. This research, therefore, not only addresses current security challenges within IoMT networks but also anticipates the future needs of the new healthcare landscape. In doing so, it invites a paradigm shift in how security is conceptualized and implemented in medical technology, advocating for solutions that are both technologically advanced and deeply attuned to the human aspects of healthcare delivery.

REFERENCES

[1] Mamoona Humayun, NZ Jhanjhi, Malak Z Alamri “IoT-based Secure and Energy Efficient scheme for E-health applications” Science and Technology2020. Available From: https://doi.org/10.17485/IJST/v13i28.861

[2] S. Sheeba Rani & Jafar A. Alzubi & S. K. Lakshmanaprabu & Deepak Gupta & Ramachandran Manikandan “Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers”Springer2019. Available from: https://doi.org/10.1007/s11042-019-07760-5

[3] Ashutosh Sharma, Geetanjali Rathee, Rajiv Kumar, Hemraj Saini, Vijayakumar Varadarajan, Yunyoung Nam and Naveen Chilamkurti “A Secure, Energy- and SLA-Efficient (SESE) EHealthcare Framework for Quickest Data Transmission Using Cyber-Physical System”MDPI2019. Available from: https://doi.org/10.3390/s19092119

[4] Sarada Prasad Gochhayat, Chhagan Lal, Lokesh Sharma, D. P. Sharma, Deepak Gupta, Jose Antonio Marmolejo Saucedo, Utku Kose “Reliable and secure data transfer in IoT networks”Springer2019.Available from: https://doi.org/10.1007/s11276-019-02036-0

[5] Mohamed Elhosen, Gustavo RamírezGonzález, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed farouk “Secure Medical Data Transmission Model for IoT-based Healthcare Systems” IEEE2018.Available from: https://doi.org/10.1109/ACCESS.2018.2817615

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308071|

[6] Sohail Saif, Rajni Gupta and Suparna Biswas "Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring"Springer2018.Available from: https://doi.org/10.1007/978-981-10-8237-5_64
[7] Hai Tao, Md Zakirul Alam Bhuiyan, Ahmed N. Abdalla, Mohammad Mehedi Hassan, Jasni Mohamad Zain, and Thaier Hayajneh "Secured Data Collection with Hardware-based Ciphers for IoT-based Healthcare"IEEE2018.Available from https://doi.org/10.1109/JIOT.2018.2854714
[8] Munish Bhatia, Sandeep K. Sood "A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective" Elsevier2017.Available from: https://doi.org/10.1016/j.compind.2017.06.009
[9] "Secure Data Transmission in WSN" Springer2017. Available from: https://doi.org/10.1007/978-3-319-92807-4_6
[10] Haiping Huang, Member, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System"2017.Available from: https://doi.org/10.1109/TII.2017.2687618

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details