International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0255
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1577 - 1579

# Efficient and Secure Authentication Scheme for IoMT – Based Healthcare

*Dr.M Ananthalakshmi[1], C Banumathy[2], T Harish[3], S Kaviya4*
*[1]Associate professor, Dept. of Electronics & Communication Engineering, Meenakshi College of Engineering, KK Nagar, Chennai*
*[2,3,4]UG Scholar, Dept. of ECE, Dept. of Electronics & Communication Engineering, Meenakshi College of Engineering, KK Nagar, Chennai*
***Emails:*** *anantha.mceece@gmail.com[1], bbanumathy592@gmail.com[2], hdtm2410@gmail.com[3], kaviya2003kavi@gmail.com[4]*

## Abstract
*The Internet of Medical Things (IoMT) has gained substantial traction in modern healthcare by enabling real-time monitoring and remote access to patient health data. This paper proposes an efficient and secure authentication-based healthcare monitoring system using cost-effective IoMT components. The system integrates biomedical sensors (LM35, MAX30102, ECG) with Arduino Nano and transmits health parameters via the ESP8266 Wi-Fi module to a Firebase cloud database. A lightweight authentication scheme using Firebase's email-password login ensures controlled access to patient data. The system is designed to detect abnormal values and generate alerts automatically. Although data encryption is not implemented in the current version, the proposed design lays the groundwork for secure remote monitoring in low-resource and rural environments. The system's modularity, affordability, and real-time responsiveness make it suitable for integration into scalable healthcare frameworks.*

***Keywords:*** *IoMT, Authentication, Remote Monitoring, ESP8266, Firebase, Arduino Nano.*

## 1. Introduction

The healthcare industry is experiencing a significant shift toward smart and connected medical systems. With the rise in chronic diseases, aging populations, and demand for remote care, real-time patient monitoring is becoming increasingly critical. The Internet of Medical Things (IoMT), an extension of the Internet of Things (IoT), plays a key role in enabling remote healthcare delivery through wearable sensors and smart medical devices. Despite the advantages, security and privacy remain major concerns. Unauthorized access to health records and unencrypted data transmission could lead to misuse of sensitive information. Traditional healthcare systems often fail to address these challenges, especially in low-resource or rural settings. To overcome these limitations, this paper introduces a lightweight and secure IoMT-based patient monitoring system. The system integrates vital sensors with an Arduino Nano microcontroller and utilizes the ESP8266 Wi-Fi module for wireless data transfer. Firebase cloud is used for real-time storage and basic authentication. The design ensures continuous patient monitoring and secure access to data for authorized users, while maintaining low cost and ease of deployment [1].

## 2. Materials and Methods

### 2.1. Hardware Description

The proposed system is implemented using an Arduino Nano as the primary controller, which manages data acquisition from various biomedical sensors. The LM35 sensor is used to measure body temperature, providing an analog voltage proportional to the patient's temperature. The MAX30102 module is responsible for measuring heart rate and blood oxygen levels (SpO2). Additionally, an ECG sensor is connected to capture the electrical activity of the heart, offering insight into the patient's cardiac health. These sensors are interfaced with the Arduino Nano using its analog and digital input pins. An LCD (16x2) display is used to present the real-time readings locally. For wireless communication, an ESP8266 Wi-Fi module is connected to the Arduino via UART (TX/RX pins). It transmits the collected data to the Firebase real-

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0255
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1577 - 1579

time database over the internet. The entire system is powered using a 5V regulated power supply module that ensures stable operation across all components.

### 2.2. Software and Cloud Technologies

The system is programmed using the Arduino IDE, with code written in Embedded C. Sensor libraries are included for data acquisition and conversion. Real-time data is pushed to the Firebase cloud using the HTTP protocol through the ESP8266. Firebase is also used to manage the database and authentication. The Firebase real-time database dynamically stores temperature, pulse, oxygen levels, and ECG values, while Firebase Authentication controls access to these readings [2].

### 2.3. Authentication Scheme

To secure the data and prevent unauthorized access, a lightweight authentication mechanism is implemented using Firebase Authentication (Figure 1). Authorized users must register and log in using an email and password. This prevents public access to patient data stored in the cloud. While advanced encryption like AES is not used in this version, Firebase's secure HTTPS communication channel ensures that data transmission is encrypted by default. The authentication scheme provides a practical and scalable solution that can be easily expanded for multi-user roles, such as doctors, nurses, or caregivers.

### 2.4. Working Procedure

Upon powering the device, the Arduino Nano begins reading sensor values continuously. The temperature, pulse rate, oxygen saturation, and ECG signals are sampled and shown on the LCD [3]. Simultaneously, these values are pushed to the Firebase cloud every few seconds. Alert thresholds are defined within the code — if any value exceeds or drops below the safe range, an alert flag is raised and stored in the database. The user, after logging in through the web or mobile interface, can monitor patient vitals and receive abnormal alerts in real-time. The modular structure allows the system to run continuously with low power consumption (Table 1).

**Table 1 Threshold Values for Alerts**

| Sensor | Parameter | Normal Range | Alert Condition |
|---|---|---|---|
| LM35 | Temperature (◦C) | 36.5 –37.5 | <35 or >38 |
| MAX30102 | Heart Rate (bpm) | 60 – 100 | <50 or >120 |
| MAX30102 | SpO2 (%) | 95 – 100 | <90 |
| ECG Sensor | Heartbeat Waveform | Normal Rhythm | Flatline / Irregular Spikes |

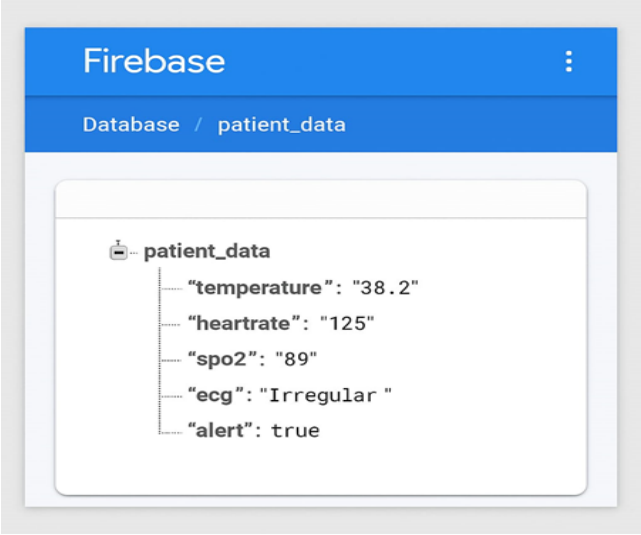


**Figure 1 Firebase**

## 3. Results and Discussion

### 3.1. Results

The system was assembled and tested under various simulated patient conditions to evaluate the performance of the sensors, data transmission, display, and alert mechanisms. The LM35 sensor provided accurate body temperature readings with a typical response time of less than two seconds. The MAX30102 sensor delivered reliable heart rate and SpO2 readings under proper finger placement and ambient conditions. ECG waveform signals from the heart were successfully captured through the ECG module, displaying consistent PQRST patterns when tested on a healthy subject. All acquired data was displayed in real-time on a 16x2 LCD screen

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0255
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1577 - 1579

connected to the Arduino Nano. Simultaneously, the ESP8266 Wi-Fi module established stable connectivity with Firebase and transmitted data without interruption or packet loss. Firebase's dashboard visibly reflected the real-time updates, confirming successful data logging. Alert thresholds were pre-defined within the Arduino code. During testing, abnormal conditions were simulated (e.g., heating the LM35 sensor or removing the finger from the MAX30102), which accurately triggered alerts. These alerts were updated in the Firebase database as flag fields, and they could be accessed instantly by an authenticated user through the web or mobile interface.

### 3.2. Discussion

The results validate the functional reliability of the proposed IoMT-based system in real-time patient health monitoring. The sensor readings were stable, and the system successfully detected deviations from normal ranges. The authentication mechanism based on Firebase email-password login prevented unauthorized data access, proving to be an effective lightweight solution for small-scale or prototype deployments. Despite its strengths, the current system has certain limitations. For instance, there is no data encryption between the ESP8266 and Firebase, which could pose privacy concerns in real-world medical applications. Additionally, the ECG waveform output is not graphically displayed to the user — it is only visible during development via the Arduino IDE's serial plotter. Nonetheless, the simplicity, affordability, and reliability of the architecture make it an ideal model for future expansion. With the addition of features like data encryption, biometric login, or integration with electronic health record (EHR) systems, the system could be scaled for use in rural clinics, home quarantine setups, or emergency response units.

## Conclusion

This paper presents a functional and efficient IoMT-based healthcare monitoring system featuring basic email-password authentication for secure data access. The system successfully captures and transmits physiological data using embedded sensors and provides real-time alerts when abnormal values are detected. While further improvements are needed to meet full-scale deployment standards, the project serves as a foundation for secure, real-time, and affordable healthcare solutions. Future work will involve integrating data encryption, two-factor authentication, and encrypted storage. Integration with AI-based diagnosis engines and hospital management systems is also planned. The system's design allows for expansion with more sensors and advanced notification systems such as SMS/email alerts.

## Acknowledgements

We express our sincere gratitude to our project guide and the faculty members of the Department of Electronics and Communication Engineering for their support throughout this project.

## References

[1]. Birari, H. P., lohar, G. V., & Joshi, S. L. (2023). Advancements in Machine Vision for Automated Inspection of Assembly Parts: A Comprehensive Review. International Research Journal on Advanced Science Hub, 5(10), 365-371. doi: 10.47392/IRJASH.2023.065.

[2]. Rajan, P., Devi, A., B, A., Dusthackeer, A., & Iyer, P. (2023). A Green perspective on the ability of nanomedicine to inhibit tuberculosis and lung cancer. International Research Journal on Advanced Science Hub, 5(11), 389-396. doi: 10.47392/IRJASH.2023.071.

[3]. Keerthivasan S P, and Saranya N. "Acute Leukemia Detection using Deep Learning Techniques." International Research Journal on Advanced Science Hub 05.10 October (2023): 372–381. 10. 47392/IRJASH.2023.066.