

IoT Based Real-Time Patient Health Monitoring System

Author: Aiman Tasneem **Programme:** BCA — Final Year Project, AI Foundation

Programme Institution: SJ Global PU & Degree College, in collaboration with Aider Digital Pvt Ltd

Abstract

Continuous patient monitoring is critical for identifying physiological deterioration early, reducing hospital readmissions, and enabling timely medical intervention. Traditional health monitoring in clinical and remote environments relies on manual periodic checks, which fail to capture rapid physiological shifts. This paper presents an IoT-Based Real-Time Patient Health Monitoring System designed as a lightweight early-warning architecture. The proposed system integrates biosensors (heart rate, SpO₂, and body temperature) interfaced with a microcontroller node to capture vital parameters continuously [4], [5]. The system is designed to process data locally for threshold breaches and stream real-time metrics to a cloud telemetry dashboard. With integrated modules — Threshold-Based Anomaly Scoring, Real-Time Automated Alerts (SMS/Email), and Emergency Protection Protocols — the system is proposed as a proactive healthcare interface for remote diagnostic assistance. **This is a design-stage paper: no hardware prototype has been built or tested yet, so no performance figures are reported as measured results — see Section 5.**

Keywords: Internet of Medical Things (IoMT), Real-Time Health Telemetry, Pulse Oximetry (MAX30102), ESP32 Microcontroller, MQTT Protocol, Cloud Telemetry Dashboard, Anomaly Detection

Table of Contents

1. Introduction & Motivation
2. Related Work — Patient Monitoring Systems and Telehealth
3. Proposed System: Design and Methodology
4. System Workflow, Logic Flow & Escalation Protocols
5. Evaluation Plan (Not Yet Executed)
6. Discussion — Technical Outcomes, Security & System Limitations
7. Conclusion and Future Scope

References

1. Introduction

Continuous health tracking has become a fundamental pillar of modern healthcare systems, driven by the need to monitor high-risk patients outside intensive care units (ICUs) and reduce overall healthcare costs [12], [14]. Traditional vital-sign recording relies on scheduled manual measurements, which frequently miss intermittent physiological anomalies such as sudden spikes in heart rate (tachycardia), acute drops in oxygen saturation (hypoxemia), or sudden febrile spikes.

1.1 Motivation — Why This Approach

Existing remote health detection and patient tracking systems encounter several structural limitations, consistent with challenges documented in the wider IoT-healthcare literature [4], [5], [12]:

- **Manual Record Bottlenecks:** Delayed data entry and periodic intermittent measurement intervals lead to missed early-warning windows during critical patient events.
- **Lack of Automated Alert Escalation:** Many standalone medical tools log data locally or onto offline SD storage without delivering actionable alerts to off-site physicians or emergency responders.
- **Infrastructure Dependency & High Cost:** Conventional hospital-grade clinical monitors are expensive, power-heavy, and lack portable telemetry options suitable for rural, home-care, or resource-constrained settings.
- **Data Fragmentation:** Standard health devices lack centralized real-time synchronization, making longitudinal physiological tracking for preventive interventions difficult.

Core Objective: To design a portable, reliable, and low-cost Internet of Medical Things (IoMT) node capable of edge sensor processing, continuous parameter monitoring, and cloud-based automated emergency escalation.

2. Related Work — Patient Monitoring Systems

Early health telemetry systems relied heavily on offline data loggers or dedicated point-of-care machinery. Recent advancements in embedded systems and wireless communication combine microcontrollers, low-power wireless networks (Wi-Fi/BLE/LoRa), and cloud telemetry engines to stream real-time patient metrics [4], [5], [6].

Table 1: Comparative Evaluation of Health Monitoring Paradigms

System Model	Core Sensors	Connectivity	Alert Mechanism	Limitation
Offline Data Loggers	Temperature, Pulse Rate	SD Card / USB	Visual LCD / Local Beeper	No remote visibility; requires physical retrieval
Standard Telehealth Portals	ECG, Blood Pressure, SpO ₂	Cellular (3G/4G)	Manual Staff Review	Delayed reaction time
Proposed IoMT Architecture	Heart Rate, SpO ₂ , Temperature	Wi-Fi (ESP32/ MQTT & HTTP)	Automated Real-Time SMS/Email + Dashboard	Requires persistent connectivity

Body sensor network (BSN) approaches to secure IoT healthcare have been specifically studied by Gope and Hwang, who proposed BSN-Care, addressing authentication and confidentiality requirements for exactly this class of system [7]. Broader IoT-aware healthcare architectures combining RFID, wireless sensor networks, and mobile technology have also been demonstrated [6]. Security and privacy of cloud-hosted health data — directly relevant to this project’s cloud telemetry dashboard — has been analyzed in depth by Rodrigues et al. [16].

3. Proposed System: Design and Methodology

The proposed framework combines a hardware sensor acquisition layer with edge signal filtering and cloud telemetry analytics to deliver real-time vital tracking and rapid anomaly detection.

3.1 Core Components

Hardware Sensing Layer: - **MAX30102 Biosensor Module:** Integrated pulse oximetry and heart-rate monitor incorporating two LEDs (Red: 660nm and Infrared: 880nm), photodetectors, and low-noise analog processing circuitry for photoplethysmography (PPG). PPG-based wearable sensing for continuous monitoring is well established in the wearable-sensor literature [8]. - **DS18B20 Digital Temperature Sensor:** High-accuracy digital thermometer using OneWire protocol, targeting $\pm 0.5^{\circ}\text{C}$ accuracy across clinical ranges (37°C – 42°C). - **Microcontroller Processing Node:** ESP32 System-on-Chip (SoC) featuring a dual-core Xtensa 32-bit LX6 processor, integrated Wi-Fi (802.11 b/g/n), Bluetooth v4.2 BR/EDR and BLE, handling analog-to-digital processing, local moving-average digital noise filtering, and telemetry streaming. - **Cloud Telemetry & Alert Unit:** Central cloud engine (Firebase / Blynk / MQTT Broker) evaluating metrics against clinical standard thresholds (e.g., $\text{SpO}_2 < 90\%$, Heart Rate > 120 BPM) and dispatching multi-channel emergency notifications.

3.2 Hardware Interface and Pin Configuration

The hardware architecture utilizes standard I2C and OneWire communication protocols for interfacing biosensors with the ESP32 microcontroller node, ensuring minimal wire count and low bus contention.

Table 2: Hardware Interface and Pin Assignments

Component	Sensor Pin	ESP32 Pin	Function
MAX30102	VCC	3.3V	Regulated Power Supply
MAX30102	GND	GND	Common Ground
MAX30102	SDA	GPIO 21	I2C Serial Data (4.7kΩ pull-up)
MAX30102	SCL	GPIO 22	I2C Serial Clock (4.7kΩ pull-up)
DS18B20	VCC	3.3V / 5V	Power Supply
DS18B20	GND	GND	Common Ground
DS18B20	DQ	GPIO 4	OneWire Digital Bus (4.7kΩ pull-up)

3.3 End-to-End System Architecture

[Sensor Layer] & Escalation]		[Processing Node]		[Telemetry Engine]		[User
MAX30102 (PPG)	→	ESP32 MCU	→	MQTT / Blynk Cloud	→	Web
Dashboard						
DS18B20 (Temp)		Noise Filter & ADC		Rule Evaluation		
Instant SMS/Email						

A full component-level breakdown is provided in the companion document, [Architecture_Paper.pdf](#).

4. System Workflow and Decision Logic

The operational pipeline is designed to execute continuous edge verification, targeting low false-positive alerts while maintaining low latency:

- Data Acquisition:** Biosensors continuously sample raw physiological signals at programmed intervals (e.g., every 2 seconds).
- Signal Filtering & Processing:** The ESP32 MCU applies a 5-sample window moving average filter to reduce ambient noise and motion artifacts.
- Anomaly Verification:** Local evaluation logic checks whether vital parameters exceed pre-set safety ranges.

4. **Cloud Telemetry & Escalation:** Telemetry packets are published via lightweight MQTT/HTTP protocols. If a threshold breach occurs, the cloud alert engine dispatches automated emergency notifications.

Decision Logic: Is $\text{SpO}_2 < 90\%$ OR $\text{BPM} > 120$ / < 50 OR $\text{Temp} > 38.0^\circ\text{C}$? → **No:** stream to dashboard for routine logging. → **Yes:** trigger emergency alert engine, dispatch SMS/Email to caregiver.

5. Evaluation Plan (Not Yet Executed)

This is a design-stage paper. **No hardware has been built or tested at the time of this draft, so no performance numbers are reported here as achieved results** — an earlier version of this paper included a results table with specific figures (heart-rate accuracy, SpO_2 deviation, and alert-trigger delays of 1.85–2.10 seconds); those numbers could not be traced to any actual test run and have been removed rather than presented as findings, consistent with the principle that a paper should never report results it cannot show were actually measured.

The evaluation plan, once a working prototype exists, is:

1. Assemble the physical hardware (MAX30102, DS18B20, ESP32) per Section 3.2.
2. Benchmark sensor readings against medical-grade reference devices (a calibrated pulse oximeter and clinical thermometer) across a defined set of test conditions (resting, post-exercise, simulated hypoxemia, simulated febrile state).
3. Record actual accuracy (heart rate and SpO_2 deviation from reference device), and actual alert-trigger latency from threshold breach to notification delivery.
4. Report the real, measured numbers — including any test runs where the system performed worse than expected — rather than only the best-case run.

6. Discussion — Technical Outcomes, Security & System Limitations

6.1 Expected Outcomes (Targets, Not Measured Results)

- **Continuous Remote Visibility:** Real-time physiological tracking on web and mobile dashboards for early clinical decision support.
- **Rapid Emergency Reaction:** Target of sub-3-second notification delivery, to be validated per the plan in Section 5.
- **Resource Efficiency:** Intended reduction in manual nursing checkup frequency for stable patients.

6.2 Security and Privacy Considerations

Medical telemetry data transmission introduces critical privacy requirements. The architecture is designed to incorporate end-to-end TLS/SSL transport encryption for all MQTT/HTTP data streams, with cloud endpoint access restricted via token-based authentication and role-based access control (RBAC) — directly informed by documented security requirements for cloud-based health record systems [16] and secure body-sensor-network healthcare designs [7], [11].

6.3 System Limitations

- **Motion Artifacts:** Photoplethysmography (PPG) sensors like the MAX30102 are sensitive to relative movement between the skin and sensor interface, which can introduce transient false readings — a well-documented limitation of PPG-based wearable sensing generally [8].
- **Network & Power Dependency:** Operational continuity relies on active Wi-Fi/cellular backhaul and steady supply power; network outages disrupt real-time cloud dispatch.
- **No validated accuracy data yet.** Per Section 5, all performance figures in this paper are design targets, not measured outcomes, until a prototype is built and tested.

7. Conclusion and Future Scope

This paper presented the design of an early-warning IoMT health monitoring architecture intended for continuous vital tracking and automatic emergency escalation. The proposed design interfaces biosensor hardware with an ESP32 node and cloud telemetry engines, aiming to reduce the delays associated with manual medical checks while keeping component costs minimal. As stated throughout, this is a pre-implementation design paper — its next milestone is building the physical prototype and executing the evaluation plan in Section 5 to produce real, reportable results.

Future Work: Future iterations may integrate embedded Machine Learning (TinyML) models directly onto the ESP32 for local predictive arrhythmia detection, and incorporate low-power, long-range LoRaWAN communication for deployment in off-grid rural communities lacking reliable Wi-Fi coverage.

References

[4] A. Pantelopoulos and N. G. Bourbakis, “A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 1, pp. 1–12, 2010.

- [5] S. Majumder, T. Mondal, and M. J. Deen, “Wearable Sensors for Remote Health Monitoring,” *Sensors*, vol. 17, no. 1, art. 130, 2017. DOI: [10.3390/s17010130](https://doi.org/10.3390/s17010130)
- [6] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, “An IoT-Aware Architecture for Smart Healthcare Systems,” *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015. (Author list corrected — the original draft listed two names, “Colella” and “Pierleoni,” who are not authors of this paper, and omitted the three real co-authors: Mainetti, Patrono, and Stefanizzi.)
- [7] P. Gope and T. Hwang, “BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network,” *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.
- [8] J. Allen, “Photoplethysmography and Its Application in Clinical Physiological Measurement,” *Physiological Measurement*, vol. 28, no. 3, pp. R1–R39, 2007. DOI: [10.1088/0967-3334/28/3/R01](https://doi.org/10.1088/0967-3334/28/3/R01)
- [11] K.-H. Yeh, “A Secure IoT-Based Healthcare System with Body Sensor Networks,” *IEEE Access*, vol. 4, pp. 10288–10299, 2016.
- [12] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, “The Internet of Things for Health Care: A Comprehensive Survey,” *IEEE Access*, vol. 3, pp. 678–708, 2015. DOI: [10.1109/ACCESS.2015.2437951](https://doi.org/10.1109/ACCESS.2015.2437951)
- [14] S. B. Baker, W. Xiang, and I. Atkinson, “Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,” *IEEE Access*, vol. 5, pp. 26521–26544, 2017. (Corrected — the original draft’s title, page range (12820–12841), and framing did not match the actual publication.)
- [16] J. J. P. C. Rodrigues, I. De la Torre, G. Fernández, and M. López-Coronado, “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Record Systems,” *Journal of Medical Internet Research*, vol. 15, no. 8, e186, 2013. (Corrected — the original draft cited this as 2018; the paper was actually published in 2013.) DOI: [10.2196/jmir.2494](https://doi.org/10.2196/jmir.2494)

Verification note: 7 references from the original 16-entry list have been removed from this version rather than carried forward with false confidence: [1] (Zhang) cited the wrong journal, wrong year, and wrong author set for a paper that — under its correct identity — is a RETRACTED publication (Wireless Communications and Mobile Computing, 2021, retracted); [2] (Khan & Chattopadhyay) could not be located in any index under the cited details; [3] (Ali et al.) cited the wrong journal and an entirely different author list than the real paper it appears to reference; [9], [10], [13], [15] could not be independently verified against any publisher record and have been removed rather than assumed correct. The 9 references retained above ([4]–[8], [11], [12], [14], [16]) were each individually confirmed

against publisher records — including [8], which in an earlier pass had been left as an unsourced placeholder note rather than a real citation; it has now been replaced with Allen’s 2007 foundational PPG review, the correct, verifiable source for the motion-artifact claim it supports.