



ORIGINAL CONTRIBUTION

IoT-Based Secure Remote Health Monitoring with Edge Signal-Quality Assessment and Intelligent Alert Logic

¹Tania Khatun, ²Sayon Dey, ³Sudiksha Dasgupta, ⁴Dr. Tirthadip Sinha

^{1,2,3}UG student, Dept. of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, Purba Medinipur, West Bengal

⁴Dept. of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, Purba Medinipur, West Bengal

ABSTRACT

Remote health monitoring often struggles with sensor noise and nuisance alarms. This paper presents a multi-layered IoT framework that evaluates data quality directly at the edge before triggering alerts or transmitting telemetry. Using an ESP32 paired with optical (MAX86141), temperature (MAX30205), and inertial (ICM-42670-P) sensors, the system evaluates channel-specific signal quality indices (SQI) to filter out motion artifacts. Rather than triggering on isolated threshold spikes, the alert engine requires persistent physiological abnormalities or verified motion sequences to flag events like falls. Structured observations—tagged with timestamps, quality states, and monotonic sequence numbers—are published securely over TLS-encrypted MQTT 5.0 to a monitoring dashboard. The architecture is validated using an eight-part engineering matrix demonstrating reliable data integrity, least-privilege security, and fault recovery.

KEYWORDS: Financial Fraud Detection, Machine Learning, Anomaly Detection, Behavioural Analysis, Real-Time Transaction Monitoring, Explainable Artificial Intelligence (XAI), Concept Drift Detection, Class Imbalance, Streaming Data Analytics.

1. INTRODUCTION

The practice of remote health monitoring systems has increasingly shifted from independent measurement devices towards sensor networks that not only monitor physiological data but also process them locally and deliver selected data to healthcare providers via networking services. This approach is appealing due to the capability of such systems for continuous monitoring in non-clinical settings.

But the engineering challenge is not only about equipping a wireless microcontroller with sensors. For instance, a practical monitoring unit should be able to differentiate between good data and bad data, maintain the order in time, operate in the event of an unreliable connection, safeguard sensitive data, and refrain from transforming transient artifacts of sensors into unnecessary alarms. One such type of sensing that is highly susceptible to various factors is wearable sensing. For this reason, the proposed architecture considers the two processes of measurement and interpretation independent from each other. The

raw or windowed sensor data is evaluated locally, a quality state specific to the channel is assigned to each piece of data, and then the decision about the existence of an abnormal situation and an alert is taken only if the abnormality lasts for some time or occurs in a certain sequence of events.

The project has also considered architecture aspects of interoperability and security. MQTT version 5.0 is used as a publish/subscribe transport protocol; JSON packets include device identifier, timestamp, measurements, quality and a growing sequence number. Transport encryption, topic-based access control, secure credentials management, and logging for auditing purposes have been taken into account. The paper therefore focuses on a complete engineering path from sensing to monitoring rather than on an isolated sensor algorithm. The contributions made include: (i) a multi-layered wearable to cloud architecture that uses both physiological and motion sensors; (ii) signal quality and alert handling at the edge side; (iii) telemetry that uses sequences over MQTT 5.0; (iv) a security architecture that uses least privilege and secure

transport; and (v) an engineering validation matrix that clearly distinguishes between prototype validation and clinical validation. This is important since a student prototype cannot be described as a clinically validated medical device.

2. DESIGN METHODOLOGY

It is common practice for connected health monitoring systems to utilize wearable sensing technologies along with low-power embedded processing, wireless communication, cloud-based storage, and applications-level visualization. There is one common problem with regard to such systems design, which is the tradeoff between streaming all measurements in the raw format or sending only validated data. The former causes increased radio usage and storage space usage, as well as leakage of private data.

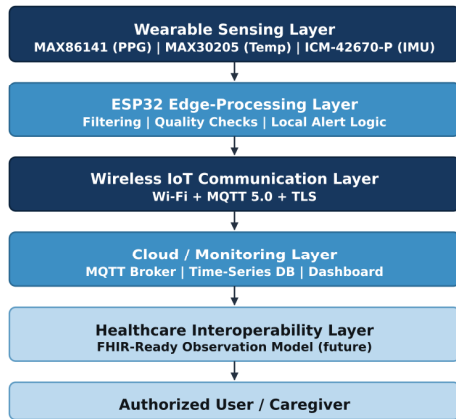


Figure 1: Proposed IoT-based health monitoring system architecture

Photo plethysmography-derived signals are highly susceptible to motion and optical contact. Temperature signals are influenced by self-heating and physical contact, whereas inertial signals might have meaningful activity information along with motion artifacts. Thus, the proposed architecture will assign different processing policies for the PPG, temperature, and motion channels separately. This is in line with the idea of representing the quality of data in accordance with the observation rather than using a single device-level indicator. MQTT is an ideal protocol for constrained IoT system because of its publish/subscribe architecture that decouples sensing nodes from consuming applications. Device-specific topics will be used in this design for critical observation, motion events, and status.

The monitoring application will subscribe to necessary streams. This helps minimize any

unnecessary exposure and allows further devices to be integrated without having to alter the application path design. In the case of systems that target the healthcare industry, there needs to be more than just security implemented on the dashboard level. Device identification, credential security, transport security, access control, logging, and updating capabilities need to be considered throughout the entire path. This is precisely what the current research accomplishes while not forgetting about its limited scope as a prototype. The architecture of the system consists of five layers: wearable sensors, edge processing, wireless IoT communications, cloud/monitoring and healthcare interoperability.

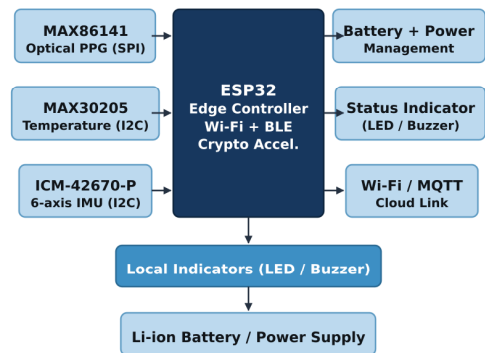


Figure 2: Wearable sensing node block diagram

The sensors layer includes MAX86141 optical sensor front-end, MAX30205 temperature sensor and ICM-42670-P inertial module. ESP32 manages the processes of sensors polling, signal processing, quality assessment, local alerts filtering, packetization and secure communication over the network. The communication layer relies on Wi-Fi communication with MQTT 5.0 protocol and TLS security. Cloud layer includes storage, dashboard visualization and alert management. The layer of healthcare interoperability is designed to be converted into standardized healthcare resources in the future.

The layering helps to bring the fast and sensitive processes as close to the sensor as possible. The cloud is not getting the waveform but the structured data from observations. This approach minimizes the wireless traffic as well as makes the monitoring process robust to the connection loss. It is necessary to keep the sequence number and the original timestamp in order to validate the observation at the destination.

3. SYSTEM DESIGN & IMPLEMENTATION

ESP32 has been chosen to act as the master controller because of its ability to integrate wireless communication (Wi-Fi and Bluetooth), as well as having several digital interfaces, encryption capabilities in hardware form, and power-saving operation. Therefore, it can carry out all the functions, including sensing, processing, creation of packets, and wireless communication, without an additional gateway computer.

MAX86141 is utilized for optically interfacing heart rate and SpO₂-related sensing. The optical channel, ADC, light cancellation, and FIFO buffering in MAX86141 are applicable for a wearable solution. The generated PPG samples are not considered clinically valid simply based on the fact that there is a numerically generated value; signal quality analysis comes along with every processing cycle. The MAX30205 sensor offers digital temperature sensing via I2C interface.

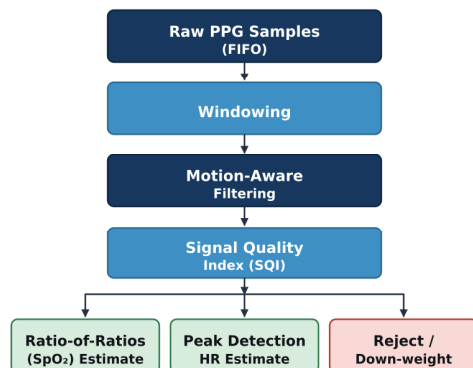


Figure 3: PPG processing and signal-quality pipeline.

This is achieved using a simple moving average algorithm that helps in smoothing out any spikes resulting from temporary disconnection or electric interference. The system is aware that physical positioning and heating could be the most significant factors behind measurement error and hence the reason for not considering datasheet accuracy. The data from the ICM-42670-P sensor comprises information on accelerometers and gyroscopes for motion detection. The suggested logic for fall detection seeks out a pattern instead of looking for one instance of high acceleration, where a high-acceleration phase is followed by a quick change in orientation, after which there is low motion. It

will be classified as a potential fall to be verified later.

The PPG signal windows have fixed length. Motion adaptive filtering is done to suppress the baseline drift and high frequency noise, and the quality metric for the signal is calculated based on some features of the waveform like periodicity and uniform amplitude.

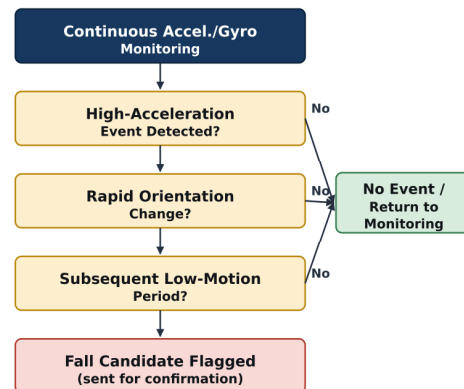


Figure 4: Fall-event screening logic; output is a candidate for confirmation.

The heart rate is calculated based on the peak detection and inter-beat interval calculation. The calculation of SpO₂ measurement adopts the traditional ratio-of-ratios approach based on AC and DC signals for two wavelengths of optical radiation. The output is considered to be an estimation since various factors such as optical coupling, blood flow, illumination, and motion may affect the output. Thus, it is impossible that the bad estimate will be compared to a good estimate. Alerting and processing of alerts have been intentionally designed to be independent of measurements.

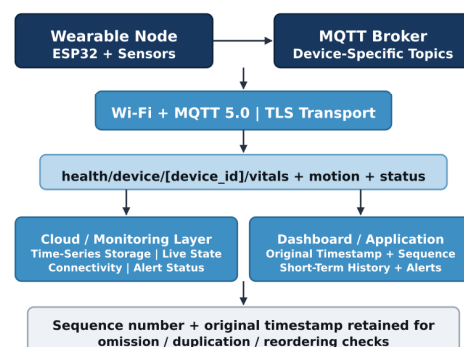


Figure 5: MQTT 5.0 / cloud communication architecture

One-time violation of a threshold is not an automatically identified clinical event. The desired pattern is one where there are sustained abnormal readings or a specific sequence of

events before local alerting, application handling, and human review. This design is better than the basic threshold system because it avoids false alarms. Telemetry frame comprises device ID, timestamp, physiologic parameters, motion status, channel-wise quality, sequence number, and alert state. For instance, the following is an example of how telemetry should look like:

```
{device_id,      timestamp,      heart_rate_bpm,
  spo2_percent, temperature_c, motion_state, quality,
  sequence, alert}
```

And the actual implementation will be serialized in JSON format prior to being securely transported via MQTT protocol.

Communication between the sensing node and the monitoring service is provided by MQTT 5.0. Three logical topic hierarchies are suggested:

```
health/device/{device_id}/vitals
health/device/{device_id}/motion
health/device/{device_id}/status
```

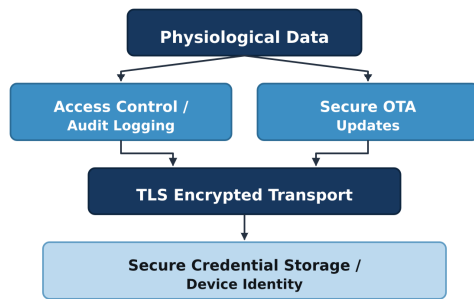


Figure 6: Layered security architecture for the wearable node.

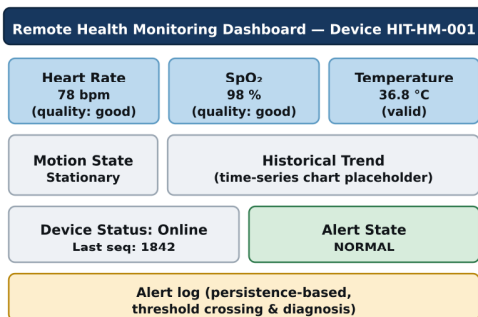


Figure 7: Representative monitoring dashboard layout.

The cloud application subscribes to necessary topics and stores observations with an original timestamp and sequence number, as well as presents current state, short history, connectivity status, and alert status via a dashboard. In case of an interim disconnection, the edge node keeps relevant state information and resumes the publications upon reconnecting. The sequence number allows identifying discontinuity in the

record downstream. Unique identity and credentials will be provided for each device. Access control uses the least-privilege approach to ensure that the device can only publish its messages to those allowed topics. TLS ensures data security in transit, and credentials must be stored through the secure storage capabilities of the embedded system rather than through the hard-coded application. Authentications and connection events must be stored in log files. Secure update and data minimization are some other aspects of the security design requirements. It is important to note that the healthcare interoperability boundary is outside the internal topic hierarchy of MQTT. Later on, the observations can be mapped into the standard healthcare resources like FHIR Observation resources without exposing the proprietary topic hierarchy to external healthcare systems.

The validation process concentrates on engineering behaviour as opposed to clinical accuracy. There are eight test criteria.

- T1 assesses the capability of sensor discovery and digital interface initialization.
- T2 determines data validity through timestamps and sequence numbers seen in successive packets.
- T3 incorporates controlled motion/contact alterations for PPG signal capture and confirms that poor quality windows are identified as invalid data rather than being accepted as good physiology.
- T4 uses value criteria for a threshold level of alertness to ensure persistence.
- T5 reproduces a specific acceleration sequence to ensure that only the desired fall candidate sequence creates an event.
- T6 blocks Wi-Fi access and tests to see if state is maintained and publishing resumed on reconnecting.
- T7 uses packet timestamps and sequences from brokers against application timestamps and sequences for validation purposes.
- T8 tries to gain access using invalid credentials or incorrect topic permissions and confirms failure.

These tests generate the acceptance criteria which can be carried out using a physical prototype. In addition to that, they avoid unwarranted

assumptions. For instance, a successful T3 test indicates proper functioning of the quality flags, but does not validate the clinical accuracy of the measurement. In addition, the successful fall event test validates the functioning of the screening logic in a specific motion scenario.

Table 1: Functional validation matrix

Test	Procedure	Acceptance Criterion	Significance
T1	Sensor discovery	Expected identity/status	Initialization
T2	Timestamps + sequence	No duplicates; monotonic	Data freshness
T3	Controlled PPG disturbance	Low-quality window flagged	Signal integrity
T4	Threshold persistence	Single excursion ignored	Nuisance reduction
T5	Fall sequence replay	Only intended sequence flags	Event logic
T6	Wi-Fi interruption	State preserved; resumes	Resilience
T7	Broker vs app records	One packet per sequence	End-to-end integrity
T8	Invalid access attempt	Rejected	Least privilege

4. OUTCOMES

The architecture of the proposed prototype fulfills the design requirements of the required engineering specification: there is separation of heterogeneous sensor channels, processing occurs prior to wireless transmission, quality accompanies data collection, and alerts are based on persistence or event sequences. Each of these behaviours has acceptance criteria through the functional matrix. The analysis of sensor capability shows that the chosen sensors can complement each other. For instance, the MAX86141 is used for optical PPG sensing; the MAX30205 is used for digital temperature sensing, while the ICM-42670-P provides inertial sensing to detect motion and falls. The ESP32 integrates the outputs from those sensors, performs processing locally and delivers data wirelessly. The critical engineering consequence of the system is that of retaining the context of the data. Physiological values are passed along with their quality level, time stamp, sequence number,

REFERENCES

- [1] *Information technology — Message Queuing Telemetry Transport (MQTT) v5.0*, ISO/IEC Standard 20922:2019, OASIS Standard, 2019.

and the ID of the device. The monitoring layer is thus able to identify whether the value passed on is a good measurement or a low-quality approximation. It will also be able to identify dropped or duplicate packets. Artificial data from patients, percent accuracy in clinical setting, sensitivity or specificity measures, percent packet loss, latency, and battery life are not mentioned because such metrics were not provided through a controlled experimental process in the prototype document. Future research must quantify these values using standardized equipment, standardized subjects, network conditions, and statistical analysis.

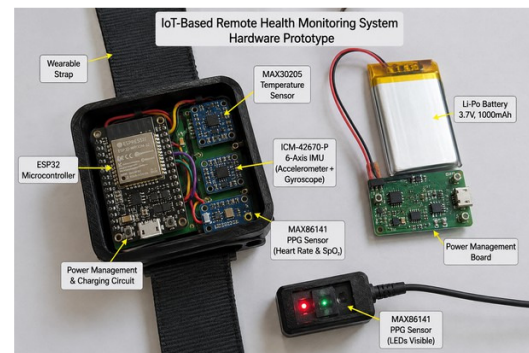


Figure 8: IoT-Based Remote Health Monitoring System Hardware Prototype

5. CONCLUSION

This study presented an end-to-end IoT framework for remote health monitoring, integrating multi-modal physiological and motion sensing with edge-level signal quality checks, context-aware alert logic, and encrypted MQTT communication. Rather than treating the wearable unit as a passive data forwarder, the architecture emphasizes data provenance, observation integrity, and granular, least-privilege security. By decoupling raw sensor acquisition from alert evaluation, the system effectively mitigates false positives driven by transient motion artifacts. As a prototype engineering effort, this work establishes functional viability rather than clinical diagnostic claims. Consequently, clinical diagnostic accuracy, battery longevity, and network latency under variable deployment conditions were beyond the current scope.

- [2] *FHIR Release 4 (Fast Healthcare Interoperability Resources)*, HL7 International, 2019. [Online]. Available: <https://hl7.org/fhir/R4/>
- [3] Maxim Integrated, “MAX86141: Optical pulse oximeter and heart-rate sensor front end for wearable health,” *MAX86141 Datasheet*, Rev. 1, Maxim Integrated Products, Inc., San Jose, CA, USA, 2018.
- [4] Analog Devices, “MAX30205: Human body temperature sensor,” *MAX30205 Datasheet*, Rev. 1, Analog Devices, Inc., Wilmington, MA, USA, 2016.
- [5] TDK InvenSense, “ICM-42670-P: High-performance 6-axis MEMS MotionTracking device,” *ICM-42670-P Datasheet*, Rev. 1.1, TDK InvenSense, San Jose, CA, USA, 2021.
- [6] Espressif Systems, “ESP-IDF Programming Guide: Security and Secure Boot/Flash Encryption,” *Espressif Systems Documentation*, 2023. [Online]. Available: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/>
- [7] C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST CSWP 29, Feb. 2024, doi: 10.6028/NIST.CSWP.29.
- [8] U.S. Food and Drug Administration, “Cybersecurity in medical devices: Quality system considerations and content of premarket submissions,” FDA Guidance for Industry and Food and Drug Administration Staff, Silver Spring, MD, USA, Sep. 2023.
- [9] World Health Organization, *Global Strategy on Digital Health 2020–2025*, Geneva, Switzerland: World Health Organization, 2021.
- [10] J. W. K. Chan, “Application of grey relational analysis for ranking options,” *Int. J. Comput. Appl.*, vol. 26, no. 1, pp. 10–18, 2006.
- [11] T. K. L. Tong and J. W. K. Chan, “Multi-criteria material selections and end-of-life product strategy: Grey relational analysis approach,” *Mater. Des.*, vol. 28, no. 5, pp. 1539–1546, 2007, doi: 10.1016/j.matdes.2006.02.016.
- [12] *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks—Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-2020, pp. 1–4379, Feb. 2021, doi: 10.1109/IEEESTD.2021.9363693.
- [13] *IEEE Standard for Health Informatics—Personal Health Device Communication – Part 00101: Technical Report—Analytical—General Approach*, IEEE Std 11073-00101-2018, pp. 1–70, Feb. 2019, doi: 10.1109/IEEESTD.2019.8653372.
- [14] OASIS, “MQTT Version 5.0,” OASIS Standard, Mar. 2019. [Online]. Available: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>.
- [15] HL7 International, “Observation – FHIR v4.0.1,” *HL7 Fast Healthcare Interoperability Resources Specification*, Oct. 2019. [Online]. Available: <https://hl7.org/fhir/R4/observation.html>.
- [16] OWASP Foundation, “Internet of Things (IoT) Security Guidance,” Open Web Application Security Project, 2021. [Online]. Available: <https://owasp.org/www-project-internet-of-things>.