ASEC 2025 Conference

The 6th International Electronic Conference on Applied Sciences

09–11 December 2025 | Online

MDPI

Secure and Efficient Biometric Data Streaming with IoT for Wearable Healthcare

Nikolaos Tournatzis[1], Stylianos Katsoulis[1], Ioannis Chrysovalantis Panagou[1], Evangelos Nannos[1], Ioannis Christakis[2], Grigorios Koulouras[1,*]

[1] TelSiP Research Laboratory, Department of Electrical and Electronic Engineering, School of Engineering, University of West Attica, Ancient Olive Grove Campus, 250 Thivon Str., GR-12241 Athens, Greece

[2] EDML Research Laboratory, Department of Electrical and Electronic Engineering, School of Engineering, University of West Attica, Ancient Olive Grove Campus, 250 Thivon Str., GR-12241 Athens, Greece

* Corresponding author

INTRODUCTION & AIM

The rapid expansion of the Internet of Medical Things (IoMT) necessitates advanced architectures that balance robust security with prolonged battery life.

- **The Challenge:** Wearable healthcare BLE devices encounter substantial limitations in battery longevity due to persistent communication requirements and further exhibit insufficient robustness in ensuring secure data transmission [1].
- **Our Objective:** To develop a secure, energy-efficient IoT framework integrating edge hardware with a cloud-native visualization stack.
- **Focus:** Utilizing encrypted BLE advertising for transmission and a containerized cloud environment for real-time monitoring [2].

METHODOLOGY

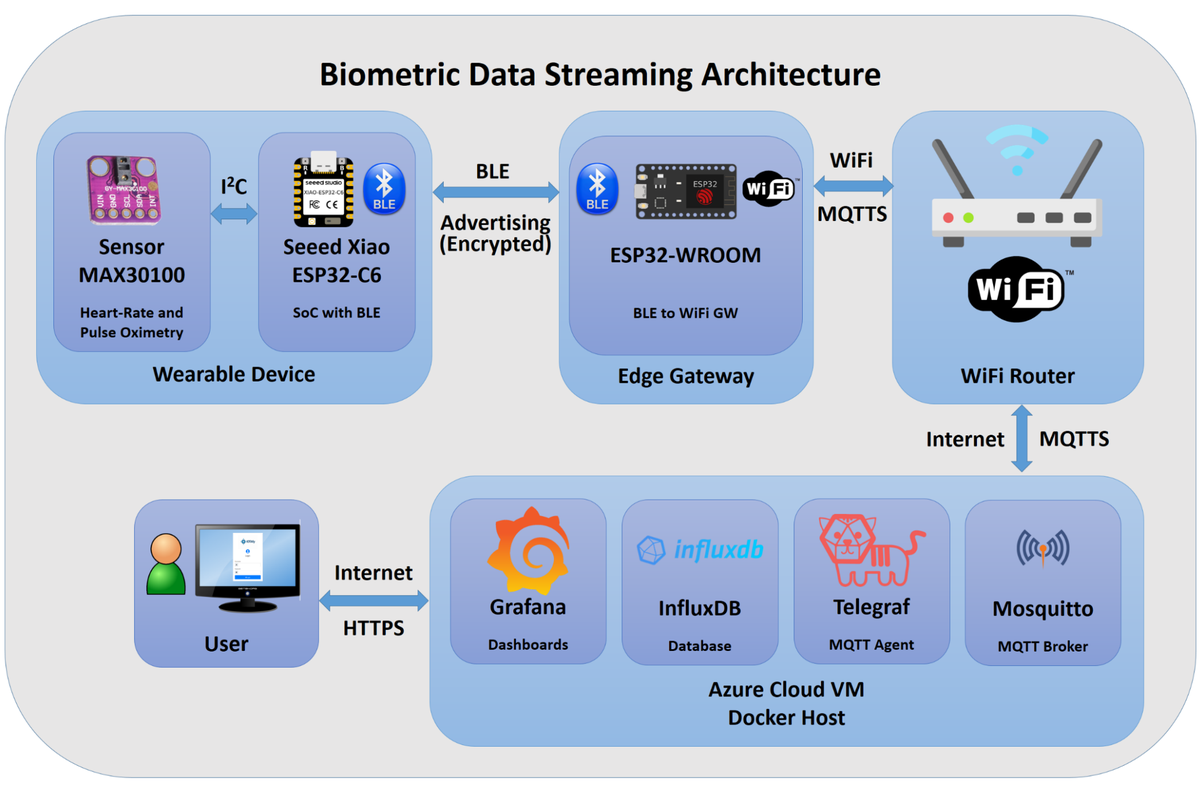
Our approach integrates specialized low-power edge hardware with a scalable, containerized cloud infrastructure to ensure seamless data flow.

A. Hardware Implementation

- **Wearable Device:** A MAX30100 sensor acquires Heart-Rate and SpO_2 via I^2C. The data is processed by a Seeed Xiao ESP32-C6 SoC.
- **Communication:** Instead of standard BLE pairing, the Xiao ESP32-C6 broadcasts biometric data using Encrypted BLE Advertising packets [3].
- **Edge Gateway:** An ESP32-WROOM node acts as a bridge that continuously monitors for specific encrypted packets, decrypts them, and forwards the payload via WiFi.

B. Cloud & Software Stack

- **Cloud Infrastructure:** Hosted on an Azure Cloud VM running Docker containers.
- **Communication:** Data is transmitted to the cloud using MQTTS (MQTT over TLS) for end-to-end security.
- **Data Pipeline:** The stack consists of Mosquitto (MQTT Broker), Telegraf (MQTT Agent), InfluxDB (Time-series Database), and Grafana (Visualization Dashboard) [2].



RESULTS & DISCUSSION

Experimental evaluation demonstrates that the proposed architecture achieves a high level of data confidentiality while significantly reducing power consumption.

A. Performance & Security

- **Encryption:** The implementation of AES-128-CCM ensures data confidentiality during the broadcast phase, preventing eavesdropping attacks [4].
- **Latency:** The lightweight MQTTS protocol combined with the local gateway processing resulted in minimal latency suitable for live monitoring.

B. Energy Efficiency

- **Savings:** Advertising at 1 Hz reduced energy consumption by 50%, while optimized sampling achieved savings up to 90% compared to standard BLE connections [3].
- **Impact:** By utilizing connectionless BLE advertising instead of permanent pairing, the wearable node's operational lifespan is drastically extended.

C. Visualization

- **Dashboards:** The Grafana dashboard successfully rendered real-time Heart-Rate and SpO_2 streams, remotely accessible via HTTPS by end-users.

CONCLUSION

This study confirms the viability of encrypted BLE advertising as a superior alternative to traditional pairing for secure, long-term healthcare monitoring.

- The proposed architecture successfully integrates specific low-power hardware (Seeed Xiao, ESP32) with a modern cloud stack (Azure VM/Docker).
- The system validates that decoupling security from connection-oriented protocols provides a scalable solution for medical IoT.
- Long-term storage in InfluxDB enables future retrospective analysis of patient health trends.

REFERENCES

1. Koulouras, G., Katsoulis, S., & Zantalis, F. (2025). Evolution of Bluetooth Technology: BLE in the IoT Ecosystem. Sensors (Basel, Switzerland), 25(4), 996. DOI: 10.3390/s25040996
2. Ali, S., & Anwer, F. (2025). An IoT-Enabled Cloud Computing Model for Authentication and Data Confidentiality using Lightweight Cryptography. *Arabian Journal for Science and Engineering*, 1-23. DOI: 10.1007/s13369-025-09983-1
3. Banani, S., Thiemjarus, S., Wongthavarawat, K., & Ounanong, N. (2021). A dynamic light-weight symmetric encryption algorithm for secure data transmission via BLE beacons. *Journal of Sensor and Actuator Networks*, *11*(1), 2. DOI: 10.3390/jsan11010002
4. Jain, H., & Gupta, N. K. (2024). Enhancing authentication in wearable devices: BLE-AES-CCM implementation. In *Intelligent Computation and Analytics on Sustainable Energy and Environment* (pp. 262-268). CRC Press. DOI: 10.1201/9781003540199