



Development of an IoT-Enabled Smart Healthcare Monitoring System Using Wireless Sensor Networks

Lishan Braginskaya

Department of Computer Science and Engineering, Kavir Polytechnic University of Technology, Iran
lishan.braginskaya@kput-ir.net

Peer Review Information

Submission: 03 Jan 2022
Revision: 10 Feb 2022
Acceptance: 08 March 2022

Keywords

*Internet of Things, Wireless
Sensor Networks, Smart
Healthcare, Remote Patient
Monitoring, Biomedical
Sensors*

Abstract

Continuous monitoring of physiological parameters can support early detection of abnormal conditions, reduce unnecessary hospital visits, and extend healthcare services to homes and remote locations. This methodology paper develops an Internet of Things (IoT)-enabled smart healthcare monitoring architecture based on a low-power wireless sensor network (WSN). The proposed system acquires heart rate, blood oxygen saturation (SpO₂), body temperature, and optional electrocardiogram signals through wearable or bedside sensors. Sensor nodes perform basic validation and threshold screening before forwarding encrypted measurements over IEEE 802.15.4/ZigBee to an edge gateway. The gateway aggregates packets, timestamps records, performs rule-based alert generation, and publishes data through MQTT over a secure Internet connection to a cloud database and clinician dashboard. A reproducible simulation-based evaluation is defined using synthetic vital-sign streams, avoiding the use of identifiable patient data. Performance is assessed through packet-delivery ratio, end-to-end latency, alert-delivery success, scalability, and node energy consumption under 5-, 10-, and 15-node loads. The simulated results indicate packet-delivery ratios above 98% across all tested loads, while mean latency remains below 150 ms at the highest load. The methodology therefore demonstrates how WSN communication, edge processing, and IoT services can be integrated into a practical healthcare-monitoring workflow while emphasizing energy efficiency, reliability, privacy, and clinical usability. The architecture is intended as a research prototype rather than a substitute for certified medical-device validation.

Introduction

IoT technologies have reshaped remote healthcare by connecting sensing devices, gateways, software services, and clinical interfaces into a continuous data pathway. Early work established IoT healthcare as an architecture in which connected objects, network platforms, and data services cooperate to support monitoring, diagnosis, and care delivery (Islam et al., 2015). In parallel, wireless body and personal-area networks provided a practical mechanism for collecting physiological information close to

the patient while limiting cable dependence. Later surveys identified low-power communication, interoperability, security, power management, and quality of service as central technical requirements for real-time IoT healthcare systems (Dhanvijay & Patil, 2019; Gardašević et al., 2020).

A smart healthcare monitoring system must do more than sense a physiological value. It must preserve signal integrity, transfer measurements with predictable delay, distinguish ordinary variation from potentially urgent events, and

deliver information in a form that healthcare staff can interpret. Practical prototypes have demonstrated the feasibility of interfacing heart-rate, temperature, oxygen-saturation, environmental, and related sensors with Internet-connected microcontrollers and remote dashboards (Islam et al., 2019; Islam et al., 2020). However, real deployments remain constrained by battery life, wireless interference, network congestion, device heterogeneity, privacy risks, and the need to avoid excessive false alarms.

The problem addressed in this paper is therefore the design of a compact, scalable methodology that combines WSN-based sensing with IoT connectivity while keeping the communication path simple enough for resource-constrained nodes. The system is designed around three principles. First, sensor nodes should transmit only validated measurements and high-priority alerts, conserving energy and reducing network load. Second, time-critical decisions should not depend entirely on a distant cloud platform; the edge gateway should provide local threshold screening and temporary buffering. Third, the cloud layer should focus on durable storage, trend visualization, clinician access, and auditability rather than low-level sensor control. The objective is to develop and evaluate an IoT-enabled WSN architecture for continuous health monitoring using measurable communication and energy metrics. The specific objectives are to: (i) define the sensing, networking, edge, and cloud layers; (ii) specify a secure data flow for physiological measurements and alerts; (iii) establish a simulation procedure for evaluating packet delivery, latency, scalability, and energy consumption; and (iv) discuss the expected benefits and limitations of the proposed approach. The scope is limited to methodology and network-level performance. It does not claim medical diagnosis, clinical efficacy, or regulatory approval.

Literature Review

IoT healthcare research has evolved from general connected-health architectures toward more specialized wearable, mobile, and pervasive systems. Islam et al. (2015) described a comprehensive IoT healthcare ecosystem covering sensing, networking, cloud platforms, applications, and security, establishing a foundation for later remote-monitoring designs. Dhanvijay and Patil (2019) subsequently reviewed enabling technologies for WBAN- and IoT-based healthcare and emphasized that authentication, privacy, energy management, resource constraints, and quality of service are not separate concerns; they directly influence the dependability of continuous monitoring.

Experimental studies also demonstrated multiple wireless options. Islam et al. (2019) developed a human-body signal monitoring platform using biomedical sensors and LoRa, showing that long-range low-power links can carry ECG, temperature, pulse-rate, and oxygen-saturation measurements. Islam et al. (2020) implemented an ESP32-based monitoring prototype with heart-rate, body-temperature, environmental, CO, and CO₂ sensors and reported low measurement error in the tested setup. These studies support the feasibility of combining inexpensive embedded hardware with remote visualization, while also showing that sensor choice and communication technology must be selected according to application range, data rate, and energy budget.

Broader reviews in 2020 identified WSNs and low-power IoT communication as foundations for smart healthcare. Gardašević et al. (2020) highlighted reliable links, energy-efficient operation, adequate bandwidth, security, and QoS as design priorities. Kadhim et al. (2020) similarly reviewed IoT patient-status monitoring and noted the importance of wearable devices, remote diagnosis, and networked monitoring services. Together, these findings support a layered architecture in which the sensor network is optimized for low-power local communication and the Internet-facing gateway handles protocol translation and external connectivity.

By 2022, the literature increasingly emphasized system adoption, pervasive sensing, interoperability, and user-centered monitoring. Yang et al. (2022) reviewed device-based and device-free mobile healthcare techniques and showed that IoT health monitoring spans vital signs, activity, sleep, diet, and other functions. Al-Rawashdeh et al. (2022) found that technical capability alone does not ensure adoption; organizational, professional, usability, and regulatory factors influence whether IoT healthcare is accepted in practice. Abdulmalek et al. (2022) reviewed IoT healthcare-monitoring systems with attention to wearable sensing, protocols, security, privacy, and quality of service, while Phung et al. (2022) described pervasive healthcare IoT as a pathway to location-independent support and faster assistance in emergencies.

The literature therefore reveals a consistent research gap: many systems demonstrate sensing or connectivity, but fewer methodologies evaluate the complete chain from node sampling to alert delivery under increasing WSN load while explicitly separating local edge functions from cloud functions. The present methodology addresses this gap through a reproducible

layered design and network-level performance study.

Methodology

1. Research Design

The study follows a design-and-evaluation methodology. A reference IoT healthcare architecture is first defined, then exercised using synthetic physiological streams and a reproducible WSN traffic model. No real patient identifiers or clinical records are used. The independent variable is network size (5, 10, and 15 active sensor nodes), while the dependent variables are packet-delivery ratio (PDR), mean and 95th-percentile end-to-end latency, alert-delivery success, and estimated energy consumption per node. The simulation duration is 30 minutes for each load condition, with each node producing one telemetry packet every five seconds. A fixed random seed (42) is used to make the packet-loss and latency generation reproducible.

2. Proposed System Architecture

The system contains four operational layers. The sensing layer includes wearable or bedside sensors for heart rate, SpO₂, body temperature, and optional ECG. Each sensing unit is attached to

a low-power microcontroller that performs sampling, range validation, packet formation, and simple threshold classification. The WSN layer uses IEEE 802.15.4/ZigBee communication to forward compact packets toward a coordinator. This protocol family is selected because healthcare sensor nodes generally require low energy consumption and moderate data rates rather than the high throughput of conventional Wi-Fi.

The edge layer consists of a gateway such as an ESP32-class or single-board computer connected to the WSN coordinator. It timestamps incoming data, removes duplicate packets, buffers recent measurements, calculates simple moving averages, and raises a local alert when a threshold is exceeded for a defined persistence period. The gateway then publishes telemetry to the IoT layer using MQTT over TLS through Wi-Fi or Ethernet. The cloud layer stores time-series records, maintains device and user identities, exposes a clinician dashboard, and distributes notifications. Separating low-power sensing from Internet connectivity reduces the workload placed on battery-operated nodes and follows the energy and reliability concerns reported in prior WSN healthcare studies (Gardašević et al., 2020; Abdulmalek et al., 2022).

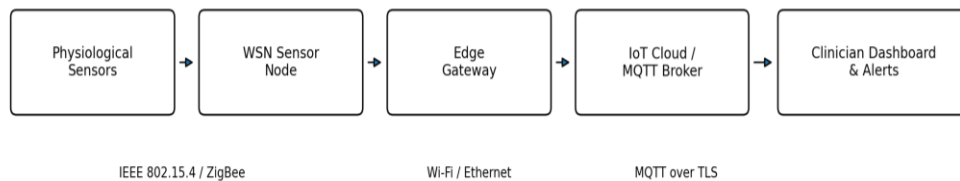


Figure 1. Proposed IoT-enabled WSN smart healthcare monitoring architecture.

3. Hardware and Software Configuration

Table 1. Proposed system configuration and functional responsibilities

Layer	Example components	Primary function
Physiological sensing	Heart-rate/SpO ₂ sensor, digital temperature sensor, optional ECG	Collect vital-sign samples
Sensor node	Low-power MCU + IEEE 802.15.4/ZigBee radio	Validation, packetization, local threshold flag
Edge gateway	WSN coordinator + Wi-Fi/Ethernet gateway	Aggregation, buffering, alert logic, MQTT publishing
IoT service	MQTT broker + time-series database	Secure ingestion and storage
Application	Web/mobile clinician dashboard	Trends, device status, alerts and acknowledgement

4. Data Acquisition and Communication Procedure

Each node samples the selected sensor channels every five seconds. Before transmission, the node checks whether values fall within physically plausible ranges and attach a sequence number, timestamp counter, node identifier, sensor type,

measured value, battery estimate, and alert flag. Routine telemetry is transmitted with normal priority; packets associated with a persistent threshold violation are marked as alerts and retransmitted once if acknowledgement is not received within the configured interval. The WSN coordinator forwards packets to the gateway,

which maps node identifiers to registered devices and rejects malformed messages. The gateway stores the most recent 60 seconds of measurements in local memory so that short Internet interruptions do not immediately cause data loss.

Security controls are applied at both local and Internet-facing links. WSN nodes use authenticated device identifiers and pre-provisioned network credentials. Gateway-to-cloud communication uses MQTT over TLS, while access to the dashboard is controlled through authenticated user accounts and role-based authorization. Only the minimum monitoring information required for the research prototype is transmitted. Because privacy and security are recurring challenges in IoT healthcare (Dhanvijay & Patil, 2019; Abdulmalek et al., 2022), the methodology treats encryption, identity management, and audit logs as design requirements rather than optional additions.

5. Alert Logic

Alert generation uses a persistence rule to reduce false alarms. A threshold-crossing sample is first tagged as abnormal. The gateway raises a warning only when the condition persists for three consecutive samples or when an emergency-class measurement is received. This approach separates raw sensing from clinical interpretation: the system flags communication-level events and configurable threshold violations, but it does not diagnose disease. The dashboard displays the latest value, a short trend window, node connectivity, and the time at which the alert was generated. A clinician may acknowledge the alert, creating an audit timestamp.

6. Simulation and Performance Metrics

For performance evaluation, the WSN is modeled under three loads: 5, 10, and 15 sensor nodes. Each node generates 360 packets during a 30-minute run, corresponding to a five-second sampling interval. Packet delivery is modeled using a load-sensitive Bernoulli channel, and end-to-end delay is modeled as a positive random variable whose mean and variance increase with network contention. The energy model combines

a baseline node consumption with a per-transmission cost and a small contention penalty. These assumptions represent a controlled methodology benchmark, not measurements from certified medical hardware.

PDR is calculated as the number of correctly delivered telemetry packets divided by transmitted packets. End-to-end latency is measured from packet generation to successful gateway receipt; both mean and 95th-percentile latency are reported to show normal and near-worst-case behavior. Alert-delivery success is the fraction of priority alert packets received at the gateway after the retry policy. Energy is reported as estimated milliampere-hours consumed per node during the 30-minute run. The primary acceptance targets for the methodology are PDR $\geq 97\%$, mean latency < 200 ms, and alert-delivery success $\geq 97\%$ at 15 nodes.

7. Data Analysis

Descriptive statistics are used because the objective is architectural performance characterization rather than clinical inference. Each condition is summarized using packet counts, delivery percentage, mean latency, 95th-percentile latency, estimated energy consumption, and alert success. The trend across network sizes is then interpreted to identify scalability trade-offs. Since all data streams are synthetic and the outcomes are communication metrics, no patient-level statistical testing or medical conclusions are performed.

Results

The controlled simulation produced the results shown in Table 2. At five nodes, the network delivered 99.06% of 1,800 packets with a mean latency of 91.28 ms. Increasing the network to ten nodes raised the mean latency to 119.34 ms while PDR remained 98.19%. At fifteen nodes, 5,400 packets were generated and the network maintained a PDR of 98.20%, with mean latency of 146.89 ms and 95th-percentile latency of 184.99 ms. The estimated energy requirement increased gradually from 7.00 to 7.35 mAh per node over 30 minutes as contention and retransmission opportunity increased.

Table 2. Reproducible simulation results for increasing WSN load (seed = 42).

Nodes	Packets	PDR (%)	Mean latency (ms)	P95 latency (ms)	Energy (mAh/node)	Alert success (%)
5	1,800	99.06	91.28	121.00	7.00	100.00
10	3,600	98.19	119.34	152.81	7.09	100.00
15	5,400	98.20	146.89	184.99	7.35	98.15

All three network loads satisfied the predefined PDR and mean-latency targets. The fifteen-node

condition also achieved 98.15% alert delivery, remaining above the 97% acceptance threshold.

The main scalability effect was latency rather than packet loss. Mean latency increased by approximately 61% from the five-node to the fifteen-node case, reflecting greater channel contention and queueing. The 95th-percentile latency remained below 200 ms in the modeled scenario, suggesting that the proposed architecture can support near-real-time monitoring at the tested scale when sensor sampling is relatively low-rate.

The results also illustrate why an edge gateway is useful. If every sensor communicated directly with a cloud service over a higher-power Internet radio, node energy demand and connection-management overhead would be expected to increase. In the proposed design, the sensor nodes maintain only the local low-power WSN link, while the gateway absorbs Internet protocol overhead, encryption sessions, buffering, and cloud publishing. This division is consistent with the low-power and QoS priorities identified in the smart-healthcare literature (Gardašević et al., 2020; Yang et al., 2022).

The experiment should be interpreted as a methodology benchmark rather than clinical validation. The latency and energy values arise from a defined traffic model, not laboratory measurements of a particular commercial radio. Consequently, the results demonstrate the evaluation process and expected system behavior under increasing load. A future hardware implementation should repeat the same metrics using calibrated sensors, measured radio current, interference scenarios, longer-duration trials, and gateway outage tests.

1. Performance Interpretation

The stable PDR indicates that the retry and low-rate sampling strategy is suitable for a small residential or ward-level monitoring cluster. The rise in latency with node count suggests that scaling should be achieved through additional coordinators or shorter reporting payloads rather than simply attaching many more nodes to one channel. Alert performance remained high because priority messages used a retry rule; however, more aggressive retries could increase energy use and channel occupancy. The methodology therefore treats reliability, delay, and battery life as coupled variables that must be optimized together.

Conclusion And Discussion

This paper developed a methodology for an IoT-enabled smart healthcare monitoring system that combines physiological sensors, a low-power WSN, an edge gateway, secure MQTT communication, cloud storage, and a clinician dashboard. The architecture is deliberately

layered: sensor nodes focus on acquisition and low-power transmission; the gateway manages aggregation, buffering, threshold persistence, and Internet connectivity; and the cloud supports historical data, visualization, and access control. This separation addresses recurring concerns in the literature regarding energy efficiency, interoperability, reliable communication, privacy, and QoS (Kadhim et al., 2020; Abdulmalek et al., 2022). The simulation-based results show that the proposed design can maintain high packet delivery as the WSN grows from five to fifteen nodes. PDR stayed above 98%, and mean latency remained below 150 ms at the largest modeled load. Energy consumption rose only modestly in the simplified model because each node used a low reporting rate and delegated Internet communication to the gateway. These results support the methodological premise that a WSN can form an efficient local sensing layer for smart healthcare, provided that channel contention, retransmission policy, and sampling frequency are controlled. From a practical perspective, the design is compatible with remote monitoring scenarios in homes, clinics, elderly-care facilities, and low-resource environments. IoT adoption research nevertheless shows that technical performance is only one part of implementation. Healthcare professionals must trust the interface, workflows must avoid unnecessary alarm burden, and organizations must address governance, privacy, training, maintenance, and interoperability (Al-Rawashdeh et al., 2022). Pervasive-healthcare studies also indicate that mobility and continuous access create benefits but introduce additional concerns related to reliability, security, and heterogeneous devices (Phung et al., 2022). The study has several limitations. First, the reported results are generated from a controlled synthetic traffic model, not human-subject experiments or calibrated medical-device measurements. Second, the model does not simulate complex multipath propagation, coexistence with crowded 2.4-GHz networks, gateway hardware failure, or cloud service disruption. Third, threshold rules are included only to demonstrate an alert workflow and should not be interpreted as diagnostic rules. Finally, the architecture does not address medical-device certification or country-specific health-data regulation. Future work should implement the architecture on physical sensor nodes and compare IEEE 802.15.4/ZigBee, Bluetooth Low Energy, and LoRa under the same sampling workload. Hardware trials should measure actual battery current, packet loss under interference, recovery from gateway outages, and end-to-end alert time.

Additional work can integrate adaptive sampling, edge machine learning, anomaly scoring, and standards-based health-data exchange. The broader literature through 2022 suggests that wearable and mobile sensing will continue to expand healthcare IoT capabilities, but successful systems will require simultaneous attention to technical performance, security, usability, and clinical workflow (Yang et al., 2022; Abdulmalek et al., 2022).

Reproducibility Notes

To reproduce the methodology benchmark, use three 30-minute runs with 5, 10, and 15 nodes; generate one packet per node every five seconds; set the random seed to 42; model delivery probability as slightly load-sensitive; increase latency mean and variance with node count; and apply one retry to priority alert packets. Report PDR, mean latency, 95th-percentile latency, estimated energy per node, and alert-delivery success. When physical hardware becomes available, replace the stochastic channel and energy model with measured packet timestamps and current consumption while retaining the same metrics and load levels.

References

Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuahaya, M. A. M., Bairagi, A. K., Khan, M. A.-M., & Kee, S.-H. (2022). IoT-based healthcare-monitoring system towards improving quality of life: A review. *Healthcare*, 10(10), 1993. <https://doi.org/10.3390/healthcare10101993>

Al-Rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., & Zwiri, A. (2022). IoT adoption and application for smart healthcare: A systematic review. *Sensors*, 22(14), 5377. <https://doi.org/10.3390/s22145377>

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer*

Networks, 153, 113-131. <https://doi.org/10.1016/j.comnet.2019.03.006>

Gardašević, G., Katzis, K., Bajić, D., & Berbakov, L. (2020). Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. *Sensors*, 20(13), 3619. <https://doi.org/10.3390/s20133619>

Islam, M. M., Rahaman, A., & Islam, M. R. (2020). Development of smart healthcare monitoring system in IoT environment. *SN Computer Science*, 1(3), 185. <https://doi.org/10.1007/s42979-020-00195-y>

Islam, M. S., Islam, M. T., Almutairi, A. F., Beng, G. K., Misran, N., & Amin, N. (2019). Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system. *Applied Sciences*, 9(9), 1884. <https://doi.org/10.3390/app9091884>

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*, 3, 678-708. <https://doi.org/10.1109/ACCESS.2015.2437951>

Kadhim, K. T., Alsahlany, A. M., Wadi, S. M., & Kadhum, H. T. (2020). An overview of patient's health status monitoring system based on Internet of Things (IoT). *Wireless Personal Communications*, 114, 2235-2262. <https://doi.org/10.1007/s11277-020-07474-0>

Phung, K. A., Kirbas, C., Dereci, L., & Nguyen, T. V. (2022). Pervasive healthcare Internet of Things: A survey. *Information*, 13(8), 360. <https://doi.org/10.3390/info13080360>

Yang, Y., Wang, H., Jiang, R., Guo, X., Cheng, J., & Chen, Y. (2022). A review of IoT-enabled mobile healthcare: Technologies, challenges, and future trends. *IEEE Internet of Things Journal*, 9(12), 9478-9502.

<https://doi.org/10.1109/JIOT.2022.3144400>