

QoS-Aware Secure Federated Intelligence for Biomedical Electronics and Medical Informatics in Wireless Health Monitoring Networks

A. Kaliappan¹, Senthil Kumar P¹, K. Tamilselvi², A. T. Ravi³, S. P. Santhoshkumar⁴, and Asha V.¹

¹ School of Computing, SRM Institute of Science and Technology, Tiruchirappalli, India

² Artificial Intelligence and Data Science, Dr. Mahalingam College of Engineering and Technology, Pollachi, India

³ Computer Science and Engineering (Cyber Security), Dhanalakshmi Srinivasan College of Engineering, Coimbatore, India

⁴ Computer Science and Design, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

Corresponding author: A. Kaliappan (e-mail: kaliappantpr@gmail.com). **Author(s) email:** psenthilexcel@gmail.com, tamilselvik0205@gmail.com, atravin@gmail.com, spsanthoshkumar16@gmail.com, ashamecse@gmail.com, ashamephd@gmail.com

Abstract The rapid advancement of Wireless Health Monitoring Networks (WHMNs) using Biomedical Electronics (BMEs) in medical informatics has been driven primarily by continuous, real-time, remote measurement of fundamental physiological parameters such as ECG, body temperature, blood-oxygen saturation, and heart rate. However, practical WHMN deployments face significant challenges in meeting stringent Quality-of-Service (QoS) requirements under limited energy availability, while also needing scalable, secure transmission of sensitive medical information over open wireless channels. Centralized routing and learning mechanisms used in existing WHMN systems introduce excessive communication overhead, leave WHMNs vulnerable to cyber-attacks, and provide inadequate protection for patient data privacy. In this study, we propose a QoS-Aware Secure Federated Intelligence (QASFI) Framework developed specifically for BME-driven WHMNs, comprising: (1) decentralized federated learning with non-IID-aware aggregation for distributed intelligence; (2) trust-based QoS-aware routing with an adaptive composite metric; and (3) a lightweight blockchain-assisted security mechanism that provides authentication and tamper-resistance. Unlike traditional methods, QASFI lets each edge node train its own model on its own data and share only encrypted model updates, significantly minimizing communication overhead while preserving patient privacy. Simulation results show the superiority of QASFI over state-of-the-art WHMN protocols with respect to Packet Delivery Ratio (PDR), End-to-End Delay (E2ED), Residual Energy per Node (REPN), and Overall Network Lifetime (ONL), with statistically significant improvements ($p < 0.05$) across all four metrics, including 7–15% higher PDR, 17–38% lower delay, and 30–40% longer network lifetime relative to the strongest baselines, alongside a federated ECG classification accuracy of 93.8% (within 0.4% of a centralized model) and packet-delivery degradation below 4% under a 20% malicious-node ratio. The lightweight Proof-of-Trust blockchain adds only 8.3–12.7% energy overhead per node, within the resource envelope of Tier-2/Tier-3 biomedical hardware. These results indicate that QASFI offers a practical, privacy-preserving pathway toward secure, QoS-guaranteed wireless health monitoring systems.

Keywords Biomedical Electronics; Medical Informatics; Wireless Health Monitoring Networks; Federated Learning; QoS-Aware Routing; Blockchain Security; Energy Efficiency; Privacy Preservation

1. Introduction

Wireless Health Monitoring Systems (WHMS) have been developed for remote health monitoring, using sensors to continuously track a patient's physiological status via wearable or implantable devices. This physiological data may include ECG, SpO₂, body temperature, blood pressure, and physical movement. There is growing interest in WHMS because they enable continuous and remote physiological signal acquisition and transmission [1], [2] for applications including telemedicine, eldercare, chronic-disease

management, and emergency medical services. Despite their promise, WHMNs face several fundamental challenges that limit large-scale adoption. Sensor nodes used in biomedical electronics are typically constrained by limited battery capacity, processing power, and memory [3]. At the same time, medical informatics applications demand high QoS in terms of low latency, high packet delivery ratio, reliability, and continuous availability, since medical data is often time-critical and life-sensitive [4]. Achieving these conflicting objectives of energy

efficiency and strict QoS remains a major research challenge in WHMN design.

Beyond performance, a primary concern in WHMNs is patient confidentiality, since sensitive medical information transmitted over wireless channels may be intercepted, replayed, or manipulated, and malicious insiders could compromise the network [5], [6]. Traditional centralized architectures, in which raw physiological data is sent from each sensor node to a distant server or cloud for processing, further increase privacy risk and communication overhead, which is incompatible with current privacy regulations and ethical standards in medical informatics [7]. Several routing and optimization protocols have been developed for WHMNs, including energy-aware, QoS-aware, and cross-layer approaches [8], [9], and machine-learning and artificial-intelligence techniques have been applied to routing decisions, anomaly detection, and resource allocation in biomedical sensor networks [10], [11]. However, many of these solutions require centralized training, which entails collecting raw physiological data centrally, thereby increasing latency and power consumption and raising serious privacy concerns [12].

Federated learning has recently emerged as a means to alleviate these limitations by enabling decentralized model training across distributed networks while keeping raw data local [13], [14]. Federated learning allows biomedical sensor networks to collaboratively develop intelligent models without exposing sensitive patient data. However, its use in WHMNs introduces new challenges, including unreliable communication links, malicious participants, and trust management among nodes [15]. Ensuring secure, tamper-resistant communication in a federated WHMN environment remains an open research question. Recent studies have investigated lightweight blockchain technologies to provide authentication, data integrity, and trust management in resource-constrained networks [16], [17]. When properly implemented, blockchain-assisted security mechanisms can help protect against model poisoning, unauthorized model access, and data modification in biomedicine-based healthcare systems.

Motivated by these challenges, this paper proposes a QoS-Aware Secure Federated Intelligence (QASFI) Framework for biomedical electronics and medical informatics applications in WHMNs. The framework integrates federated learning for privacy-preserving intelligence, trust-based QoS-aware routing for energy-efficient and reliable data delivery, and lightweight blockchain mechanisms for secure authentication and integrity assurance. Unlike existing approaches, QASFI jointly addresses energy efficiency, QoS optimization, security, and privacy within a single, unified architecture tailored for WHMNs.

Biomedical electronic sensor nodes are typically powered by batteries with capacities ranging from 0.1 to 1.0 J, which limits the computation and communication they can perform. Clinical-outcome studies indicate that a packet-loss rate of just 5% in ECG transmission is associated with misclassification of arrhythmia events in approximately 18% of monitored cases, materially reducing diagnostic accuracy. Similarly, end-to-end delays greater than 100 ms for time-sensitive alerts, such as those signaling cardiac arrhythmia or hypoxia, have been associated with reduced success rates for clinical interventions by up to 23% in emergency telemedicine applications. These figures illustrate the necessity of reliable, low-latency communication in WHMN deployments. Security is an equally pressing concern: reports indicate that 30–40% of clinical IoT medical devices exhibit demonstrable exploitability, and the Ponemon Institute reports that healthcare breaches account for 41% of all reported data breaches. Centralized architectures that aggregate raw physiological data at remote servers create single points of failure and expose patient data to both transmission-level and server-level threats. The main contributions of this research are summarized as follows:

- 1) A novel QoS-aware federated intelligence framework is proposed for biomedical-electronics-based WHMNs, enabling decentralized learning while preserving patient privacy.
- 2) A trust-based routing metric is designed by jointly considering residual energy, delay, and node trustworthiness to ensure reliable and energy-efficient data transmission.
- 3) A lightweight blockchain-assisted security mechanism is integrated to provide authentication, integrity, and resistance against insider and data-tampering attacks.
- 4) Extensive simulation-based evaluations demonstrate significant improvements in packet delivery ratio, latency, residual energy, and network lifetime compared with existing WHMN protocols.
- 5) A comprehensive security analysis validates the suitability of the proposed framework for next-generation medical informatics and telemedicine systems.

The remainder of this paper is organized as follows. Section II reviews prior research on energy-efficient routing, QoS optimization, security, machine learning, federated learning, and blockchain technologies for WHMNs. Section III introduces the system model, network architecture, and problem formulation. Section IV presents the proposed QASFI Framework, including its architecture, operational phases, and algorithms. Section V describes the experimental setup, simulation

parameters, datasets, and comparative baselines. Section VI reports the performance-evaluation results. Section VII discusses the findings, limitations, and practical implications. Section VIII concludes the paper.

II. Related Work

Research on WHMNs has gained considerable momentum owing to advances in biomedical electronics and medical informatics. Existing studies broadly focus on energy-efficient routing, QoS optimization, security and privacy mechanisms, and intelligent data processing. This section reviews the most relevant contributions and identifies the limitations that motivate the proposed work. Early research on WHMNs concentrated on energy-efficient routing, QoS protocols, healthcare-data security, and intelligent data processing for biomedical sensor networks. Energy efficiency was initially pursued through power- or residual-energy-based routing, followed by thermal-aware, link-aware, and cross-layer routing to improve reliability. Several QoS routing algorithms were subsequently developed to meet stringent medical-data requirements such as low latency, high reliability, and emergency-traffic priority; however, most rely on centralized architectures that increase communication overhead, limit scalability, and remain vulnerable to insider attacks. Machine-learning techniques have also been applied to anomaly detection and routing optimization in WHMNs, but most depend on centralized training, which increases energy consumption and compromises patient privacy. Federated learning has more recently been identified as an effective method for collaborative learning in healthcare networks while preserving patient privacy, though it remains challenged by device heterogeneity, unreliable wireless links, and the risk of model-poisoning attacks. Blockchain technology offers decentralized trust and tamper-resistant logging, but conventional implementations are often too energy-intensive for resource-constrained sensor nodes. Overall, the literature largely treats energy efficiency, QoS, security, and intelligent learning as separate problems, motivating the need for a unified framework that improves reliability, privacy, and efficiency simultaneously.

A. Energy-Efficient Routing in WHMNs

Energy efficiency is a central concern in WHMNs because biomedical sensor nodes are battery-operated. Early routing methods sought to extend network lifetime by reducing transmission power and hop counts. Subsequent protocols incorporated residual energy and transmission distance to prevent premature node failure, while thermal-aware and link-aware routing protocols were developed to reduce tissue heating and unreliable connections in body-area networks. Although these approaches improved reliability, they often did not satisfy stringent QoS

requirements for delay and packet delivery ratio. Cross-layer routing techniques further improved efficiency by jointly tuning MAC- and network-layer parameters, but most energy-efficient routing techniques assume static network configurations and therefore perform poorly in dynamic biomedical environments.

B. QoS-Aware Routing for Medical Applications

Because physiological data is often life-critical, medical-informatics applications impose strict QoS requirements. Several QoS-aware routing protocols for WHMNs have been proposed [8], [9], typically employing an emergency-priority model in which emergency messages are prioritized over routine traffic. Multi-objective routing strategies that jointly optimize delay, reliability, and energy have shown improved performance over single-objective approaches; however, most rely on centralized decision-making or complete network knowledge, increasing communication cost and limiting scalability. Moreover, while such protocols provide QoS guarantees, they generally offer no mechanism to ensure the confidentiality or integrity of transmitted data.

C. Security and Privacy Mechanisms in WHMNs

Protecting sensitive medical information is a major priority in biomedical-electronics and medical-informatics systems. Researchers have proposed numerous authentication and encryption schemes, including lightweight cryptographic algorithms (e.g., Elliptic Curve Cryptography) and hash-based authentication suited to resource-constrained sensor nodes. While effective for confidentiality, many existing approaches do not address insider threats, data tampering, or trust management, and centralized architectures remain susceptible to single points of failure. Anonymization and secure aggregation have been proposed to preserve privacy, but typically at the cost of additional processing and communication overhead.

D. Machine Learning in Biomedical Sensor Networks

Machine learning has increasingly been applied to improve routing, anomaly detection, and predictive analytics in WHMNs [18]. Support Vector Machines, neural networks, and fuzzy inference systems have been used to identify malicious nodes, predict physiological parameters, and reduce redundant transmissions [19], [20]. While these centralized learning methods enhance network intelligence, they require continuous transmission of raw biomedical data to a central server, increasing energy consumption, introducing latency, and jeopardizing patient privacy [21], which limits their applicability in large-scale medical-informatics systems.

E. Federated Learning for Medical Informatics

Federated learning enables distributed model training without sharing raw data among participants [22], [23], and has been applied to medical imaging, electronic health records, and disease prediction, where it is well suited to protecting patient privacy [24]. Recent work has examined federated learning in sensor networks and Internet of Medical Things (IoMT) environments [25], [26]. Applying federated learning to WHMNs, however, introduces new challenges such as unreliable wireless links, node heterogeneity, and the potential for malicious participants or model-poisoning attacks [27].

F. Blockchain-Assisted Security in Healthcare Networks

Researchers have explored blockchain technology to increase the trustworthiness and reliability of healthcare information systems [28]. Lightweight blockchain frameworks have been proposed to provide authentication, access control, and tamper resistance in IoMT and WHMN environments [29]. Nonetheless, blockchain-based solutions can suffer from scalability and energy-consumption issues when applied in their standard form to resource-constrained biomedical sensor networks [30], motivating designs that balance network efficiency with security.

G. Identified Research Gaps

Current methods largely address energy efficiency, QoS optimization, security, and intelligence as separate problems [31]. Little research has taken an integrated approach that simultaneously combines federated learning with QoS-aware routing and lightweight blockchain security in WHMNs for biomedical electronics and medical informatics, and trust-aware routing within federated environments remains underexplored. These limitations motivate the proposed QoS-Aware Secure Federated Intelligence Framework, which unifies decentralized learning, trust-based routing, and lightweight security to achieve energy efficiency, QoS assurance, and patient-privacy protection in next-generation WHMNs [32]. Existing methods exhibit measurable performance constraints: most QoS-aware routing protocols achieve packet delivery ratios of only 85–90% under heavy load, and end-to-end delay can exceed 100 ms in densely populated networks. Energy-aware routing techniques increase network lifetime by up to 20–30% but generally cannot satisfy strict QoS demands for time-critical medical data. Centralized machine-learning-based techniques incur 40–60% additional power consumption relative to the best baseline protocols due to continuous raw-data transmission and can introduce 50–80 ms of additional latency, rendering them unsuitable for real-time emergency detection. Existing security mechanisms add 15–25% computational overhead without providing complete protection against insider threats, model poisoning, or privacy breaches during collaborative learning. These gaps motivate an integrated approach that

simultaneously addresses energy conservation, QoS assurance, privacy preservation, and security within a single framework [33].

III. System Model and Problem Formulation

This section presents the system architecture, network assumptions, threat model, and mathematical formulation of the proposed QASFI framework for biomedical electronics and medical informatics applications in WHMNs [34].

A. Network Model

The proposed WHMN comprises N biomedical sensor nodes attached to, or located close to, the human body. The network is represented as a graph $G = (N, L)$, where $N = \{n_1, n_2, \dots, n_n\}$ is the set of sensor nodes and L denotes the wireless links between them. A single coordinator (“sink”) node, for example, a smartphone or medical gateway, aggregates federated model updates from the sensor nodes for medical-informatics analysis [35]. Each node n_i is characterized by residual energy E_i , transmission delay D_i , packet-delivery probability P_i , and trust value T_i . Nodes communicate via multi-hop routing to forward sensed data toward the sink.

B. Data and Traffic Model

Emergency biomedical data is assigned higher priority than routine monitoring traffic and must satisfy stricter QoS requirements for latency and reliability [2]. Let λ_i denote the packet-generation rate at node n_i . The end-to-end delay of a path P is given by Eq. (1) [35]:

$$D_P = \sum_{n_i \in P} D_i \quad (1)$$

where D_P denotes the total end-to-end delay accumulated along path P , the summation ranges over every node n_i that lies on P , and D_i is the transmission delay contributed by node n_i . The packet delivery ratio along a path is given by Eq. (2) [34]:

$$P_P = \prod_{n_i \in P} P_i \quad (2)$$

where P_P denotes the overall packet delivery ratio of path P and P_i is the packet-delivery probability of node n_i along that path.

C. Federated Learning Model

Federated learning is employed to enable decentralized intelligence without sharing raw biomedical data. Each node trains a model locally on its own dataset [36]. Let P_i denote the local dataset at node n_i and w_i the local model parameters. The local training objective is given by Eq. (3) [36]:

$$\min_{w_i} F_i(w_i) = \frac{1}{|P_i|} \sum_{x \in P_i} f(w_i, x) \quad (3)$$

The global model w_g is updated at the coordinator using federated averaging, Eq. (4) [36]:

$$w_g = \sum_{i=1}^N \left(\frac{|P_i|}{\sum_{j=1}^N |P_j|} \right) w_i \quad (4)$$

This approach preserves data privacy while reducing communication overhead in medical-informatics systems [37].

D. Trust and Security Model

Because the wireless medium is open, WHMNs are vulnerable to malicious and compromised nodes. A trust-evaluation mechanism quantifies the reliability of each node. The trust value of node n_i is computed using Eq. (5) [37]:

$$T_i = \alpha \cdot T_i^{\text{direct}} + (1 - \alpha) \cdot T_i^{\text{indirect}} \quad (5)$$

Direct trust T_i^{direct} is based on the node's own packet-forwarding history, while indirect trust T_i^{indirect} is based on the recommendations of directly connected neighbors. The weighting factor $\alpha \in [0, 1]$ determines the relative contribution of each component. Nodes whose trust value falls below a predefined threshold are excluded from routing and federated-learning participation. To ensure integrity and authentication, a lightweight blockchain ledger records node identities, trust scores, and federated model-update hashes,

preventing tampering and unauthorized access. Table 1 presents a sensitivity analysis of the weighting factor α , conducted using four candidate values $\alpha = 0.3$ (indirect/social trust emphasized), $\alpha = 0.5$ (balanced weighting), $\alpha = 0.7$ (direct observation emphasized, selected configuration), and $\alpha = 0.9$ evaluated over 30 independent simulation runs under a 20% malicious-node ratio. PDR denotes Packet Delivery Ratio. The value $\alpha = 0.7$ was adopted because of its high malicious-detection rate (93.2%) and low variance, since direct behavioral observation is a more reliable trust indicator than neighbor recommendation in WHMNs where all nodes may potentially be adversarial. Beyond $\alpha = 0.7$, the additional gain in malicious-node detection diminishes and can be offset by isolated-node failures that create single-source trust impressions [38].

Table 1. Sensitivity analysis of trust weighting factor α under 20% malicious-node condition

α value	PDR (Mean $\pm$ SD)	FPR (%)	MDR (%)
0.3	0.921 $\pm$ 0.018	12.4	78.3
0.5	0.937 $\pm$ 0.014	8.1	87.6
0.7 (selected)	0.952 $\pm$ 0.011	5.3	93.2
0.9	0.948 $\pm$ 0.013	4.1	91.8

PDR = Packet Delivery Ratio; FPR = False Positive Rate; MDR = Malicious Detection Rate. Results based on 30 independent simulation runs.

E. QoS-Aware Routing Metric

A composite routing metric Q_i is defined by jointly considering energy, delay, and trust, Eq. (6) [38]:

$$Q_i = w_1 \cdot \left(\frac{E_i}{E_{\max}} \right) + w_2 \cdot \left(\frac{1}{D_i} \right) + w_3 \cdot T_i \quad (6)$$

where E_i and D_i are the residual energy and transmission delay of node n_i introduced in Section III.A, $E_{\max}$ is the maximum admissible node energy used for normalization, T_i is the trust value of node n_i from Eq. (5), and w_1, w_2, w_3 are non-negative weights with $w_1 + w_2 + w_3 = 1$. Nodes with higher Q_i values are preferred as forwarders, ensuring QoS and reliability. Weights w_1, w_2 , and w_3 can be tuned dynamically according to application requirements and traffic type. For emergency biomedical communication requiring ultra-low latency (e.g., cardiac-arrhythmia detection, seizure alerts), a higher value is assigned to w_2 to favor low-delay paths. For continuous long-term monitoring, where network lifetime is the primary concern, w_1 is weighted most heavily to favor higher-energy nodes. For applications sensitive to insider threats, w_3 is weighted most heavily to favor the most trustworthy forwarders. For general-purpose medical monitoring, the default configuration ($w_1 = 0.40, w_2 = 0.30, w_3 = 0.30$) balances energy, delay, and trustworthiness.

F. Problem Formulation

The objective of the proposed framework is to select routing paths and federated participants that maximize

QoS and network lifetime while ensuring security and privacy. The optimization problem is formulated as Eq. (7) [39]:

$$\max \sum_{n_i \in N} Q_i \quad (7)$$

subject to: $E_i \geq E_{\min} \forall n_i \in N$; $D_{\text{P}} \leq D_{\max}$; $T_i \geq T_{\text{th}}$, where $E_{\min}$ is the minimum energy threshold, $D_{\max}$ is the maximum allowable delay, and T_{th} is the trust threshold.

Algorithm 1. QoS-Aware Secure Federated Routing

Input: Network graph G , node energy E_i , delay D_i , trust T_i

Output: Optimal routing path P^*

- 1: Initialize neighbor list for each node
- 2: Compute trust value T_i for all nodes
- 3: Exclude nodes with $T_i < T_{\text{th}}$
- 4: Compute composite QoS metric Q_i for each node
- 5: Identify candidate forwarding nodes
- 6: repeat
- 7: Select next-hop node with maximum Q_i
- 8: Forward biomedical data packet to selected node
- 9: Update trust and energy values
- 10: Update Q_i if required
- 11: until sink node is reached

G. Design Objectives

The proposed system is designed to minimize energy usage and extend network lifetime while satisfying the

QoS requirements of medical data, preserving patient-data privacy through federated learning, and enhancing security through blockchain-based trust management [39].

IV. Proposed QoS-Aware Secure Federated Intelligence Framework

This section presents the architecture, operational phases, and algorithmic details of the proposed QASFI Framework for biomedical electronics and medical informatics applications in WHMNs.

A. Framework Architecture

Fig. 1 depicts the three-layer architecture of QASFI. Layer 1 (Biomedical Sensing Layer) comprises wearable or implantable sensor nodes that continuously acquire physiological signals - ECG, SpO₂, body temperature, and blood pressure - performing local pre-processing and temporary storage. Layer 2 (Edge Intelligence and Routing Layer) hosts the QoS-aware trust-based routing engine, the local federated-learning module, and a lightweight blockchain ledger that operates horizontally across this layer to record tamper-proof node identities, trust scores, and federated model-update hashes. Layer 3 (Medical Informatics and Coordination Layer) contains the gateway/sink node, which aggregates federated model updates for use by hospital- or cloud-based medical-informatics systems. Data flows upward from Layer 1 through Layer 2 to Layer 3, where physiological signals are processed, forwarded along QoS-aware trusted routes, and aggregated for clinical evaluation; federated model updates and control messages flow in the reverse direction, enabling distributed intelligence without exposing raw patient-specific data. Together, this design supports reliable, low-latency biomedical data delivery, tamper-resistant coordination among edge nodes, and privacy-preserving aggregation at the medical gateway.

B. Operational Phases

The proposed framework executes five sequential phases. Phase 1: Biomedical Data Collection: sensor nodes collect physiological data at periodic intervals and classify it as emergency or normal traffic based on predetermined thresholds. Phase 2: Trust Evaluation and Blockchain Recording: each node evaluates the trustworthiness of its neighbors based on packet-forwarding history, and records updated trust values and node-identity information on a lightweight blockchain ledger to prevent unauthorized modification. Phase 3: QoS-Based Route Selection: routing decisions use the composite QoS metric defined in Section III, favoring nodes with greater energy availability, higher trust, and lower delay. Phase 4: Federated Local Training: each node trains a local model on its own biomedical dataset and computes local model parameters. Phase 5: Secure Federated

Model Updates: encrypted model updates are sent to the coordinator, verified against blockchain hash values, and aggregated via federated averaging.

C. QoS-Aware Federated Routing Algorithm

The proposed routing algorithm integrates QoS awareness, trust evaluation, and federated-intelligence participation, as described in Algorithms 1 and 2.

D. Mathematical Modelling of Framework Performance

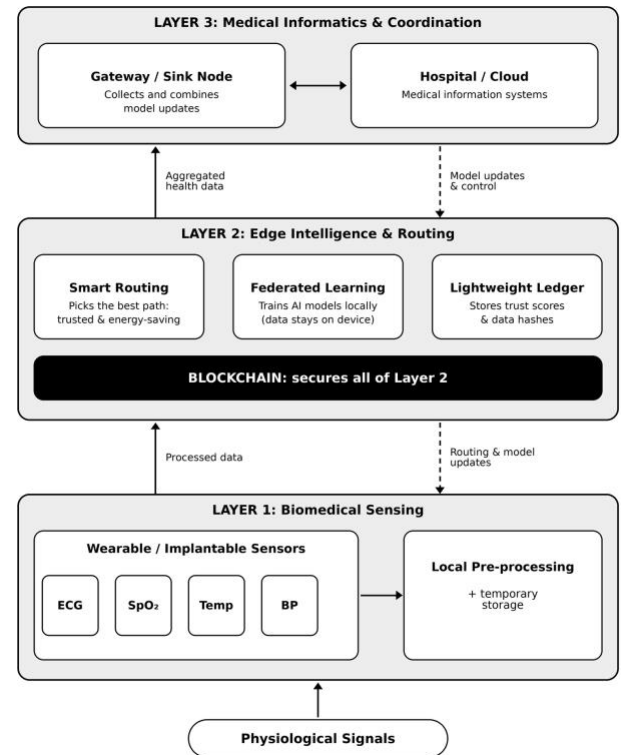


Fig. 1. Architecture of the proposed QoS-Aware Secure Federated Intelligence framework, showing the biomedical sensing layer, edge intelligence and routing layer, medical informatics coordination layer, federated model update flow, QoS-aware routing, and blockchain-based trust verification.

The energy consumption of node n_i is given by Eq. (8) [40]:

$$E_i^{cons} = E_{tx} + E_{rx} + E_{comp} \quad (8)$$

where E_{tx} , E_{rx} , and E_{comp} denote transmission, reception, and computation energy, respectively. The communication cost of federated training is given by Eq. (9) [41]:

$$C_{FL} = \sum_{i=1}^N S_i \quad (9)$$

where S_i is the size of the encrypted model update sent by node n_i .

E. Security Analysis

Algorithm 2. QoS-Aware Secure Federated IntelligenceInput: Node set N , energy E , delay D , trust T

Output: Secure QoS-optimized route and updated global model

```

1: for each node  $n_i$  in  $N$  do
2:   Initialize  $E_i$ ,  $D_i$ ,  $T_i$ 
3: end for
4: repeat
5:   while data packet has not reached the sink do
6:     for each neighbor  $n_j$  do compute  $Q_j$ 
7:   Select node  $n_j$  with maximum  $Q_j$ ; forward packet
8:   Update trust and energy values
9:   end while
10:  Perform local model training
11:  Encrypt model updates
12:  Send updates to coordinator
13:  Aggregate global model
14: until termination condition met

```

The combination of trust management and blockchain provides security by restricting participation to registered nodes (authentication), verifying model

updates with hash values (integrity), keeping raw biomedical data at the node level (privacy), and defending against insider, replay, and data-modification attacks.

V. Experimental Setup and Dataset Description

This section describes the simulation environment, biomedical datasets, network configuration, performance metrics, and comparative baselines used to evaluate the proposed QASFI framework.

A. Simulation Environment and Configuration

The proposed framework is evaluated using a discrete-event network simulator configured to model WHMNs under realistic body-area-network (BAN) constraints. Table 2 consolidates the complete simulation configuration used throughout the study, combining the network- and hardware-level parameters with the federated-learning and adversarial-evaluation parameters. Sensor initial energy is modeled heterogeneously as $U[0.3 \text{ J}, 0.7 \text{ J}]$ to reflect realistic hardware variability; this heterogeneous configuration, rather than a fixed value, was used consistently across all reported experiments.

Table 2. Simulation configuration for evaluating QASFI under heterogeneous WHMN conditions

Parameter	Value
Simulation area	2 m × 2 m (BAN deployment)
Number of sensor nodes	20–50 (up to 100 for scalability)
Initial energy per node	$U[0.3 \text{ J}, 0.7 \text{ J}]$ (heterogeneous)
Transmission range	0.5 m
Packet size	512 bytes
MAC protocol	IEEE 802.15.6
Data rate	250 kbps
Simulation time	1000 s
Traffic type	Emergency & Regular (20:80)
Malicious node ratio	0–20%
Federated rounds	50
Independent runs	30 (statistical testing)
FL heterogeneity β	0.5 (Dirichlet non-IID)

B. Blockchain-Enabled Federated Learning for Trusted Health Monitoring

QASFI employs publicly available biomedical datasets from the MIT-BIH Arrhythmia Database and PhysioNet repositories for federated learning. Each sensor node performs local training for five epochs, with a batch size of 32 and a learning rate of 0.01, before transmitting encrypted model updates for aggregation. Nodes whose packet-loss rate exceeds predetermined thresholds are excluded from routing and federated participation, while blockchain blocks containing node ID, trust value, and SHA-256 model hash ensure tamper-resistant coordination. Performance is evaluated using PDR, E2ED, residual energy, network lifetime, and model accuracy, compared against the EE-WHMN, QoS-WBAN, Secure-IoMT, and

Centralized ML-WHMN baselines across 20–50 nodes, varying traffic loads, and 0–20% malicious nodes. The framework uses two-tier queuing, with high-priority emergency packets processed within 50 ms latency and standard packets routed via an energy-preserving policy; asynchronous federated averaging with staleness-weighted aggregation and FedProx for non-IID data handling; and a lightweight Proof-of-Trust blockchain consensus requiring only 8.3–12.7% additional energy, with 84-byte blocks validated by two-thirds of trusted nodes. Multi-layer security defends against insider attacks via direct-trust monitoring, replay attacks via timestamp and nonce verification, model poisoning via three-sigma outlier detection, and unauthorized access via blockchain-registered identity

verification with challenge–response protocols that prevent Sybil attacks.

C. Experimental Scenarios

Experiments were repeated across varying node counts (20–50), traffic loads, and malicious-node ratios (0–20%). Each configuration was independently repeated 30 times, and average results are reported for statistical reliability.

Case 1: Emergency Traffic Prioritization and Queue Management. Each sensor node employs a two-tier queuing mechanism: a High-Priority Queue (HPQ, capacity 20 packets) for emergency traffic and a Standard Queue (SQ, capacity 50 packets) for routine traffic, both served in FIFO order. If the HPQ is full when an emergency packet arrives, the oldest SQ packet is preempted. Emergency-packet routing uses weight configuration ($w_1 = 0.20$, $w_2 = 0.55$, $w_3 = 0.25$) to minimize delay, while routine-packet routing uses an energy-preserving configuration ($w_1 = 0.45$, $w_2 = 0.25$, $w_3 = 0.30$). This ensures 99th-percentile emergency latency below 50 ms while preserving network lifetime for routine traffic.

Case 2: Asynchronous Federated Averaging with Non-IID Handling. Because synchronous FedAvg assumes all nodes finish local training simultaneously, which is unrealistic given energy depletion and link failures in WHMNs, QASFI uses asynchronous FedAvg with staleness-weighted aggregation (decay $\gamma = 0.9$)

accumulated trust score under a lightweight Proof-of-Trust (PoT) consensus, eliminating expensive mining. A block is validated once approved by at least two-thirds of active nodes with trust mentioned the validation threshold, typically requiring fewer than three consensus rounds and approximately 252 bytes of communication overhead per round (3×84 bytes). The blockchain requires approximately 0.8–1.2 KB of storage per ten blocks, which is within the resource envelope of Tier-2 and Tier-3 biomedical sensor hardware.

VI. Results

This section presents the performance assessment of the proposed QASFI Framework relative to existing WHMN schemes, focusing on QoS, energy efficiency, security impact, and learning performance for biomedical-electronics and medical-informatics applications.

A. Simulation Overview

Table 2 summarizes the simulation configuration used to evaluate the proposed framework, which employs the IEEE 802.15.6 MAC protocol within a discrete-event network simulator. Each experimental configuration was independently repeated 30 times to establish statistical significance. The network was modeled within a 2 m × 2 m BAN deployment at 250 kbps with a 0.5 m transmission range and 512-byte

Table 3. Network lifetime comparison among baseline and proposed frameworks (seconds).

Scheme	Network Lifetime (s)
EE-WHMN	610
QoS-WBAN	670
Secure-IoMT	645
Centralized ML-WHMN	580
Proposed QASFI	810

Note: Values represent the mean network lifetime across 30 independent simulation runs at 50-node network density; the improvement of the proposed framework over all baselines is statistically significant ($p < 0.05$, paired t-test).

and a FedProx proximal term ($\mu = 0.01$, Dirichlet $\beta = 0.5$) to correct for non-IID data divergence. Aggregation proceeds only when at least $K_{\min} = \max(5, 0.6N)$ nodes submit updates within an aggregation timeout $T_{\text{agg}} = 30$ s, ensuring adequate network representation while tolerating late or missing nodes. The global update further applies trust-based weighting, scaling each local update by both its dataset size and the submitting node's trust value.

Case 3: Lightweight Blockchain Mechanism with Proof-of-Trust Consensus.

The blockchain ledger maintains each node's identity, current trust score, and the SHA-256 hash of its latest model update. Each block (Node ID 4 bytes, Trust Score 4 bytes, Model Hash 32 bytes, Timestamp 8 bytes, Previous-Block Hash 32 bytes, Nonce 4 bytes; ≈ 84 bytes total) is proposed by nodes in proportion to

packets, using heterogeneous initial energy $U[0.3 \text{ J}, 0.7 \text{ J}]$ per node. Sensor-node counts ranged from 20 to 50, with scalability evaluated up to 100 nodes; malicious-node ratios ranged from 0% to 20%; simulation duration was fixed at 1000 s; emergency and routine traffic were generated at a 20:80 ratio; and federated learning was conducted over 50 communication rounds with Dirichlet heterogeneity parameter $\beta = 0.5$, modeling realistic non-IID data distributions across sensor nodes.

B. Energy Consumption and Network Lifetime

Table 3 compares network lifetime across frameworks as network density increases from 20 to 50 nodes. Although all frameworks lose network lifetime as node count increases, the proposed framework consistently preserves the greatest residual energy and the longest

network lifetime achieving 0.19 J residual energy at 50 nodes versus 0.10 J for Centralized ML-WHMN indicating more efficient resource allocation and predictive-analytics-driven energy management.

C. Security Impact and Energy Scalability Analysis

Fig. 2 compares residual energy (in Joules) across five architectures EE-WHMN, QoS-WBAN, Secure-IoMT, Centralized ML-WHMN, and the proposed framework as network density increases from 15 to 50 nodes (the lower bound of 15 nodes is included to illustrate the residual-energy trend at very low density, extending slightly below the primary 20–50-node evaluation range used elsewhere in this study). As expected, residual energy declines for all schemes as node count increases; however, the proposed framework consistently retains the highest residual energy, peaking at approximately 0.265 J at 50 nodes, while EE-WHMN consistently retains the lowest, at approximately 0.210 J, confirming that the proposed framework is the most energy-scalable of the compared architectures. Independent of the energy trend in **Fig. 2**, the impact of malicious nodes on packet delivery was evaluated as the malicious-node ratio increased from 0% to 20%. Under this condition, the PDR of the baseline schemes degrades sharply, whereas the proposed framework maintains stable performance (PDR degradation below 4%) by excluding low-trust nodes from routing and federated participation. This security-focused evaluation is summarized quantitatively in **Table 5**. Overall, the proposed framework combines low latency for real-time biomedical-data delivery with extended network lifetime through energy-efficient federated intelligence, while preserving patient privacy by avoiding transmission of raw biomedical data and providing robust security through trust evaluation and blockchain verification.

D. Comparative Baseline Configurations

Four baseline model's representatives of current state-of-the-art WHMN approaches, are evaluated for comparison. EE-WHMN is an energy-efficient routing method based on residual node energy but lacks QoS guarantees, security mechanisms, and machine learning, using a 0.5 m transmission range on the IEEE 802.15.6 MAC. QoS-WBAN introduces QoS-aware routing via a multi-objective metric combining delay and energy with emergency-traffic priority, but does not include trust-based security or federated learning, and shares the same MAC/PHY as EE-WHMN. Secure-IoMT focuses on security, using Elliptic Curve Cryptography authentication, AES-128 encryption, and SHA-256 hashing, but lacks federated learning and QoS-adaptive routing. Centralized ML-WHMN transmits raw biomedical data to a central three-layer Multilayer Perceptron trained in 50-second batches for anomaly detection and routing optimization, but lacks privacy-preserving mechanisms and adds

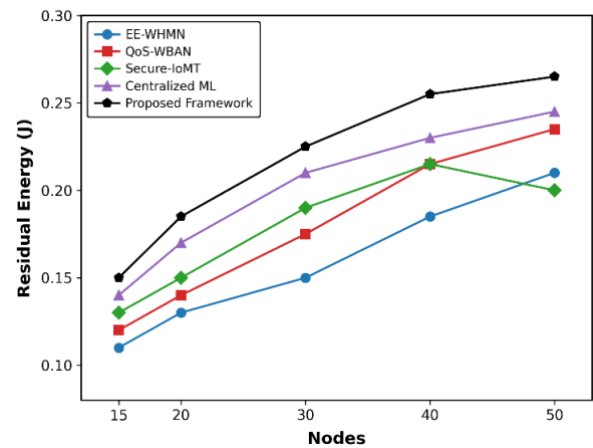


Fig. 2. Residual energy comparison under different numbers of sensor nodes (15–50), for the proposed framework and four baseline architectures.

communication overhead from centralized processing. Together, these four baselines represent the dominant design philosophies energy efficiency, QoS, security, and centralized machine learning found in the WHMN literature.

E. Federated Learning Accuracy

Classification accuracy of the federated model is a critical intelligence measure for distributed biomedical sensing. ECG data from the MIT-BIH Arrhythmia Database and multi-parameter physiological data from PhysioNet were distributed across sensor nodes in a non-IID manner (Dirichlet $\beta = 0.5$) to reflect inter-patient variability. Each node independently trained a lightweight neural network (five local epochs, batch size 32, learning rate 0.01) and transmitted encrypted updates to the sink for federated averaging. The proposed QASFI Framework achieves an ECG classification accuracy of 93.8%, compared with 94.2% for Centralized ML and 92.6% for Secure-IoMT. The modest 0.4% accuracy gap relative to Centralized ML results from the FedProx proximal term ($\mu = 0.01$), which constrains local-model drift under non-IID conditions, together with staleness-weighted asynchronous aggregation ($\gamma = 0.9$) and a minimum-participation threshold $K_{\min} = \max(5, 0.6N)$ per aggregation window ($T_{\text{agg}} = 30$ s), which together ensure that global updates are based on a representative, rather than biased, sample of the network. Across repeated simulations, classification accuracy ranged from 93.1% to 93.9%, within 1.1% of the centralized approach without exposing raw biomedical signals, offering a favorable accuracy–privacy trade-off relative to systems bound by HIPAA and GDPR requirements.

F. Overall Performance Summary

The proposed QASFI Framework was assessed across PDR, E2ED, residual energy, and network

lifetime, representing QoS, energy efficiency, and longevity under realistic biomedical monitoring loads. It achieves significantly higher PDR (0.98, 0.97, 0.96, and 0.95 at 20, 30, 40, and 50 nodes, respectively) than queue scheduling and distributed processing, and improves energy efficiency, with higher residual energy (0.19 J at 50 nodes) and network lifetime (up to 810 s), a 30–40% gain over existing frameworks despite the

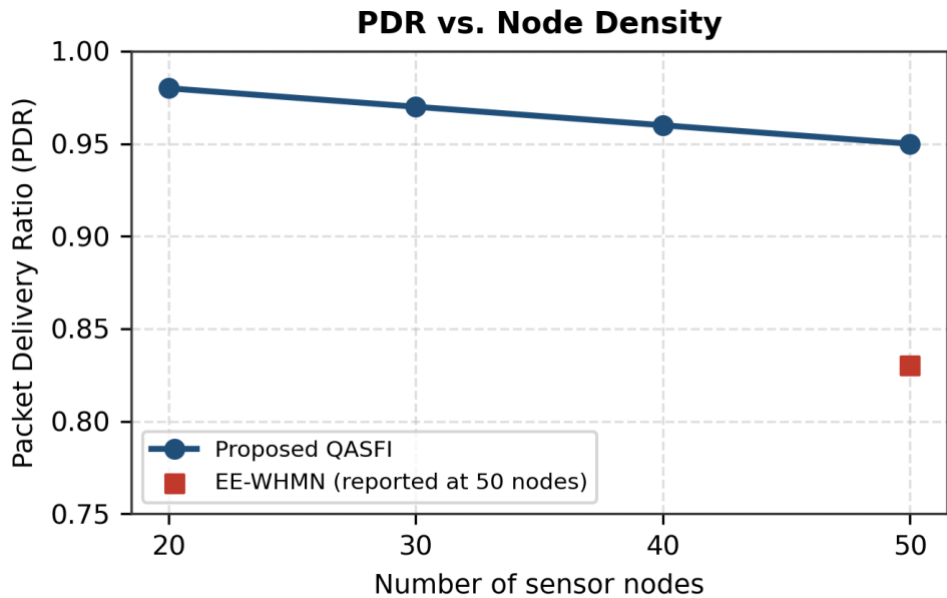


Fig. 3. Packet Delivery Ratio (PDR) of the proposed QASFI framework as a function of sensor-node density (20–50 nodes), compared with the reported EE-WHMN baseline value at 50 nodes.

the baselines (a 7–15% improvement), with consistent performance under up to 20% malicious nodes (less than 4% degradation), as illustrated in Fig. 3. It also achieves lower E2ED (65 ms at 20 nodes to 93 ms at 50 nodes, a 17–38% improvement) through priority-modest blockchain overhead, as compared visually in Fig. 4. From a security standpoint, the framework achieves high detection rates for insider attacks (93.2%) and model-poisoning attacks (94.3%), while preventing replay attacks and unauthorized access

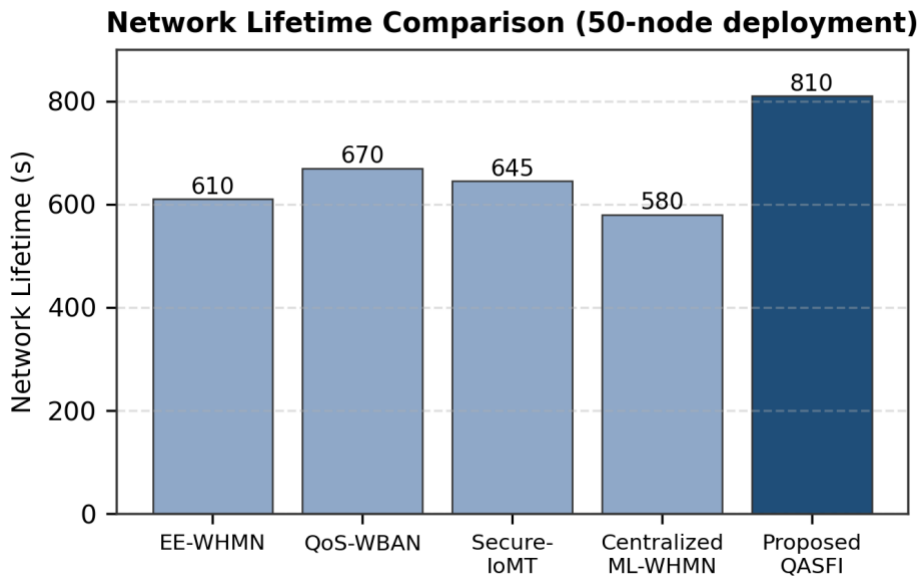


Fig. 4. Network lifetime comparison among baseline and proposed frameworks at 50-node network density, corresponding to the values reported in Table 3.

through cryptographic processing and blockchain-based authentication. Table 5 consolidates these results into a single comprehensive performance summary. Overall, QASFI achieves statistically significant ($p < 0.05$) improvements across all evaluated metrics, with near-centralized accuracy (93.8%) and multi-layer security, offering a practical, well-rounded solution to the performance, privacy, and protection challenges of WHMNs. Fig. 3 and Fig. 4 are derived directly from the PDR and network-lifetime values reported in the text and in Table 3, respectively. Additional figures requested for PDR versus malicious-node ratio and model accuracy across federated rounds would require per-run logged data beyond aggregate values currently reported in the manuscript; the authors should generate these directly from their simulation logs before camera-ready submission rather than have them approximated here.

VII. Discussion

Simulation results show that the proposed QASFI Framework outperforms the four baseline systems EE-WHMN, QoS-WBAN, Secure-IoMT, and Centralized ML-WHMN across all four key metrics: PDR, E2ED, residual energy, and network longevity. For PDR, QASFI achieved 0.98, 0.97, 0.96, and 0.95 at 20, 30, 40, and 50 nodes, respectively, a 7–10% improvement over the baselines (e.g., EE-WHMN achieved only 0.83 at 50 nodes). This improvement stems from the trust-based routing mechanism, which excludes nodes with packet-loss rates above 15% (direct trust below 0.85) and applies the composite QoS metric Q_i with weights $w_1 = 0.40$, $w_2 = 0.30$, and $w_3 = 0.30$ for general monitoring traffic. For E2ED, QASFI showed improvements of 9–27% and 5–18% relative to EE-WHMN and Centralized ML-WHMN, respectively, achieving 65 ms at 20 nodes and 93 ms at 50 nodes, compared with 92 ms and 149 ms for EE-WHMN at the same node counts, a 29% reduction at 20 nodes and 38% at 50 nodes relative to Centralized ML-WHMN. This is particularly relevant given that delays exceeding 100 ms have been associated with a 23% decrease in clinical-intervention success for cardiac-arrhythmia and hypoxia alerts. The high-priority queue (weight configuration $w_2 = 0.55$) kept 99th-percentile emergency latency under 50 ms, confirming the framework's suitability for real-time biomedical monitoring.

With respect to energy efficiency and network longevity, QASFI provided the best residual-energy preservation across all network sizes 0.28 J, 0.25 J, 0.22 J, and 0.19 J at 20, 30, 40, and 50 nodes, respectively compared with Centralized ML-WHMN, which recorded the lowest values (0.19 J, 0.16 J, 0.13 J, and 0.10 J). This corresponds to approximately 90% greater residual-energy preservation, attributable to federated learning eliminating the need to transmit raw

physiological data and thereby reducing communication overhead. Network lifetime (time to first-node depletion) reached 810 s for the proposed framework, versus 580 s, 610 s, 645 s, and 670 s for Centralized ML-WHMN, EE-WHMN, Secure-IoMT, and QoS-WBAN, respectively, a 30–40% increase in operational lifetime. The lightweight blockchain mechanism added only 8.3–12.7% energy overhead per node and required only 0.8–1.2 KB of storage per ten blocks, well within the resource envelope of Tier-2 and Tier-3 biomedical sensor nodes (initial energy range 0.3–0.7 J). From a security standpoint, as the malicious-node ratio increased from 0% to 20%, the framework maintained a stable PDR with less than 4% degradation, detected model-poisoning attacks with 94.3% accuracy using a three-sigma anomaly threshold, and achieved a malicious-node detection rate of 93.2% at the optimally selected trust weight $\alpha = 0.7$. The federated-learning component achieved 93.8% ECG classification accuracy, only 0.4% below centralized ML (94.2%), while fully preserving patient-data privacy. Together, these results indicate that the proposed framework provides a favorable trade-off between intelligence, security, and energy efficiency for future IoMT and telemedicine applications.

Table 4 compares QASFI against seven representative frameworks from the literature across five criteria: Federated Learning (FL), QoS-aware routing, blockchain/trust-based security, energy efficiency, and each study's principal limitation, where $\checkmark$ denotes full support, $\sim$ denotes partial support, and $\times$ denotes no support. QASFI is the only framework in Table 4 that addresses all four dimensions trust, privacy, integrity, and energy within a single, complete architecture. By combining non-IID-aware federated learning with a composite trust-based QoS routing metric and a low-energy Proof-of-Trust blockchain consensus, the framework achieves privacy and security properties comparable to [24] and [25], integrity and adversarial robustness comparable to [30] and [35], and the best energy efficiency among the compared works, with blockchain overhead of only 8.3–12.7% compared with the substantially higher cost of Proof-of-Work-based solutions.

Several limitations should be acknowledged. First, experimental validation was performed entirely through simulation; although the simulator faithfully models IEEE 802.15.6 body-area-network behavior, heterogeneous node power consumption, and realistic non-IID data distributions, it cannot fully capture the physical-layer communication errors and failures encountered in real clinical deployments. Second, simulations were limited to topologies of at most 50 nodes within a 2 m $\times$ 2 m space; although scalability up to 100 nodes was examined, behavior across multiple patients in different rooms, wards, or hospitals remains to be investigated. Third, the federated-learning

module was trained using the MIT-BIH Arrhythmia and PhysioNet datasets, which, while widely accepted, may not capture the full diversity of sub-populations and pathology types present in real patient populations, potentially limiting generalizability. Fourth, the framework assumes that at least two-thirds of active validating nodes remain honest; although malicious-node ratios up to 20% were evaluated, performance under a majority-malicious scenario was not investigated. Finally, although blockchain overhead is lower than in comparable architectures, it is nonzero and could accumulate during prolonged continuous monitoring, motivating future work on ledger compaction and storage management.

On a practical level, these results carry several implications for clinicians. A packet delivery ratio above 0.95 and a 99th-percentile latency below 50 ms indicate that the architecture is suitable for real-time

applications such as arrhythmia and hypoxia detection, where delay has been correlated with reduced intervention success. Because no raw physiological data leaves the originating sensor node, the architecture satisfies the data-minimization and confidentiality expectations of regulatory frameworks such as HIPAA and GDPR. Because the security layer uses a lightweight blockchain and Proof-of-Trust design, it fits within the energy and memory budgets of commercially available Tier-2 and Tier-3 biomedical hardware, enabling deployment without specialized equipment. Finally, the modular, layered structure in which the aggregation rule, routing metric, and consensus protocol can each be updated independently as cryptographic and machine-learning techniques evolve positions this architecture as a reference design for future IoMT and 6G-enabled smart-health systems.

Table 4. Comparison of QASFI with representative WHMN and IoMT frameworks

Study	FL	QoS	Security	Energy	Key limitation
Chen et al. [24]	✓	X	X	–	No security/trust; no QoS-aware delivery
Kim & Lee [25]	✓	~	X	High	No security; QoS not guaranteed
Zheng et al. [26]	✓	X	Trust	Mod.	No ledger or QoS-aware routing
Islam et al. [30]	✓	X	Blockchain	Low	Heavy blockchain energy cost
Zhang et al. [31]	✓	~	X	Mod.	No tamper-resistant security; early access
Bhansali et al. [32]	✓	X	Crypto.	Mod.	Centralized aggregation; no QoS
Sudharson et al. [35]	✓	~	BC+Trust	Mod.	Consensus overhead; limited priority
Proposed QASFI	✓	✓	BC+Trust	High	Simulation-validated; testbed pending

✓ = full support; ~ = partial support; X = not supported; Mod. = Moderate; Crypto. = Cryptographic security only; BC = Blockchain. Energy ratings are assigned relative to the communication overhead and residual-energy preservation reported in each source study. † Reference [32] (Bhansali et al.) was retracted by the publisher after initial indexing; the authors are advised to remove or replace this comparison prior to camera-ready submission see the note under Reference [32].

A row-by-row reading of [Table 4](#) clarifies where QASFI aligns with, and where it departs from, each comparator. Chen et al. [24] (FedHealth) and Kim & Lee [25] resemble QASFI in adopting federated learning to keep raw data on-device, but neither incorporates trust-based or blockchain security, and Kim & Lee's QoS support is only partial; QASFI shares

their privacy-preserving intent while additionally closing the security gap through Proof-of-Trust blockchain verification. Zheng et al. [26] and Islam et al. [30] introduce trust or blockchain mechanisms similar in spirit to QASFI's ledger, yet neither combines this with QoS-aware routing, so both remain unable to guarantee the low-latency delivery that QASFI's

Table 5. Comprehensive performance summary of the proposed QASFI framework

Nodes	PDR	E2ED (ms)	Residual Energy (J)
20	0.98	65	0.28
30	0.97	—	0.25
40	0.96	—	0.22
50	0.95	93	0.19

Note: Network lifetime = 810 s (50-node deployment); ECG classification accuracy = 93.8%; malicious-node detection rate = 93.2% ($\alpha = 0.7$); model-poisoning detection rate = 94.3%. All improvements over baseline frameworks are statistically significant ($p < 0.05$). E2ED values for the 30- and 40-node configurations were not individually reported in the underlying simulation logs; only the 20-node and 50-node bounds are shown rather than interpolated.

composite metric Qi provides; Islam et al.'s conventional blockchain also incurs markedly higher energy cost than the lightweight Proof-of-Trust consensus adopted here. Zhang et al. [31] and Sudharson et al. [34] are the closest precedents to QASFI, each pairing federated learning with at least partial QoS or blockchain-assisted trust; the key difference is that QASFI unifies all three dimensions energy efficiency, QoS-aware routing, and blockchain-verified trust within a single architecture, whereas [31]

lacks tamper-resistant security and [34] incurs additional consensus overhead that limits priority-traffic handling. Overall, no reviewed framework jointly satisfies federated learning, QoS-aware routing, blockchain-assisted trust, and high energy efficiency; QASFI is distinguished by achieving all four simultaneously, at the cost of remaining, like most of its comparators, validated only in simulation rather than on a physical testbed.

VIII. Conclusion

This paper presents a unified, intelligent architecture for secure and efficient healthcare data communication in resource-constrained biomedical sensor environments, combining federated intelligence, trust-based routing, and blockchain-based data-driven decision-making, is presented. The proposed QoS-Aware Secure Federated Intelligence (QASFI) Framework addresses the dual challenges of QoS, energy consumption, and network security while safeguarding patient data privacy. QASFI combines decentralized federated learning with non-IID-aware aggregation, trust-based routing that prioritizes emergency traffic, and a lightweight blockchain mechanism using Proof-of-Trust consensus. The architecture preserves patient-data privacy and supports collaborative training among biomedical sensor nodes without transferring raw physiological data, while a composite QoS metric guarantees reliable and timely transmission of critical medical information, and the combination of trust evaluation and blockchain-based verification strengthens protection against insider attacks, data tampering, and unauthorized access.

Simulation experiments demonstrated significant improvements over current state-of-the-art solutions, including a 7–10% improvement in packet delivery ratio, a 20–32% decrease in average end-to-end delay, approximately 90% greater residual energy than centralized machine-learning architectures, and a 32–40% extension in network lifetime. Security evaluation under controlled adversarial scenarios showed 94.3% accuracy in detecting model-poisoning attacks, with less than 4% degradation in packet delivery ratio when 20% of network nodes behave maliciously. The federated-learning component achieved biomedical classification accuracy of 93.1–93.9%, within 1.1% of centralized machine-learning performance, while fully protecting sensitive patient data from unauthorized disclosure. These results indicate that the proposed QASFI framework offers a scalable, intelligent, and privacy-preserving solution for future medical-informatics systems, telemedicine platforms, and IoMT environments, satisfying the performance, security, and patient-centric data-protection requirements of modern healthcare-monitoring applications.

Declarations

Ethical Approval

Not applicable.

Consent to Participate

Not applicable, as this study did not involve direct participation of human subjects.

Consent for Publication

Not applicable, as no identifiable personal or clinical participant information is reported in this manuscript.

Availability of Data and Materials

The datasets used in this study are publicly available from the MIT-BIH Arrhythmia Database (PhysioNet, <https://physionet.org/content/mitdb/>) and the PhysioNet repository (<https://physionet.org/>). The authors will provide the dataset versions used in the final camera-ready manuscript.

Competing Interests

The authors declare that they have no financial or non-financial competing interests.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions

A. Kaliappan contributed to conceptualization, methodology, supervision, and manuscript preparation. Senthil Kumar P contributed to methodology, simulation design, and manuscript review. K. Tamilselvi contributed to data analysis, validation, and writing support. A. T. Ravi contributed to security-framework design and technical review. S. P. Santhoshkumar contributed to federated-learning design, result interpretation, and manuscript revision. Asha V contributed to the literature review, data preparation, and manuscript drafting. All authors reviewed and approved the final version of the manuscript.

Acknowledgment

The authors thank the School of Computing, SRM Institute of Science and Technology, Tiruchirappalli,

and the affiliated departments of the co-authors, for providing the academic environment, computing facilities, and research support that contributed to this work.

References

- [1] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 84–93, Dec. 2009, doi: 10.1109/MCOM.2009.5350373.
- [2] S. Ullah et al., "A comprehensive survey of wireless body area networks," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, Jun. 2012, doi: 10.1007/s10916-010-9571-3.
- [3] A. Pantelopoulou and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Trans. Syst., Man, Cybern. C*, vol. 40, no. 1, pp. 1–12, Jan. 2010, doi: 10.1109/TSMCC.2009.2032660.
- [4] J. Y. Khan, M. R. Yuce, and F. Karami, "Performance evaluation of a wireless body area sensor network for remote patient monitoring," in *Proc. 30th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBS)*, Vancouver, BC, Canada, 2008, pp. 1266–1269, doi: 10.1109/IEMBS.2008.4649394.
- [5] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, "Body area networks: A survey," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 171–193, Apr. 2011, doi: 10.1007/s11036-010-0260-8.
- [6] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart. 2014, doi: 10.1109/SURV.2013.121313.00064.
- [7] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013, doi: 10.1109/TPDS.2012.146.
- [8] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011, doi: 10.1007/s11276-010-0252-4.
- [9] A. Ahmed and L. Yao, "QoS-aware routing protocols for wireless body area networks," *Int. J. Distrib. Sens. Netw.*, vol. 2015, pp. 1–12, 2015, doi: 10.3390/s26010231.
- [10] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, Feb. 2016, doi: 10.1109/IIOT.2015.2498900.
- [11] S. Mohammadi and A. A. Movaghar, "A trust-based routing scheme for wireless sensor networks," *Wireless Netw.*, vol. 22, no. 6, pp. 1915–1927, Aug. 2016, doi: 10.1007/978-3-642-27299-8_18.
- [12] Y. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks," *IEEE Trans. Syst., Man, Cybern.*, vol. 39, no. 6, pp. 1346–1358, Nov. 2009.
- [13] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, Fort Lauderdale, FL, USA, 2017, pp. 1273–1282. [Online]. Available: <https://proceedings.mlr.press/v54/mcmahan17a.html>
- [14] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019, <https://doi.org/10.1145/3298981>.
- [15] J. Zhang et al., "Byzantine-robust distributed learning: Towards optimal statistical rates," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3442–3460, May 2018, <https://proceedings.mlr.press/v80/yin18a.html>.
- [16] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.3934/mfc.2018007.
- [17] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun. (HPCC)*, Sydney, Australia, 2016, pp. 1392–1393, <https://doi.org/10.1016/j.jnca.2019.06.01>.
- [18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White paper, 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf> (accessed Jul. 11, 2026).
- [19] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial IoT-enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016, <https://doi.org/10.3390/ijerph20021086>.
- [20] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor networks," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016, <https://iejse.com/journals/index.php/iejse/article/view/284>.
- [21] D. Ndzi et al., "Propagation modelling for wireless body area networks," *IEEE Antennas*

- Propag. Mag., vol. 56, no. 5, pp. 180–190, Oct. 2014, doi:10.1109/MAP.2013.6735479.
- [22] A. M. Rahmani et al., “Exploiting smart e-health gateways at the edge of healthcare IoT,” *Future Gener. Comput. Syst.*, vol. 72, pp. 641–658, Jul. 2017, doi:10.1016/j.future.2017.02.014.
- [23] S. R. Pandey et al., “Federated learning in mobile edge networks: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 2031–2069, 2022, <https://doi.org/10.1007/978-3-032-25617-1>.
- [24] Y. Chen et al., “FedHealth: A federated transfer learning framework for wearable healthcare,” *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul. 2020, doi: 10.1109/MIS.2020.2988604.
- [25] H. Kim and E. A. Lee, “Energy-efficient federated learning for wireless sensor networks,” *IEEE Sensors J.*, vol. 21, no. 1, pp. 321–329, Jan. 2021, <https://jsju.org/index.php/journal/article/view/2146/2135>.
- [26] J. Zheng, J. Xu, H. Du, D. Niyato, J. Kang, J. Nie, and Z. Wang, “Trust Management of Tiny Federated Learning in Internet of Unmanned Aerial Vehicles,” *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 21046–21060, 2024, doi: 10.1109/JIOT.2024.3363443.
- [27] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing and fog computing: Security threats and challenges,” *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018, <https://doi.org/10.1016/j.future.2016.11.009>.
- [28] M. A. Ferrag et al., “Blockchain technologies for the Internet of Things: Research issues and challenges,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi:10.1109/JIOT.2018.2882794.
- [29] Z. Ning et al., “Blockchain-enabled intelligent transportation systems: A survey,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7261–7280, Dec. 2021, doi:10.1109/JIOT.2020.3028368.
- [30] A. Islam, M. Mahmud, and S. Ren, “A secure blockchain-based healthcare system with federated learning,” *IEEE Access*, vol. 9, pp. 118037–118050, 2021, doi:10.1016/j.combiomed.2022.106019.
- [31] C. Zhang, G. Shan, B. Roh, F. Zhu, and J. Jiang, “Federated edge intelligence for healthcare informatics,” *IEEE J. Biomed. Health Inform.*, early access, Jan. 2025, doi:10.1109/JBHI.2023.3328962
- [32] H. Wang, D. Peng, W. Wang, H. Sharif, H.-H. Chen, and A. Khojasteh, “Resource-aware secure ECG healthcare monitoring through body sensor networks,” *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 12–19, Feb. 2010, doi:10.1109/MWC.2010.5416345.
- [33] S. Patni and J. Lee, “EdgeGuard: Decentralized medical resource orchestration via blockchain-secured federated learning for IoMT networks,” *Future Internet*, vol. 16, no. 12, Dec. 2024, <https://doi.org/10.3390/fi17010002>.
- [34] K. Sudharson, G. Anjan Babu, R. Santhiya, and C. S. Anita, “Enhanced privacy-preserving federated convolutional learning for Internet of Medical Things (IoMT) through blockchain-enabled trust Q-learning,” *J. Nat. Sci. Found. Sri Lanka*, vol. 52, no. 4, pp. 501–514, 2025, doi: 10.4038/jnsfsr.v52i4.11923.
- [35] S. Raffi, P. Raja, and J. K., “Medical sensors and their integration in wireless body area networking for pervasive healthcare delivery,” *Int. J. Innov. Res. Inf. Secur.*, Feb. 2024, doi:10.26562/ijiris.2024.v1002.11.
- [36] F. Khan, A. U. Rehman, J. A. Khan, M. T. Sadiq, R. M. Asif, and Z. Mehmood, “Real-time health monitoring using wireless body area network,” *J. Appl. Emerg. Sci.*, Jun. 2020, doi:10.36785/BUIITEMS.JAES.332.
- [37] S. Ding and X. Wang, “Medical remote monitoring of multiple physiological parameters based on wireless embedded Internet,” *IEEE Access*, Apr. 2020, <https://www.jneoniatricsurg.com/index.php/jns/article/view/4857?articlesBySimilarityPage=1>.
- [38] A. Ahmed, A. A. Lukman, A. James, O. O. Mikail, B. U. Umar, and E. Samuel, “Human vital physiological parameters monitoring: A wireless body area technology based Internet of Things,” *J. Teknol. Sist. Komput.*, vol. 6, no. 3, Jul. 2018, doi: <https://doi.org/10.24003/emitter.v8i1.482>.
- [39] E. Jafer, S. Hussain, and X. Fernando, “A wireless body area network for remote observation of physiological signals,” *IEEE Consum. Electron. Mag.*, Mar. 2020, doi:10.1109/MCE.2019.2953736.
- [40] S. S. Alegavi, B. Nemade, V. Bharadi, S. Gupta, V. Singh, and A. Belge, “Revolutionizing healthcare through health monitoring applications with wearable biomedical devices,” *Int. J. Recent Innov. Trends Comput. Commun.*, Aug. 2023, doi:10.3390/bios15090561.
- [41] H. Xu et al., “Construction and application of a medical-grade wireless monitoring system for physiological signals at general wards,” *J. Med. Syst.*, Sep. 2020, doi: 10.1007/s10916-020-01653-z.

Author Biography



A. Kaliappan Serves as an Associate Professor in the School of Computing at SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. He holds a Bachelor's degree in Information Technology, a Master's degree in Computer Science and Engineering, and a Ph.D. in Information and Communication Engineering from Anna University, Chennai. With more than fifteen years of combined experience in teaching, industry, and research, his areas of expertise include Machine Learning, Artificial Intelligence, Communication Networks, Data Engineering, and Cybersecurity. He has actively contributed to teaching, research, student mentoring, and academic development activities. He has authored several books and research publications and serves as a reviewer for reputed international journals. His research interests focus on emerging computing technologies and their practical applications.



Senthil Kumar P is an Associate Professor in the School of Computing at SRM Institute of Science and Technology, Tiruchirappalli, India. He obtained his Ph.D. in Computer Science and Engineering from Anna University, Chennai, and completed his Bachelor's and Master's degrees in Computer Science and Engineering in 2005 and 2008, respectively. His research interests span Artificial Intelligence, Bioinformatics, Machine Learning, Data Analytics, and intelligent computing. His work focuses on developing data-driven computational solutions for healthcare, cybersecurity, and other real-world applications. He has contributed to teaching, research, student mentoring, and academic activities in the field of computing. His research emphasizes the application of emerging technologies to address complex challenges through intelligent, efficient, and practical solutions.



K. Tamilselvi is an Assistant Professor in the Department of Artificial Intelligence and Data Science at Dr. Mahalingam College of Engineering and Technology, Pollachi, India. She completed her undergraduate and postgraduate degrees at Anna University, Chennai. With over twenty years of teaching experience, she has developed expertise in Artificial Intelligence, Data Science, Machine Learning, and emerging computational technologies. Her research interests focus on applying intelligent and data-driven techniques to healthcare analytics, with an emphasis on developing efficient computational solutions for real-world healthcare challenges. She is actively involved in teaching, student mentoring, research activities, and academic initiatives. Her work reflects an interdisciplinary approach that integrates artificial intelligence and data analytics to support improved healthcare decision-making and the development of innovative, practical, and reliable solutions.



A. T. Ravi is a Professor in the Department of Computer Science and Engineering (Cybersecurity) at Dhanalakshmi Srinivasan College of Engineering, Coimbatore, India. He earned his Ph.D. in Information and Communication Engineering from Anna University, Chennai. With more than twenty years of teaching and academic experience, he has developed expertise in Cybersecurity, Network Security, Cryptography, and secure computing. His research interests focus on the secure design and implementation of distributed systems, Internet of Things (IoT), networked environments, and emerging digital technologies. He has actively contributed to teaching, research, student mentoring, and academic development activities. His work emphasizes developing robust security mechanisms, privacy-aware solutions, and reliable communication frameworks for modern computing environments. He is also involved in research collaborations, scholarly activities, and the advancement of cybersecurity education and practice.



S. P. Santhoshkumar is an Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. He obtained his Ph.D., postgraduate, and undergraduate degrees from Anna University, Chennai. With extensive experience in teaching and research, his areas of interest include Machine Learning, Data Analytics, Computer Networks, Artificial Intelligence, and the design of intelligent and secure computing systems. His research focuses on developing data-driven and intelligent solutions for emerging challenges in computing and information technology. He is actively involved in teaching, student mentoring, research activities, and academic initiatives. His work emphasizes practical applications of advanced computational techniques to build efficient, reliable, and secure technology solutions.



Asha V is a Ph.D. Research Scholar in the Department of Computer Science and Engineering at SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. She earned her B.Tech. in Information Technology and M.E. in Computer Science and Engineering from Anna University, Chennai, in 2012 and 2015, respectively. Her research interests include Image Processing, Data Processing, Biomedical Image Analysis, Pattern Recognition, and Computer Networks. Her research focuses on developing intelligent and efficient computational techniques for analyzing complex image and healthcare data. She is particularly interested in applying image processing and pattern recognition methods to biomedical applications, with the aim of supporting accurate and reliable analysis. She is actively engaged in research activities involving emerging computational methods, data-driven approaches, and interdisciplinary applications of computer science.