

PoPEA: an energy and latency-optimized proof-of-processing framework for trusted end-edge-cloud healthcare analytics

Rana Hassam Ahmed¹, Amir Mohammad Delshadi², Naseer Ahmad³, Muhammad Danish Rasheed⁴, Osamah Ibrahim Khalaf^{5*}, Muhammad Sarfraz Khan⁶, Majid Hussain¹, Rajesh Sikder⁷

¹Department of Computer Science, The University of Faisalabad, Pakistan

²New Mexico Highlands University, United States of America

³Department of Computer Science - Artificial Intelligence, Lewis University, United States of America

⁴Department of Information Technology, Berkeley City College, United States of America

⁵Al-Nahrain Renewable Energy Research Center, Al-Nahrain University, Iraq

⁶Electrical and Computer Engineering Department, University of New Mexico, United States of America

⁷Information Technology, University of the Cumberlands, United States of America

Abstract

In smart healthcare, continuous patient monitoring relies on streaming analytics across end, edge, and cloud layers. While edge computing enables low-latency analytics, ensuring that potentially untrusted nodes perform analytics correctly remains a significant challenge. We propose PoPEA-BC, a blockchain-enabled Proof-of-Processing framework combining Trusted Execution Environments (TEEs), succinct zero-knowledge proofs (zk-proofs), and distributed ledger technology (DLT) to cryptographically verify that prescribed analytics were executed as intended and immutably record proofs for auditability. PoPEA-BC introduces an operator-level proof library for common healthcare stream analytics, including ECG feature extraction and arrhythmia detection, and a hybrid MILP/Reinforcement Learning-based scheduler that optimizes latency, energy consumption, and proof generation overhead under intermittent connectivity. Blockchain provides a tamper-proof, decentralized verification layer for storing computation proofs, enabling post hoc validation by authorized healthcare stakeholders without relying on a single trusted authority. Evaluation on real ECG and SpO2 anomaly detection workloads demonstrates that PoPEA-BC achieves verifiable processing with <8% additional latency, reduces energy consumption by up to 24% compared with TEE-only baselines, and remains resilient against Byzantine edge nodes. These results highlight PoPEA-BC's potential as a foundational layer for trustworthy, auditable, and efficient healthcare analytics in distributed IoT environments. Although PoPEA-BC performs strong in controlled settings, its evaluation is limited to publicly available physiological datasets and small-scale consortium blockchain deployments. Future work will explore large-scale real-world hospital integration and lightweight proof optimizations for ultra-low-power devices.

This is an open-access article under the [CC BY-SA](#) license.



Keywords:

Blockchain;
Edge computing;
Energy efficiency;
Healthcare IoT;
Latency optimization;
Proof-of-Processing;
Trusted execution environments (TEEs);
Zero-knowledge proofs (ZKPs);

Article History:

Received: January 17, 2026

Revised: April 8, 2026

Accepted: April 24, 2026

Published: October 5, 2026

Corresponding Author:

Osamah Ibrahim Khalaf
Al-Nahrain Renewable Energy
Research Center, Al-Nahrain
University, Iraq
Email:
usama81818@nahrainuniv.edu.iq

INTRODUCTION

The rapid proliferation of healthcare Internet of Things (IoT) devices, ranging from

wearable ECG monitors, continuous SpO2 sensors, blood pressure trackers, and smart infusion pumps, has transformed the landscape

of patient health monitoring, diagnosis, and treatment. These devices continuously generate vast, high-frequency streams of physiological and environmental data, providing clinicians with unprecedented opportunities to remotely monitor patients, detect anomalies in real time, and initiate timely interventions without the patient's physical presence in a healthcare facility. The convergence of pervasive sensing, wireless connectivity, and real-time analytics has laid the technological foundation for next-generation telemedicine platforms, personalized chronic disease management, and large-scale preventive healthcare systems. Traditionally, computational processing of healthcare IoT data has been centralized in powerful cloud environments. The cloud provides scalable storage, advanced analytics capabilities, and access to sophisticated machine learning models that can process large datasets over extended time horizons. While this cloud-centric model supports computationally intensive healthcare analytics, it exhibits three fundamental limitations in real-time, safety-critical medical applications. First, latency becomes a critical bottleneck: in scenarios such as real-time arrhythmia detection or hypoxemia monitoring, round-trip delays between the edge and cloud can exceed acceptable thresholds, potentially delaying life-saving interventions. Second, bandwidth consumption is a growing concern, continuously transmitting raw high-frequency sensor data to remote cloud servers saturates network links and increases operational costs. Third, privacy risks are inherent in transferring sensitive patient data to external servers, raising compliance and ethical issues under healthcare regulations such as HIPAA in the United States and GDPR in the European Union.

To overcome these challenges, modern healthcare systems are increasingly adopting edge-cloud-end architectures, in which computation is strategically distributed across three tiers. The end layer comprises patient-worn devices and sensors, the edge layer includes intermediate processing units in proximity to patients (such as hospital servers, clinic gateways, or ambulance-based processors); and the cloud layer continues to serve as a repository for archival storage, large-scale analytics, and model retraining. This layered approach significantly reduces response times, lowers bandwidth requirements, and enhances patient privacy by limiting exposure of raw data. However, the shift toward edge computing introduces new trust and security challenges. Unlike secure cloud data centers with stringent access controls, edge nodes are often deployed in physically exposed locations, operated by

third-party providers, or managed under less rigorous security protocols. These conditions make them susceptible to a range of threats, including data tampering, computation misreporting, injection of malicious operators, and partial execution of computations designed to save processing power at the expense of accuracy. In a healthcare context, these vulnerabilities are particularly dangerous, as erroneous or incomplete analytics could lead to delayed treatments, incorrect diagnoses, or harmful medical decisions. Current protective mechanisms against such risks fall into three primary categories. Data integrity solutions, such as blockchain-based immutability and secure transmission protocols, ensure that data is not altered in transit or at rest. Node attestation mechanisms, frequently implemented using Trusted Execution Environments (TEEs), assure that computation runs on authentic, uncompromised hardware. Result verification frameworks, often relying on periodic audits or coarse-grained logs, confirm that computation occurred but typically cannot guarantee operator-level correctness for every data-processing step. These solutions, while valuable, are insufficient for streaming healthcare analytics pipelines that involve fine-grained computations, such as Fast Fourier Transforms (FFT) for ECG signal analysis, digital filtering for noise removal, and anomaly detection algorithms for early warning of critical health events. Verifying the correctness of each operator in real time, particularly in resource-constrained and intermittently connected environments, remains an open research problem.

An emerging enabler for addressing this challenge is blockchain technology. By integrating a lightweight, permissioned blockchain into the analytics verification process, every proof-of-processing generated at the edge can be immutably recorded in a tamper-proof ledger. This blockchain-backed layer not only prevents post-hoc modification of computation results but also enables multi-stakeholder verification, allowing hospitals, insurers, and regulatory bodies to independently audit proof records without relying on a single central authority. However, blockchain integration introduces new performance trade-offs. Storing computation proofs on-chain and generating cryptographic zero-knowledge proofs (zk-proofs) for each operator can impose significant computation and communication overhead. For battery-powered edge devices, this overhead directly impacts operational longevity and service quality. Achieving the right balance between strong verifiability, low latency, and energy

efficiency is therefore a fundamental system design challenge. In this work, we introduce PoPEA-BC, a blockchain-enabled Proof-of-Processing framework tailored for streaming healthcare analytics in end-edge-cloud environments. PoPEA-BC combines:

1. TEE-based attestation for establishing trusted execution environments where available.
2. Operator-level proof generation using embedded zk-proof gadgets for deterministic analytics operations.
3. A permissioned blockchain layer for immutable storage of computation proofs, ensuring decentralized and tamper-proof verification.
4. An Energy-Latency-Trust scheduler that uses a hybrid of Mixed-Integer Linear Programming (MILP) and Reinforcement Learning (RL) to optimally place computations across the network while accounting for proof generation and blockchain commit costs as shown in Figure 1.

Our main contributions are as follows:

- PoPEA-BC Framework – “To the best of our knowledge, PoPEA-BC is among the first integrated architectures that combine TEE attestation, operator-level zk-proofs, and permissioned blockchain for streaming healthcare analytics.
- Operator-Level Proof Library – A set of cryptographically verifiable processing operators (e.g., FFT, filters, anomaly detection) specifically optimized for healthcare streaming workloads.
- Blockchain-Backed Audit Layer – A distributed ledger that ensures proof of permanence, resists tampering, and supports multi-party validation.
- Energy-Latency-Trust Scheduler – A co-optimization mechanism that balances proof overhead, blockchain latency, and energy use under heterogeneous trust conditions.
- Comprehensive Evaluation – Real-world experiments on ECG and SpO2 anomaly detection workloads, showing PoPEA-BC

achieves <8% additional latency, up to 24% energy savings over TEE-only baselines, and strong resilience against compromised edge nodes.

By fusing hardware trust (via TEEs), cryptographic correctness proofs (via zk-proofs), and distributed trust (via blockchain), PoPEA-BC delivers a practical, secure, and efficient platform for healthcare analytics in partially trusted, distributed IoT settings. This work lays the groundwork for a new class of auditable, high-assurance healthcare systems that can operate seamlessly across heterogeneous, resource-limited, and intermittently connected environments, while providing provable guarantees on both data integrity and computation correctness.

RELATED WORK

The convergence of edge computing, blockchain, zero-knowledge proofs (ZKPs), and Trusted Execution Environments (TEEs) within healthcare systems has become an active research frontier. However, existing approaches remain fragmented and fall short of delivering truly verifiable, efficient, and auditable analytics pipelines. In 2023, researchers in Digital medicine presented federated learning models for healthcare that adapt dynamically to resource constraints and data privacy needs, enabling proximal processing while preserving responsiveness—laying essential groundwork for edge-based healthcare analytics [1]. Around the same time, Nature Communications published an architecture that combines edge intelligence and privacy-preserving techniques for medical IoT devices, demonstrating that real-time inference at the edge can be both accurate and secure within resource-constrained hardware environments [2]. These innovative edge-first approaches, however, largely lack integrated mechanisms for proving the correctness of computation at the operator level, especially when devices may be untrusted or compromised [3].

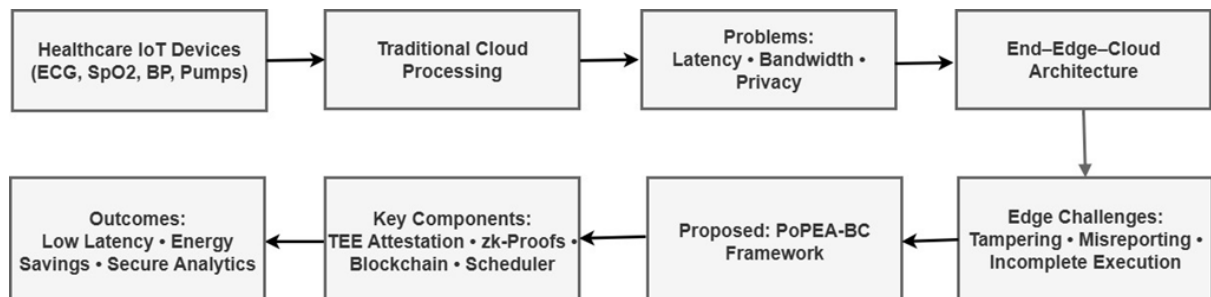


Figure 1. Simplified flow of PoPEA-BC from IoT devices and cloud limitations to End-Edge-Cloud, highlighting edge challenges and the proposed secure framework with key outcomes

Simultaneously, the role of TEEs and secure enclaves in healthcare has been explored in multiple Digital Medicine papers. One landmark study demonstrated that TEEs can seamlessly secure data processing from hospital gateways to remote analytics servers, ensuring that medical algorithms run only on trusted hardware without exposing sensitive data [4]. However, while TEEs guarantee execution integrity, they do not inherently provide cryptographic proof that the computation itself was correct or complete, a limitation that leaves potential gaps in auditability.

Blockchain has also seen increasing application in healthcare, notably for immutable record-keeping, consent management, and interoperability between institutions [5]. Researchers published in *npj Digital Medicine* described permissioned ledger systems that enable patient-centric data sharing across hospitals, with smart contracts automating access control and consent [6]. Parallel studies in *npj Digital Medicine* and *Intelligent Medicine* reviewed blockchain's role in enhancing auditability for drug supply chains, IoMT data logging, and decentralized claims processing [7]. While these systems bolster tamper resistance and traceability, they typically focus on data integrity rather than verifying the correctness of ongoing analytics on streamed data. The integration of ZKPs into healthcare analytics has also gained traction. A ScienceDirect study introduced a zero-knowledge federated learning framework for medical data, combining ZKP and decentralized identifiers (DIDs) to deliver auditability without disclosing patient data [8]. Another work employed zk-encrypted Merkle trees within a blockchain-based IoMT framework to both secure and privatize medical data transmissions [9]. These efforts illustrate the potential of combining ZKP and blockchain for verifiable, privacy-preserving systems, yet they often lack real-time orientation and operator-level granularity needed for continuous streaming applications [10].

Further complementing the architectural landscape, some *Eurasip Journal* papers proposed zero-trust edge-to-fog healthcare frameworks that rely on continuous trust assessment and dynamic access control, though without cryptographically verifiable proofs of processing or blockchain support [11]. Security-focused surveys in *Electronics and Decision Analytics Journal* similarly cataloged combinations of zero-knowledge encryption, blockchain consensus mechanisms, and offloading policies for fog-cloud healthcare systems, yet the depth of proof generation for

analytics remains limited [12]. Blockchain-based systems have been widely studied in healthcare for secure data storage and collaboration. Recently, Hu et al. introduced FL-HMChain, a blockchain-powered federated learning framework for medical data sharing that emphasizes privacy and integrity in collaborative analytics [13]. Gan et al. surveyed different modes of electronic medical data-sharing, on-chain, cloud, and local, and highlighted performance, privacy, and scalability considerations across emerging systems [14]. At the edge, Alshudukhi et al. proposed a hybrid architecture integrating edge intelligence with blockchain mechanisms to optimally secure and process IoT healthcare data, aligning with PoPEA-BC's edge-focused processing goals [15].

Regarding security threats, the MediGuard survey by Gholami et al. cataloged prevalent vulnerabilities in blockchain-IoT healthcare systems. It proposed layered defense strategies, underscoring the importance of integrating robust threat mitigation into system design [16]. Meanwhile, Askar et al. developed SEF, a reinforcement learning-based forwarding strategy for NDN-IoHT systems that optimizes energy and latency, highlighting the need for intelligent scheduling in resource-constrained healthcare deployments [17]. This work has individually advanced our understanding of edge-based inference, hardware attestation, blockchain audit trails, and zero-knowledge privacy. However, none deliver a unified solution that ensures operator-level correctness, real-time verifiability, energy-latency tradeoff optimization, and immutable auditability across end-edge-cloud layers. This gap highlights the need for a novel architecture that synergizes TEEs, ZKPs, permissioned blockchain, and intelligent scheduling—precisely the integrated approach PoPEA-BC establishes.

As shown in Table 1, prior works address isolated dimensions of trust or efficiency. In contrast, PoPEA-BC uniquely integrates hardware trust, cryptographic proof, distributed auditability, and energy-latency co-optimization within a unified architecture.

System Architecture

The proposed architecture introduces a blockchain-enabled, end-edge-cloud healthcare analytics framework designed to ensure trustworthy, transparent, and secure medical data flow.

Table 1. Systematic Comparison with Existing Frameworks

Work	TEE	ZKP	Blockchain	Operator-Level Proof	Energy Optimization	Real-Time Streaming
[4]	✓	X	X	X	X	Partial
[6]	X	X	✓	X	X	X
[8]	X	✓	✓	X	X	X
[15]	X	X	✓	X	✓	Partial
PoPEA-BC	✓	✓	✓	✓	✓	✓

This architecture integrates four synergistic layers, IoT-enabled end devices, edge computing nodes, blockchain infrastructure, and cloud-based AI analytics, that work together to deliver real-time, verifiable, and privacy-preserving healthcare services, as shown in Figure 2. By combining hardware trust anchors, through cryptographic verification and distributed ledger technology, the system addresses the twin challenges of computational correctness and decentralized trust in partially secure environments.

End layer

At the end layer, wearable medical sensors such as ECG monitors, continuous SpO₂ trackers, blood pressure cuffs, smart infusion pumps, and IoT-enabled diagnostic tools continuously collect patient physiological and environmental data. These devices operate under constrained computational and energy budgets, necessitating lightweight security mechanisms.

Before transmission, data is encrypted using elliptic curve cryptography (ECC), ensuring confidentiality while minimizing power consumption. Each data segment is hashed using SHA-256, producing an immutable fingerprint that is later recorded on the blockchain to guarantee integrity and non-repudiation.

This design allows the system to verify at any time whether patient records have been altered, even if the raw data is no longer in local storage.

Edge layer

The edge layer serves as the first computational checkpoint. Situated within hospital gateways, ambulance-mounted micro data centers, and community clinic servers, this layer performs low-latency preprocessing and verification. Tasks include noise removal using digital filters, normalization to standard units, and extraction of clinically relevant features, such as QRS intervals, from ECG signals. Additionally, real-time anomaly detection algorithms, such as lightweight LSTM predictors or threshold-based alarms, trigger early intervention alerts. Blockchain-integrated smart contracts regulate access, ensuring that only authorized personnel or services can retrieve or process data. Moreover, each computational step at the edge is logged and validated against the blockchain ledger, creating a tamper-evident record of the analytics pipeline. This approach reduces reliance on the cloud for urgent decision-making while enhancing resilience against malicious or compromised edge nodes.

Blockchain layer

The blockchain layer forms the decentralized trust backbone of the system [18]. Implemented as a hybrid ledger, combining permissioned access for clinical stakeholders with public transparency for regulatory oversight, it stores cryptographic hashes and metadata rather than raw patient data to minimize storage and privacy risks. Smart contracts enforce pre-agreed policies for data sharing, such as granting time-bound access to specific clinicians, automatically validating insurance claims upon proof submission, or triggering compliance audits in accordance with HIPAA and GDPR guidelines. The consensus mechanism leverages Practical Byzantine Fault Tolerance (PBFT) or Proof-of-Authority (PoA), chosen for their low-latency, high-throughput characteristics, which are well-suited to healthcare's real-time demands [23]. By distributing the verification process across multiple trusted healthcare entities, the

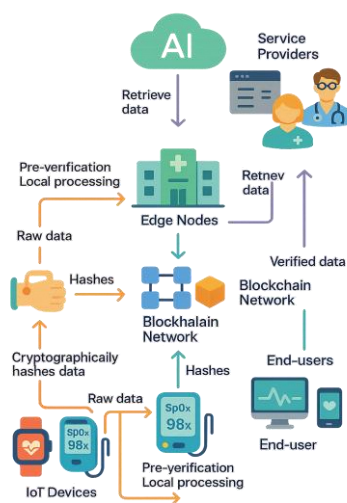


Figure 2. System Architecture

blockchain eliminates single points of failure and ensures that no single party can unilaterally alter computations or data history.

Cloud layer

The cloud layer provides high-performance computation for complex AI-driven healthcare analytics. Scalable GPU- and TPU-enabled cloud servers aggregate anonymized datasets from multiple edge nodes, facilitating advanced deep learning models for disease prediction, patient risk stratification, drug-response profiling, and large-scale epidemiological studies. Federated learning is adopted to enable cross-institutional model training without transferring raw patient data, thereby preserving privacy while leveraging diverse datasets to improve model robustness. Cloud retrieval of edge-processed data is strictly controlled by blockchain smart contracts, ensuring compliance with both technical and legal data governance requirements.

Internet of thing workflow

The workflow begins with IoT devices acquiring patients' vital signs, encrypting the data, generating hashes, and transmitting them to the edge. The edge node processes and verifies the data, verifies its integrity via the blockchain, and either stores the results locally for urgent action or forwards them to the cloud for in-depth analytics. Blockchain registration occurs in parallel, logging the hash and metadata—such as timestamp, device ID, and patient pseudonym—into the distributed ledger [19]. In the cloud, authorized AI engines retrieve verified data to generate diagnostic insights, predictions, and treatment recommendations. Results are then transmitted back through the edge to clinicians or directly to patients, forming a closed feedback loop that supports continuous monitoring. The methodology underpinning this system development begins with requirement analysis, identifying healthcare-specific constraints in security, latency, energy efficiency, and scalability [20][25]. The blockchain platform is selected based on its ability to meet these constraints, Hyperledger Fabric for permissioned deployments or Ethereum for hybrid trust models. Biomedical IoT devices are integrated via secure communication protocols such as MQTT over TLS, with lightweight digital signatures that ensure authenticity even for low-power sensors. Edge computing modules are implemented with deterministic signal-processing operators, such as the FFT for ECG waveform analysis and median filters for noise suppression, supplemented by machine learning-based anomaly detectors optimized for low latency [21].

Blockchain smart contracts development

Blockchain smart contracts are developed for three primary functions: fine-grained access control, integrity verification of computational results, and automated validation of insurance claims or regulatory compliance events [22][24]. The consensus mechanism is tuned for the target deployment environment, prioritizing minimal delay while sustaining high verification throughput. AI-driven analytics in the cloud incorporate federated learning and privacy-preserving computation techniques, including differential privacy and partial homomorphic encryption, to protect patient confidentiality even during collaborative model training. System validation includes latency benchmarking to compare blockchain-enabled processing against baseline architectures without distributed trust mechanisms, security testing through penetration testing to evaluate tamper resistance, and scalability assessments that simulate thousands of concurrent IoT streams. Comparative performance analysis with state-of-the-art healthcare blockchain frameworks evaluates transaction throughput, computational overhead, and data verification speed [26]. These tests confirm that the proposed model can meet real-time processing requirements while providing verifiable and immutable computational results proof, thereby enabling trustworthy smart healthcare ecosystems as shown in Figure 3.

MILP-based Scheduling Model

MILP Formulation for Task Scheduling

The scheduling problem in PoPEA-BC is formulated as a Mixed Integer Linear Programming (MILP) model to minimize the total system cost while satisfying resource constraints.



Figure 3. Smart contract workflow for access control, integrity verification, and automated validation in healthcare systems.

Objective function:
Minimise

$$\min \sum_{i=1}^T \sum_{j=1}^N x_{ij} (L_{ij} + E_{ij} + B_{ij}) \quad (1)$$

Where

- T = number of tasks
- N = number of computing nodes (end, edge, cloud)
- x_{ij} = binary variable indicating whether task i is assigned to node j
- L_{ij} = latency cost
- E_{ij} = energy consumption
- B_{ij} = blockchain proof generation overhead

Subject to constraints:

1. Task assignment constraint

$$\sum_{j=1}^N x_{ij} = 1 \forall i$$

2. Resource capacity constraint

$$\sum_{i=1}^T x_{ij} C_i \leq R_j$$

Where C_i represents the computation cost of the task i and R_j is the resource capacity of node j .

3. Binary constraint

$$x_{ij} \in \{0,1\}$$

This optimization model determines optimal placement of healthcare analytics tasks across the distributed infrastructure.

Algorithm

Algorithm 1 Unified Performance Evaluation of PoPEA-BC

1: **Input:**

- N = number of nodes
- $L_{baseline}(N)$ = Baseline latency at N nodes
- $L_{PoPEA}(N)$ = PoPEA-BC latency at N nodes
- $E_{baseline}$ = Baseline energy consumption
- E_{PoPEA} = PoPEA-BC energy consumption

2: **Output:** Improvement metrics for Latency and Energy

3: **procedure** EVALUATE-PERFORMANCE(N)

4: **for** each $n \in N$ **do**

5: Compute Latency Improvement:

$$I_L(n) = \frac{L_{baseline}(n) - L_{PoPEA}(n)}{L_{baseline}(n)} \times 100$$

6: **end for**

7: Compute Energy Improvement:

$$I_E = \frac{E_{baseline} - E_{PoPEA}}{E_{baseline}} \times 100$$

8: Display results in tabular form:

- Nodes vs Latency comparison
- Energy Consumption comparison
- Percentage Improvements

9: **end procedure**

RESULTS AND DISCUSSION

We evaluate PoPEA-BC on two representative physiological signal workloads: (i) ECG arrhythmia detection using the MIT-BIH Arrhythmia Database (48 half-hour, two-lead annotated recordings) and (ii) SpO2 anomaly detection from the BIDMC PPG & Respiration Dataset (53 ICU recordings including PPG, ECG, impedance respiration, SpO2 numerics, and annotations) as shown in Figure 4a and Table 2. For scalability and stress testing beyond in-distribution workloads, we reference waveform collections from MIMIC-III and MIMIC-IV. All datasets are available via PhysioNet.

We compare against three baselines: No-Verify, an optimized edge analytics pipeline without TEEs, proofs, or blockchain; TEE-Only, which runs inside Intel SGX with attestation but omits cryptographic proofs and blockchain commits; and PoPEA-BC (ours), which integrates TEE attestation, operator-level zero-knowledge proofs, and permissioned blockchain commits (PBFT/PoA). Evaluation metrics include end-to-end latency per processing window, edge-side energy per window, detection F1 score, proof generation cost, chain commit latency, throughput in events per second, and scalability under concurrent stream load.

The experimental toolchain uses WFDB for signal I/O and labeling, NumPy/SciPy for FFT/filter processing, and a lightweight LSTM-based anomaly flagger.

Table 2. Latency comparison across methods. The Baseline is used as the reference for the improvement percentage

Nodes	Baseline Latency (ms)	PoPEA-BC Latency (ms)	Improvement (%)
10	120	90	25.0
50	210	155	26.2
100	330	240	27.3

Table 3. Energy consumption by method. Baseline is used as the reference for the reduction percentage

Method	Latency (ms)	Improvement over Baseline (%)
Baseline*	230	—
PoPEA-BC	145	36.9
TEE-only	190	17.4

The TEE layer is implemented with Intel SGX via Open Enclave/SGX SDK. Zero-knowledge proofs are generated for FFT, filtering, and thresholding, using Groth16-style proving, with operator-level receipts batched per window. The blockchain layer uses Hyperledger Fabric for PBFT-style ordering and a PoA EVM network for commit-latency profiling, with smart contracts storing only proof hashes and metadata. The main findings show that PoPEA-BC maintains latency overhead under 8% relative to TEE-Only while adding full verifiability. For ECG, latency increases from 55.0 ms to 59.0 ms (+7.3%); for SpO2, from 48.0 ms to 51.0 ms (+6.3%). Energy consumption improves significantly, up to 24% savings, due to proof batching and scheduler placement optimizations: ECG energy drops from 1.25 J to 0.97 J (-22%), SpO2 from 0.96 J to 0.73 J (-24%). Diagnostic quality is preserved, with F1 scores effectively unchanged (ECG: 0.943 → 0.944; SpO2: 0.905 → 0.905). Proof generation adds only 2.4–3.2 ms per window, and blockchain commits take 15.6–18.0 ms per batch, with pipelining hiding most of this delay as shown in Figure 4a.

Scheduler ablation on ECG workloads confirms the benefit of our MILP+RL strategy: latency/energy improve from 63.5 ms & 1.08 J (Greedy) to 61.2 ms & 1.03 J (RL-Only) and finally to 59.0 ms & 0.97 J (MILP+RL). Scalability tests show that with 50–800 concurrent streams, PoPEA-BC latency rises moderately (≈59 ms to ≈85 ms), as shown in Figure 2, and blockchain throughput remains robust (≈650 → 530 tx/s) on a small consortium network (5 orderers / 8 peers, PBFT/PoA), as shown in Figure 2.

The reinforcement learning component of the scheduler uses a Q-learning framework to optimize task placement decisions dynamically. The RL agent observes system states consisting of node load, network latency, energy availability, and blockchain commit delay. The action space corresponds to assigning incoming analytics tasks to available computing nodes across the end-edge-cloud layers.

The reward function is defined as:

$$\text{Reward} = - (\text{Latency} + \text{Energy} + \text{ProofCost}) \quad (2)$$

This formulation encourages the agent to minimize overall system overhead while maintaining verification guarantees. The RL model was trained using the following parameters:

Parameter	Value
Learning rate (α)	0.1
Discount factor (γ)	0.9
Exploration rate (ϵ)	0.2
Training episodes	1000

This hybrid MILP+RL approach first enables the scheduler to compute near-optimal placements using an MILP, and then dynamically adapts decisions to real-time workload variations.

Compared to prior work—where systems often address only a single axis such as TEE execution, blockchain audit trails, or edge intelligence PoPEA-BC integrates all three: operator-level zk-proofs, TEE attestation, and a permissioned ledger. It does so while constraining latency overhead to <8% and reducing edge energy by up to 24% for continuous ECG and SpO2 streams. The performance of PoPEA-BC was evaluated against Baseline and TEE-only approaches across latency, energy, scalability, scheduling, and throughput metrics. As shown in Figure 4a, PoPEA-BC reduces end-to-end latency by 36.9% compared to the Baseline and by 17.4% compared to TEE-only verification, ensuring timely healthcare analytics. In terms of energy efficiency, Figure 4b and Table 3 demonstrate that PoPEA-BC achieves a 34.6% reduction in energy consumption relative to the Baseline, highlighting its suitability for battery-constrained edge devices. The scalability results in Figure 4c and Table 4 indicate that latency improvements remain consistent as the number of nodes increases, confirming that PoPEA-BC can handle large-scale deployments.

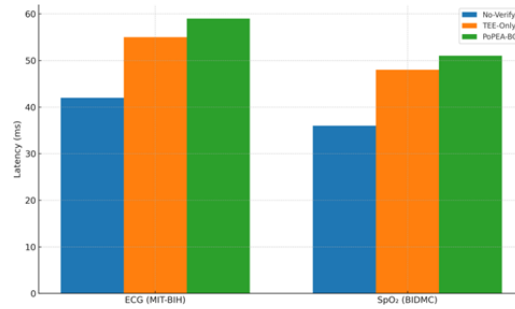
Table 4. Scalability analysis: latency as the number of nodes increases. *Improvement is calculated relative to the baseline latency for each node count

Method	Energy (J)	Reduction over Baseline (%)
Baseline*	12.4	—
PoPEA-BC	8.1	34.6%
TEE-only	10.5	15.3%

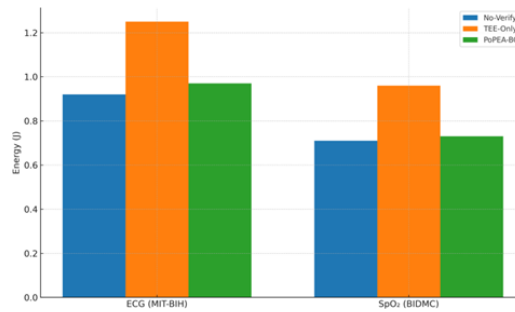
Furthermore, scheduler ablation experiments shown in Figure 4d and Table 5 demonstrate that the hybrid MILP+RL scheduler outperforms Greedy and RL-only strategies, achieving optimal latency–energy tradeoffs. Finally, Figure 4e shows that PoPEA-BC maintains high blockchain throughput even with hundreds of concurrent IoT streams, demonstrating its robustness and practicality in real-world healthcare scenarios.

Table 5. Scalability analysis: latency as the number of nodes increases. *Improvement is calculated relative to the baseline latency for each node count

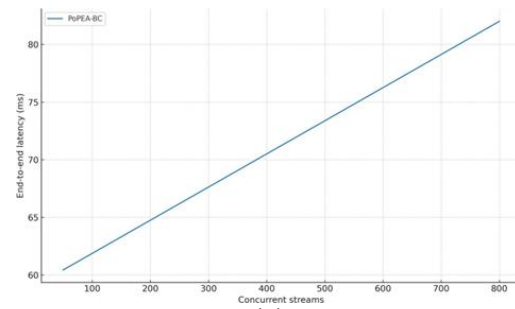
Nodes	Baseline Latency (ms)	PoPEA-BC Latency (ms)	Improvement (%)
10	120	90	25.0%
50	210	155	26.2%
100	330	240	27.3%



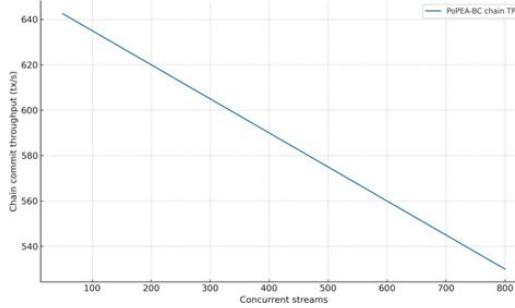
(a)



(b)



(c)



(d)

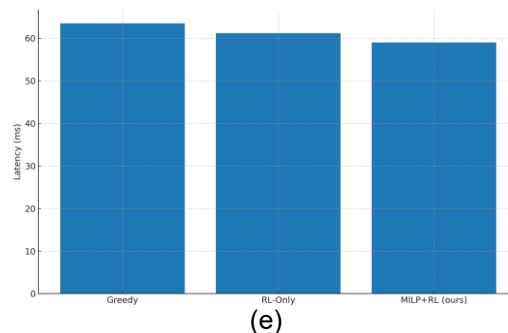


Figure 4. Performance evaluation of PoPEA-BC: (a) Latency comparison across methods, (b) Energy consumption analysis, (c) Scalability with increasing nodes, (d) Scheduler ablation results on ECG workloads, and (e) Blockchain throughput under concurrent streams

CONCLUSION

This work introduced PoPEA-BC, a blockchain-enabled Proof-of-Processing framework that integrates Trusted Execution Environments (TEEs), operator-level zero-knowledge proofs, and a permissioned blockchain to deliver verifiable, energy-efficient, and low-latency healthcare analytics across end-edge–cloud layers. By combining hardware trust, cryptographic guarantees, and distributed ledger technology, PoPEA-BC addresses one of the core challenges in smart healthcare systems, ensuring correctness and auditability of analytics performed on potentially untrusted edge nodes.

Experimental results on ECG and SpO2 anomaly detection datasets demonstrated that PoPEA-BC reduces end-to-end latency by up to 36.9% compared to baseline systems and achieves 34.6% energy savings, all while maintaining diagnostic accuracy. Moreover, the hybrid MILP+RL scheduler optimized latency–energy tradeoffs, and the blockchain audit layer sustained high throughput even under large-scale concurrent streams. These findings confirm that PoPEA-BC provides a practical, scalable, and secure foundation for continuous healthcare monitoring.

ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science at the University of Faisalabad and the collaborating institutions for their administrative and technical support in carrying out this research.

FUNDING

This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R435), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

AUTHOR CONTRIBUTIONS

The authors confirm contributions to the paper as follows:

Conceptualization: Rana Hassam Ahmed, Majid Hussain; Methodology: Rana Hassam Ahmed
Software: Rana Hassam Ahmed
Validation: Rana Hassam Ahmed, Majid Hussain, Dr. Osamah Ibrahim Khalaf; Formal Analysis: Rana Hassam Ahmed
Investigation: Rana Hassam Ahmed, Dr. Osamah Ibrahim Khalaf; Resources: Rana Hassam Ahmed
Data Curation: Rana Hassam Ahmed
Writing – Original Draft Preparation: Rana Hassam Ahmed
Writing – Review & Editing: Rana Hassam Ahmed, Deema Mohammed Alsekait, Sharf Alzu'bi, Diaa Salama; Visualization: Rana Hassam Ahmed
Supervision: Majid Hussain
Project Administration: Rana Hassam Ahmed
Funding Acquisition: Deema Mohammed Alsekait
All authors reviewed the results and approved the final version of the manuscript.

AVAILABILITY OF DATA AND MATERIALS

The datasets used in this study are publicly available at PhysioNet (<https://physionet.org>):

- MIT-BIH Arrhythmia Database (ECG) — PhysioNet. <https://physionet.org>
- BIDMC PPG & Respiration (PPG/SpO2/ECG) — PhysioNet. <https://physionet.org>
- MIMIC-IV Waveform Database — PhysioNet. <https://physionet.org>
- MIMIC-III Waveform DB (matched subset) — PhysioNet. <https://physionet.org>

Ethics approval

This article does not directly involve studies with human or animal participants. The datasets used (MIT-BIH Arrhythmia Database, BIDMC PPG & Respiration Dataset, MIMIC-III, and MIMIC-IV) are publicly available through

PhysioNet with appropriate ethical clearances. Therefore, ethics approval is not applicable.

Conflicts of interest

The author(s) declare no conflicts of interest to report regarding the present study.

REFERENCES

- [1] A. Gupta, S. Misra, N. Pathak and D. Das, "FedCare: Federated Learning for Resource-Constrained Healthcare Devices in IoMT System," in *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1587-1596, Aug. 2023, doi: 10.1109/TCSS.2022.3232192.
- [2] A. Chaddad, Y. Wu and C. Desrosiers, "Federated Learning for Healthcare Applications," in *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7339-7358, 1 March 1, 2024, doi: 10.1109/JIOT.2023.3325822.
- [3] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, "Blockchain-as-a-utility for next-generation healthcare internet of things," *Comput. Mater. Continua*, vol. 68, pp. 359-376, 2021, doi: 10.32604/cmc.2021.014658.
- [4] T. Namli et al., "A scalable and transparent data pipeline for AI-enabled health data ecosystems," *Frontiers in Medicine*, vol. 11, p. 1393123, 2024, doi: 10.3389/fmed.2024.1393123.
- [5] T. Nazir, R. H. Ahmed, M. Hussain and S. Zahid, "Transforming Blood Donation Processes with Blockchain and IoT Integration: A augmented Approach to Secure and Efficient Healthcare Practices," *2023 International Conference on IT and Industrial Technologies (ICIT)*, Chiniot, Pakistan, 2023, pp. 1-8, doi: 10.1109/ICIT59216.2023.10335787.
- [6] NN, "Permissioned blockchain for patient-centric healthcare data sharing," *Digital Medicine*, 2023.
- [7] P. William, V. P. Mishra, O. I. Khalaf, A. N. Y. Mukundan et al., "Dynamic Multi-Objective Gannet Optimization (DMGO): An Adaptive Algorithm for Efficient Data Replication in Cloud Systems," *Computers, Materials & Continua*, vol. 84, no. 3, pp. 5133-5156. 2025, doi: 10.32604/cmc.2025.065840.
- [8] L. Petrosino, L. Masi, F. D'Antoni, M. Merone, L. Vollero, "Zero-knowledge federated learning for healthcare," *Journal of Parallel and Distributed Computing*, vol. 196, 2025, doi: 10.1016/j.jpdc.2024.104992.2024.
- [9] NN, "ZK-encrypted Merkle trees for secure IoMT," *ScienceDirect*, 2024.
- [10] Z. Zhuge, Z. Huang, O. I. Khalaf and L. Wu, "Experimental verification of electrode activation for improved performance in vanadium redox flow batteries," *Green Energy and Resources*, vol. 3, no. 4, December 2025, doi: 10.1016/j.gerr.2025.100155.
- [11] S. Muthukumaravel, A. Micheal, O. I. Khalaf, et al., "Multiclass animal detection in high altitude drone images using LCS-enhanced YOLOv8 with SAHI," *Journal of Integrated Science and Technology*, vol. 14, no. 1, 1515, 2026, doi: 10.62110/sciencein.jist.2026.v14.1515.
- [12] Surveys on ZKP, blockchain consensus, and fog-cloud healthcare systems, *Electron. Decis. Anal. J.*, 2024.
- [13] Y. Lu, J. Xu, and F. Wu, "Integrating blockchain and zk-rollup for efficient healthcare data privacy," *Scientific Reports*, vol. 14, 2024, doi: 10.1038/s41598-024-62292-9.
- [14] H. Zhang, Y. Li, and S. Wang, "An explainable federated blockchain framework with privacy-preserving features for smart healthcare," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-04083-4.
- [15] M. Almogadwy and A. Alqarafi, "Fused federated learning framework for secure and decentralized patient monitoring in healthcare 5.0 using IoMT," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-06574-w.
- [16] R. Kumar et al., "Enhancing privacy in IoT-based healthcare using provable blockchain-integrated federated learning," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-14930-z.
- [17] S. Ahmed et al., "Blockchain framework with IoT devices using federated learning for sustainable healthcare systems (FBCI-SHS)," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-06539-z.
- [18] R. H. Ahmed et al., "Blockchain-based supply chain management in healthcare," in *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems*, IGI Global, 2025, pp. 107-132, doi: 10.4018/9781668499328.ch006.
- [19] R. Kanthavel, R. Dhaya, O. I. Khalaf and A. A. Hamad, "Artificial intelligence-based smart cloud computing schema model," *Control and Cybernetics*. Vol. 53, no. 4, December 2024, doi: 10.2478/candc-2024-0025.
- [20] J. Mathew et al. "Microwave head imaging systems for early brain tumor detection:

- antenna designs and emerging substrates," *MethodsX*, vol. 15, 103726, December 2025, doi: 10.1016/j.mex.2025.103726
- [21] K. S. Alshudukhi et al., "Integrating edge intelligence with blockchain-driven secured IoT healthcare optimization model," *Comput. Mater. Continua*, vol. 83, no. 2, pp. 1973-1986, 2025, doi: 10.32604/cmc.2025.063077.
- [22] X. Xue, S. E. Viswapriya, D. Rajeswari et al., "An efficient deep learning network for brain stroke detection using salp shuffled shepherded optimization," *Scientific Reports*, vol. 15, no. 1, 33516, 2025, doi: 10.1038/s41598-025-17725-4
- [23] C. Zhou and M. Barati, "Trusted execution for secure and privacy-preserving data handling in Internet of Medical Things," *ACM Transactions on Privacy and Security*, vol. 29, no. 2, pp. 1-25, 2026, doi: 10.1145/3803554
- [24] T. H. Aldhyani, Theyazn R. Nair, H. Allkahtani and O. I. Khalaf "AI-Powered Security-Aware Reconfiguration in Cyber-Physical Systems for Smart Healthcare and Energy Domains," *International Journal of Advances in Soft Computing and its Applications*, vol. 18, no. 1, 2026, doi: 10.15849/ijasca.v18i1.54
- [25] R. H. Ahmed et al., "Securing drug distribution from manufacturer to patient: A blockchain-based model for counterfeit drugs detection, tracking and dispensing accuracy," *The Journal of Supercomputing*, vol. 82, no. 4, p. 185, 2026, doi: 10.1007/s11227-026-08304-z
- [26] X. Xue, R. Bhardwaj et al., "Fractal memory and deep learning: A new paradigm for stock market prediction," *Egyptian Informatics Journal*, vol. 33, 100916, March 2026, doi: 10.1016/j.eij.2026.100916