Chapter 6

Energy-Efficient and Privacy-Preserving Blockchain Based Federated Learning for Smart Healthcare System

6.1 Introduction

According to the WHO, the aging population is vulnerable to chronic illnesses, mental health issues, and other health conditions. These factors can lead to problems like a shortage of medical resources and a decline in healthcare quality [2]. Consequently, there is a growing demand for technological solutions designed to monitor patients' health conditions remotely. A particularly promising strategy involves employing a WBAN. This network places multiple physiological sensors on a patient's body, and an LD, such as a smartphone, tablet, or laptop, is utilized to transmit the gathered sensor data to a server for subsequent analysis [3]. WBAN-based health monitoring facilitates real-time tracking of vital health parameters like heart rate, body temperature, and patient activity. It presents a convenient solution for emergency scenarios in which

patients may not promptly receive medical attention until they reach a medical facility. For instance, WBAN can gather and monitor a patient's real-time health metrics while they are in transit.

Amidst the growing utilization of WBANs for collecting patient health data, researchers have harnessed this substantial dataset to train ML models for diverse healthcare applications [2]. Nevertheless, conventional ML approaches necessitate the transmission of patients' health data to a central server, consequently raises privacy vulnerabilities. In response to this challenge, the FL paradigm has gained prominence as a widely adopted framework that allows for localized computation of patient data. By doing so, it obviates the need to expose raw health data, thereby effectively safeguarding privacy [57].

In view of the constrained energy capacity of WBANs, it is imperative to consider both local computation and transmission energy in the FL process. To curtail energy consumption associated with the computation and transmission of local models, researchers have proposed the adoption of a QNN operating at reduced precision levels. This choice is driven by the unsuitability of the standard 32-bit precision level for WBANs operating under resource constraints [132]. While WBANs transmit only model weights to the aggregation server, the prospect of privacy breaches remains, as adversaries might exploit these weights to potentially infer original data [18].

To mitigate privacy concerns in the FL framework, strategies like DP [19] and HE [18] have been employed. Furthermore, the conventional FL framework, centered around a singular server, inherently introduces a single point of failure. To counteract this vulnerability, the integration of blockchain technology with FL has yielded a decentralized and secure platform for the aggregation of models [20].

This chapter introduces a blockchain based FL framework designed to enhance energy efficiency and privacy while enabling collaborative training across multiple WBANs in the HD. Nevertheless, concerns arise from potential data-sharing reluctance among

WBAN users due to inadequate REwards (REs), and the hesitation of miners due to the energy-intensive nature of blockchain maintenance. To address these challenges, we propose utility maximization problem that considers computation and communication energy, WBAN rewards, miner revenue, and FL loss. In our proposed framework, each WBAN adopts QNN to reduce computation and transmission energy consumption. Additionally, we bolster user privacy through the integration of DP technique [133] and Paillier HE [134]. DP ensures robust privacy protection during FL model training, while Paillier HE facilitates the aggregation of encrypted local model weights, thereby generating global model weights without the need for decryption. Furthermore, our approach incorporates blockchain technology for decentralized model weight sharing, employing the Proof-of-Work (PoW) consensus mechanism due to its strong security, decentralization, robustness, and tamper-resistant properties. Unlike Proof-of-Stake (PoS) and Delegated PoS (DPoS), where wealthier validators or miners with larger stakes have more control over the validation process, PoW requires significant computational resources, making it more resistant to control by a few entities. Additionally, PoS and DPoS can lead to fluctuating gas fees due to increased competition among validators for transaction validation [135, 136]. In summary, the main contributions of this chapter include:

- Formulate an optimization problem that maximizes the utility of WBANs and miners, considering energy consumption, rewards of WBANs, revenue of miners, and FL loss altogether as an NP-hard problem.
- Propose a stable WBAN-Miner Association (WMA) heuristic that matches WBANs with miner-reward level pairs to maximize the utility in $O(MP^2G)$ time complexity, where M, P, and G denote the numbers of miners, WBANs, and reward levels, respectively.
- Propose an energy-efficient and privacy-preserving smart healthcare system that utilizes blockchain based FL and employs DP and HE to enhance the privacy

protection of WBAN users, with $O(T|\mathbf{w}|(|\mathbb{Y}| + M^2))$ communication cost, where I, $|\mathbb{Y}|$, and $|\mathbf{w}|$ are the numbers of global iterations, participating WBANs, and model weights, respectively.

- Extensive experiments on real-world data demonstrate the proposed framework's effectiveness, achieving an average improvement of 15.1%, 9.03%, and 15.35% compared to state-of-the-art works.

6.2 System Model and Problem Formulation

We consider a smart healthcare system comprising P WBAN users and M FC-enabled hospitals, represented by $\mathbb{P} = \{1, \ldots, p, \ldots, P\}$ and $\mathbb{M} = \{1, \ldots, m, \ldots, M\}$ respectively, along with a trusted entity[1]. The FC-enabled hospitals are interconnected via blockchain and function as miners. Prior to the FL process, the trusted entity establishes a connection between WBANs and miners, illustrated in Fig. 6.1. The system's objective is to train an FL model for a specific task, such as heart disease detection, utilizing the substantial data collected from WBAN users. Let $\mathbb{D}_p = \{\mathfrak{n}_p^1, \ldots, \mathfrak{n}_p^d, \ldots, \mathfrak{n}_p^{D_p}\}$ be the set of D_p data samples for WBAN p. Each WBAN trains a model using its local data, avoiding the transfer of raw health data to a central server, and sends the model weights to a miner for aggregation [138]. However, establishing a proper association between WBANs and miners is vital for ensuring a reliable FL process. Thus, the aforementioned scenario is categorized into two stages as follows:

Stage 1: WBAN-Miner Association (WMA): In this stage, the trusted entity orchestrates the creation of associations between WBANs and miners using DAA, which considers the utilities of both WBANs and miners (given in Subsection 6.3.1).

Stage 2: Efficient blockchain based FL: WBANs independently train local models on their data and transmit only model weights to their respective miners. To

[1]We assume WBANs are honest, and miners are honest yet curious, implying they operate faithfully but seek WBAN user data [137].

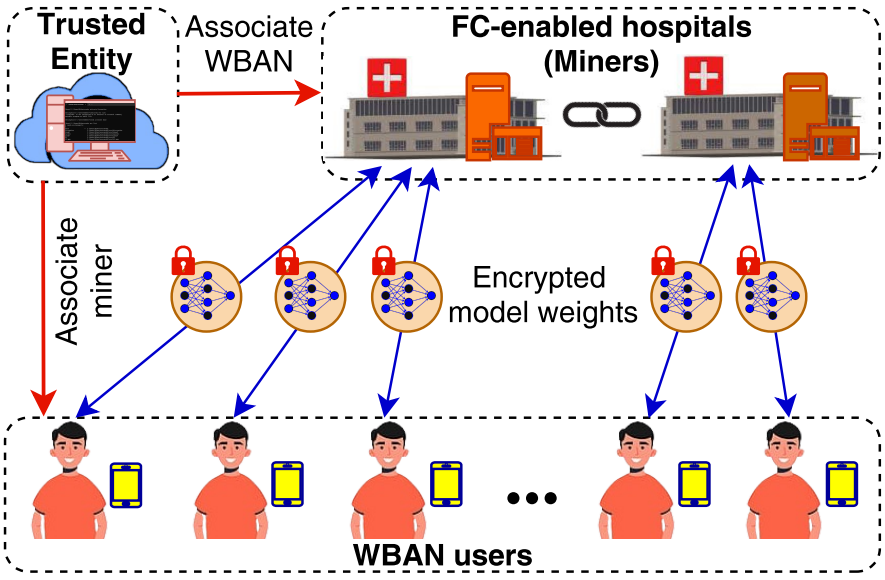


Fig. 6.1. Blockchain-based FL framework.

bolster energy efficiency and preserve privacy, our framework employs quantization and HE technique. Quantization curbs the computational burden on WBANs, consequently lowering energy consumption. Furthermore, HE facilitates computations on encrypted data, eliminating the necessity for decryption and thereby upholding user privacy.

Fig. 6.2 illustrates the data flow diagram for the aforementioned two stages. To establish associations between WBANs and miners in Stage 1, a preference order is required, driven by the utility as elaborated below.

6.2.1 Utility of WBAN

We consider a processing chip available within the WBAN for local model training, comprising a main memory and a local memory. However, as WBANs typically operate under energy constraints and cannot engage in local FL model training, we employ quantization of model weights using finite j precision levels to reduce computational energy consumption. Let $\mathbb{O} = \{\mathfrak{o}_1, \ldots, \mathfrak{o}_p, \ldots, \mathfrak{o}_P\}$ be the count of Multiply-Accumulate (MAC) units on the WBAN chip. Consequently, the energy consumption of a MAC

operation utilizing j-bit precision is defined as follows [132]:

$$\mathcal{O}_{MAC}(\mathrm{h}) = \mathfrak{A}\left(\frac{j}{\mathrm{h}_{max}}\right)^{\mathrm{z}}, \tag{6.1}$$

where $\mathfrak{A} > 0, 1 < \mathrm{z} < 2$, and h_{max} is the maximum precision level (discussed in Section 6.3.2).

The energy consumption at WBAN p is defined as the sum of the computation energy $\mathcal{O}^{cm}(\mathrm{h})$, the access energy for weights from memory $\mathcal{O}_p^{we}(\mathrm{h})$, and the access energy for activations from memory $\mathcal{O}_p^{ac}(\mathrm{h})$. Thus, the energy consumption of WBAN p during local model training using j bits quantization in one local iteration is given as follows:

$$\mathscr{O}_p(\mathrm{h}) = \mathcal{O}^{cm}(\mathrm{h}) + \mathcal{O}_p^{we}(\mathrm{h}) + \mathcal{O}_p^{ac}(\mathrm{h}), \tag{6.2}$$

$$\mathcal{O}^{cm}(\mathrm{h}) = \mathcal{O}_{MAC}(\mathrm{h})\mathfrak{P}_s + 4\mathfrak{P}_o\mathcal{O}_{MAC}(\mathrm{h}_{max}), \tag{6.3}$$

$$\mathcal{O}_p^{we}(\mathrm{h}) = 2\mathcal{O}_{MAC}(\mathrm{h})\mathfrak{P}_w + \mathcal{O}_{MAC}(\mathrm{h})\mathfrak{P}_s\sqrt{j/\mathfrak{o}_p\mathrm{h}_{max}}, \tag{6.4}$$

$$\mathcal{O}_p^{ac}(\mathrm{h}) = 4\mathcal{O}_{MAC}(\mathrm{h})\mathfrak{P}_o + \mathcal{O}_{MAC}(\mathrm{h})\mathfrak{P}_s\sqrt{j/\mathfrak{o}_p\mathrm{h}_{max}}, \tag{6.5}$$

where $\mathfrak{P}_s, \mathfrak{P}_w,$ and $\mathfrak{P}_o$ are the number of MAC operations, the number of weights, and the number of outputs in the local model, respectively. Therefore, the total energy consumption of WBAN p in $\mathfrak{K}_p$ local training iteration is given by:

$$\mathcal{O}_p^{comp}(\mathrm{h}) = \mathfrak{K}_p\mathscr{O}_p(\mathrm{h}) = \mathfrak{K}_p\left(\mathcal{O}^{cm}(\mathrm{h}) + \mathcal{O}_p^{we}(\mathrm{h}) + \mathcal{O}_p^{ac}(\mathrm{h})\right). \tag{6.6}$$

Thus, the cost of energy consumption at WBAN p is defined as follows [139]:

$$\mathfrak{O}_p^{comp}(\mathrm{h}) = \alpha_p\big(\mathcal{O}_p^{comp}(\mathrm{h})\big)^2, \tag{6.7}$$

where α_p is the unit cost per energy consumption for WBAN p. It is proportional to the

overall severity index of WBAN p, i.e., $\alpha_p = f(\rho_p)$ [139]. Further, the overall severity index of WBAN p is defined as the average of the severity indices of all data samples at WBAN p, as follows [3]:

$$\rho_p = \frac{1}{D_p} \sum_{\mathfrak{n}_p^d \in \mathbb{D}_p} \varkappa_p^d, \tag{6.8}$$

where $\varkappa_p^d$ is the severity index of a data sample $\mathfrak{n}_p^d$ at WBAN p, defined as follows [38]:

$$\varkappa_p^d = \left| \frac{(\mathscr{X}_{up} - \mathfrak{n}_p^d)^2 - (\mathfrak{n}_p^d - \mathscr{X}_{low})^2}{(|\mathscr{X}_{up}| + |\mathscr{X}_{low}|)^2} \right|, \tag{6.9}$$

where $\mathscr{X}_{low}$ and $\mathscr{X}_{up}$ are the lower and the upper limits of the reference range, which is defined as the range of health data values under normal conditions for a healthy person[2]. The severity index value $\varkappa_p^d$ ranges between 0 and 1.

After the local model training, model weights are transmitted from the WBAN to the associated miner using the underlying cellular 5G network. The data transmission rate between WBAN p and miner m is calculated as $\mathfrak{V}_{p,m} = \mathfrak{p}_{p,m}\omega \log_2(1 + \mathfrak{S}_{p,m})$ [15], where $\mathfrak{p}_{p,m}$ is the number of allocated PRBs, and $\mathfrak{S}_{p,m}$ and ω represent Signal-to-Interference-plus-Noise Ratio[3] and bandwidth, respectively. However, the data transmission rate between WBAN and miner should be greater than the minimum required rate to ensure successful transmission of model weights, i.e., $\mathfrak{V}_{p,m} \geq \mathfrak{V}_{min}$. Additionally, to enhance the privacy of WBAN users, we encrypt the local model weights $\mathbf{w}_{\mathfrak{Q}}$ using the Paillier HE scheme [134] into $Enc(\mathbf{w}_{\mathfrak{Q}})$ before transmission to the associated miner. Therefore, the transmission time[4] for a WBAN to upload encrypted model weights to the miner

[2] A detailed explanation to calculate lower $\mathscr{X}_{low}$ and upper $\mathscr{X}_{up}$ limits, is given in Appendix A of [38].

[3] We assume that the channel exhibits flat fading. However, this can be easily extended to frequency-selective fading channels as well [15].

[4] We assume that download time between miners and WBANs is negligible compared to transmission time since downlink bandwidth is generally much larger than uplink bandwidth [140].

is given as follows [132]:

$$\mathfrak{q}_{p,m}^{trans}(\mathrm{h}) = \frac{||Enc(\mathbf{w}_{\Omega})||}{\mathfrak{V}_{p,m}} = \frac{||Enc(\mathbf{w})||\ \mathrm{h}}{\mathfrak{V}_{p,m}\ \mathrm{h}_{max}}, \tag{6.10}$$

where h represents the number of bits used for quantization, and $\mathbf{w}$ is represented using h_{max} bits.

The energy consumption for transmitting local model weights is given by [141]:

$$\mathcal{O}_{p,m}^{trans}(\mathrm{h}) = \varpi_p \mathfrak{q}_{p,m}^{trans}(\mathrm{h}), \tag{6.11}$$

where ϖ_p denotes the transmit power of WBAN p. Therefore, the transmission cost can be modeled as a linear function of transmission energy, formulated as [139]:

$$\mathfrak{O}_{p,m}^{trans}(\mathrm{h}) = \mathfrak{w}_p \mathcal{O}_{p,m}^{trans}(\mathrm{h}), \tag{6.12}$$

where $\mathfrak{w}_p$ represents the unit price of transmission energy.

Thus, the utility of WBAN p can be calculated as follows:

$$\mathcal{Z}_{p,m}^{g}(\mathrm{h}) = \mathfrak{B}_{p,m}^{g}(\mathrm{h}) - I\Big(\mathfrak{O}_{p}^{comp}(\mathrm{h}) + \mathfrak{O}_{p,m}^{trans}(\mathrm{h})\Big), \tag{6.13}$$

where I represents the number of global iterations, and $\mathfrak{B}_{p,m}^{g}(\mathrm{h})$ is the reward of WBAN p offered by associated miner m with reward level g (defined in Eq. (6.17)).

6.2.2 Utility of Miner

The blockchain network offers mining rewards to miners as an incentive for verifying and adding blocks to the blockchain. When a miner adds a block, it receives mining reward from the blockchain network [142]. To encourage WBANs' participation in the FL process, they also need to be incentivized. However, a miner provides a reward to

a WBAN only if they are associated with each other. Let $\mathbb{G} = \{1, \ldots, g, \ldots, G\}$ be the set of reward levels that miners are willing to allocate among the associated WBANs. A reward level indicates the percentage of revenue that a miner is willing to distribute to the associated WBANs, with g ranging between 0 and 1. Furthermore, we introduce a binary decision variable, $Y^g_{p,m}(\mathrm{h})$, as follows:

$$Y^g_{p,m}(\mathrm{h}) = \begin{cases} 1, & \text{WBAN } p \text{ using } j \text{ bits precision is associated to miner } m \\ & \text{with reward level } g; \\ 0, & \text{otherwise.} \end{cases} \tag{6.14}$$

Let Q be the maximum mining reward provided by the blockchain network for adding a block. In each iteration, each miner performs PoW multiple times and adds local models from WBANs into the blockchain[5]. We consider that a miner's reward is proportional to its relative computation power in the network[6]. Hence, the revenue of miner m for adding blocks in I global iterations is given as follows [143]:

$$\mathcal{Q}_m(\mathrm{h}) = I\left(Q\frac{\mathfrak{x}_m}{\sum_{p\in\mathbb{P}}\sum_{m\in\mathbb{M}}\sum_{g\in\mathbb{G}} Y^g_{p,m}(\mathrm{h})\mathfrak{x}_m} - \mathfrak{y}(\mathrm{h})\mathfrak{x}_m\right), \tag{6.15}$$

where $\mathfrak{x}_m$ represents the mining power of miner m, and $\mathfrak{y}(\mathrm{h})$ represents the unit cost of mining power for adding a block, represented using j bits.

Furthermore, we consider that the reward for a WBAN is proportional to the number of data samples and the overall criticality of the WBAN. Therefore, we introduce a parameter $\mathfrak{N}_p(\mathrm{h})$ that defines the importance of a WBAN, calculated as the weighted sum of the overall criticality and the proportion of data samples for that WBAN. Mathematically, parameter $\mathfrak{N}_p(\mathrm{h})$ of WBAN p is defined as follows:

$$\mathfrak{N}_p(\mathrm{h}) = \mathfrak{t}_1\frac{D_p}{\sum_{p\in\mathbb{P}}\sum_{m\in\mathbb{M}}\sum_{g\in\mathbb{G}} Y^g_{p,m}(\mathrm{h})D_p} + \mathfrak{t}_2\rho_p, \tag{6.16}$$

[5]Miners exchange and verify model weights, and then perform PoW to add a new block containing aggregated weights to the blockchain [20].

[6]We assume that there is at least one association in the network.

where $\mathfrak{t}_1$ and $\mathfrak{t}_2$ are weights given to the proportion of data samples and criticality, respectively, where[7] $\mathfrak{t}_1 + \mathfrak{t}_2 = 1$. Then, reward of WBAN p from miner m is defined as [20]:

$$\mathfrak{B}^g_{p,m}(\mathrm{h}) = g\ \mathcal{Q}_m(\mathrm{h})\ \mathfrak{N}_p(\mathrm{h}). \tag{6.17}$$

We define the utility of miner m as the difference between its revenue and the rewards of the associated WBANs, as:

$$\mathcal{S}_m(\mathrm{h}) = \mathcal{Q}_m(\mathrm{h}) - \sum_{p\in\mathbb{P}}\sum_{g\in\mathbb{G}} Y^g_{p,m}(\mathrm{h})\mathfrak{B}^g_{p,m}(\mathrm{h}). \tag{6.18}$$

6.2.3 Problem Formulation

In the blockchain based FL framework, both WBANs and miners require incentives for their participation in the FL process. Thus, the aim of WBANs and miners is to optimize their utility by maximizing their rewards and revenues, respectively. To achieve this, we formulate an optimization problem of maximizing the overall utility by determining suitable associations between WBANs and miner-reward level pairs while satisfying various constraints, as follows:

$$\textbf{P4:} \max_{Y^g_{p,m}(\mathrm{h})} \sum_{p\in\mathbb{P}}\sum_{m\in\mathbb{M}}\sum_{g\in\mathbb{G}} \Big(Y^g_{p,m}(\mathrm{h})\mathcal{Z}^g_{p,m}(\mathrm{h}) + \mathcal{S}_m(\mathrm{h})\Big) \tag{6.19}$$

Subject to the constraints:

$$\mathcal{Z}^g_{p,m}(\mathrm{h}) \geq 0, \tag{6.19a}$$

$$\sum_{p\in\mathbb{P}}\sum_{g\in\mathbb{G}} Y^g_{p,m}(\mathrm{h})\mathfrak{B}^g_{p,m}(\mathrm{h}) \leq \mathcal{Q}_m(\mathrm{h}), \tag{6.19b}$$

$$\mathfrak{V}_{p,m} \geq \mathfrak{V}_{min}, \tag{6.19c}$$

$$Y^g_{p,m}(\mathrm{h}) \in \{0,1\}, \tag{6.19d}$$

[7]The values of $\mathfrak{t}_1$ and $\mathfrak{t}_2$ may depend on age, sex and medical history of the WBAN user [38].

$\forall p \in \mathbb{P}, \forall m \in \mathbb{M}$ and $\forall g \in \mathbb{G}$. Constraint in Eq. (6.19a) ensures that the utility of each WBAN is non-negative. Constraint in Eq. (6.19b) specifies that the total reward distributed by a miner to its associated WBANs should not exceed the miner's revenue. Constraint in Eq. (6.19c) states the minimum data rate requirement for WBANs. Constraint in Eq. (6.19d) is described in the Eq. (6.14).

The formulated problem **P4** is computationally hard, as discussed in the following.

Theorem 6.1 *Utility maximization problem **P4** is NP-hard.*

Proof: To prove the NP-hardness of the formulated problem **P4**, we map it to the multiple subset sum problem [144]. For simplicity, Constraints in Eqs. (6.19a) and (6.19c) are warded off. Multiple subset sum problem involves finding subsets of given items with varying values, such that the sum of each subset does not exceed its capacity, while maximizing the sum across all subsets. We map the set of miners $\mathbb{M}$ to M subsets with capacity $\mathcal{Q}_m(\mathrm{h})$ each, and the set of WBANs $\mathbb{P}$ to P items with sizes $\mathfrak{B}^g_{p,m}(\mathrm{h})$. The goal is to form M subsets using items from $\mathbb{P}$ while ensuring that the total sizes of items in each subset do not exceed its capacity, i.e., $\sum_{p\in\mathbb{P}} \sum_{g\in\mathbb{G}} Y^g_{p,m}(\mathrm{h}) \mathfrak{B}^g_{p,m}(\mathrm{h}) \leq \mathcal{Q}_m(\mathrm{h})$. Therefore, the maximization problem **P4** can be represented as a multiple subset sum problem, which is a well known NP-hard problem [144]. Thus, the formulated problem **P4** is NP-hard. □

Due to the high conditionality and complexity of the proposed maximization problem, this chapter proposes an algorithm based on the DAA to provide a feasible sub-optimal solution, described in the following section.

6.3 Proposed Scheme

The proposed scheme for smart healthcare consists of two stages: (1) WBAN-Miner Association (WMA); and (2) Efficient blockchain based FL, as discussed in Section 6.2. In the WMA stage, a trusted entity executes Algorithm 6.1 (levels 1, 2, and 3 in

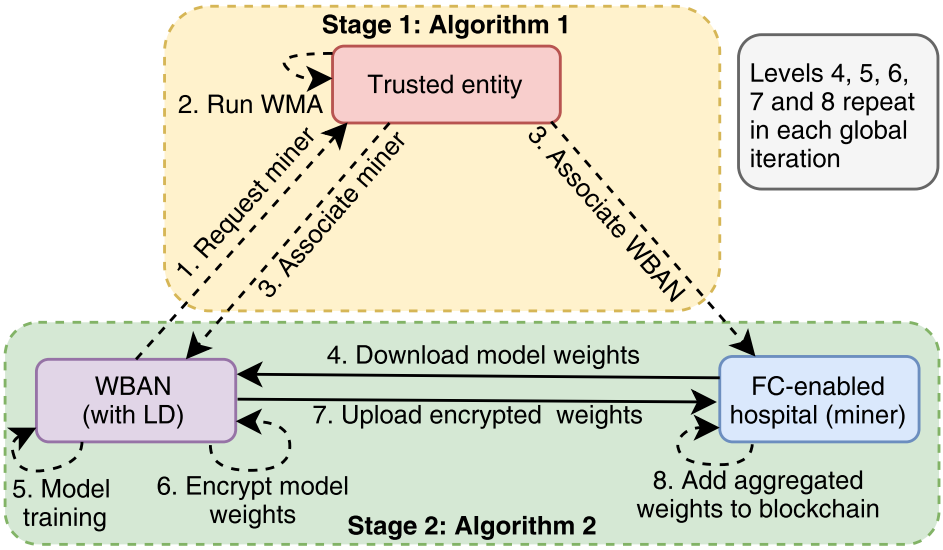


Fig. 6.2. Data flow diagram of the proposed framework.

Fig. 6.2) to associate WBANs, miners, and reward levels by considering the utilities of WBANs and miners using DAA. After association, the FL process starts between WBANs and miners, i.e., Algorithm 6.2 (levels 4, 5, 6, 7, and 8 in Fig. 6.2), where the associated WBANs train local models, encrypt the model weights, and transmit them to the associated miner. Miners then aggregate the encrypted model weights and add them to the blockchain. Labels 1, 2, 3, 5, 6, and 8 are handled by control signals (e.g., beacons [15]), whereas labels 4 and 7 are handled by data signals.

6.3.1 Stage 1: WBAN-Miner Association

Associations of WBANs, miners, and reward levels are formed in coordination with a trusted entity, as shown in Figs. 6.1 and 6.2. An association is defined as an allocation of a miner and corresponding reward level to WBANs, forming the set $\{p, m, g\} \in \mathbb{P}\times\mathbb{M}\times\mathbb{G}$. While a miner can be allocated multiple WBANs, each WBAN can only be assigned to a single miner at a specific reward level, as described below:

Definition 6.1 *WMA: An association Ψ between WBAN p and miner m with reward level g is define as a function, i.e., $\Psi : \mathbb{P} \times \mathbb{M} \times \mathbb{G} \rightarrow \mathbb{P} \times \mathbb{M} \times \mathbb{G}$ such that,*

(i) $\Psi(p) \in \mathbb{M} \times \mathbb{G} \cup \{\varnothing\}$ *and* $|\Psi(p)| \in \{0, 1\}$

(ii) $\Psi(m) \in \mathbb{P} \times \mathbb{G}$ *and* $|\Psi(m)| \in \{1, 2, \ldots, P\}$

where $\Psi(p)=(m,g) \Leftrightarrow \Psi(m)=(p,g)$, $\forall p \in \mathbb{P}, \forall m \in \mathbb{M}, \forall g \in \mathbb{G}$, and $|\Psi(.)|$ denotes cardinality of association outcome $\Psi(.)$.

Definition 6.1 implies that Ψ is a many-to-one association, meaning that Ψ is unique for a given WBAN p. The interpretation of $\Psi(p) = \varnothing$ indicates that no association exists for WBAN p due to the violation of constraints. The association result determines the set of associated miners and their corresponding reward levels, i.e., $\mathbb{Y} \equiv \Psi$, where:

$$\mathbb{Y} = \{Y^g_{p,m}(\mathrm{h}) \mid Y^g_{p,m}(\mathrm{h}) = 1\}. \tag{6.20}$$

6.3.1.1 Proposed WMA Algorithm

We adopt a modified version of the DAA [30] in the proposed WMA due to its feasibility and stability, allowing it to find a stable association, as described in the following.

To find a stable association between WBANs and miner-reward level pairs, it is necessary to create preference lists for WBANs and miners, denoted as $\mathcal{P}_p(\mathbb{M}, \mathbb{G})$ and $\mathcal{P}_m(\mathbb{P}, \mathbb{G})$ respectively, while satisfying constraints in Eqs. (6.19a) and (6.19c) from problem **P4**. Particularly, WBANs check constraint in Eq. (6.19a) when preparing their preference lists and include a miner-reward level pair only if the constraint is satisfied. WBANs then arrange the miner-reward level pairs in decreasing order of preference based on their utility. The preference list for WBAN p over the set of all (m, g) pairs can be constructed using the following relationship:

$$(m, g) \succeq_p (m', g') \Leftrightarrow \mathcal{Z}^g_{p,m}(\mathrm{h}) \geq \mathcal{Z}^{g'}_{p,m'}(\mathrm{h}). \tag{6.21}$$

On the contrary, miners check constraint in Eq. (6.19c) while setting up the preference list and include WBANs in the list that fulfill the constraint. A miner prefers

a subset $\mathcal{F}$ of WBAN-reward level pairs to another subset $\mathcal{G}$ if either *(i)* $\mathcal{F}$ contains WBAN-reward level pairs, i.e., (p, g) that satisfy constraint in (6.19b) and the miner's utility is higher when associated with the pairs in $\mathcal{F}$ or *(ii)* $\mathcal{F}$ contains WBAN-reward level pairs that violate constraint in Eq. (6.19b). Following [55], the preference list of miner m is defined as:

$$\mathcal{F} \succeq_m \mathcal{G} \Leftrightarrow \begin{cases} (i)\ \mathfrak{U}_m^{\mathcal{F}}(\mathrm{h}) \ \geq\ \mathfrak{U}_m^{\mathcal{G}}(\mathrm{h});\ \ \sum_{p\in\mathcal{F}} \sum_{g\in\mathbb{G}} Y_{p,m}^{g}(\mathrm{h})\, \mathfrak{B}_{p,m}^{g}(\mathrm{h}) \ \leq \\ \mathcal{Q}_m(\mathrm{h}), \sum_{p\in\mathcal{G}} \sum_{g\in\mathbb{G}} Y_{p,m}^{g}(\mathrm{h})\ \mathfrak{B}_{p,m}^{g}(\mathrm{h}) \leq \mathcal{Q}_m(\mathrm{h}) \text{ or}, \\ (ii)\ \sum_{p\in\mathcal{G}} \sum_{g\in\mathbb{G}} Y_{p,m}^{g}(\mathrm{h})\, \mathfrak{B}_{p,m}^{g}(\mathrm{h}) > \mathcal{Q}_m(\mathrm{h}), \end{cases} \tag{6.22}$$

where $\mathfrak{U}_m^{\mathcal{F}}(\mathrm{h})$ and $\mathfrak{U}_m^{\mathcal{G}}(\mathrm{h})$ represent the utility of miner m when associated with the WBAN-reward level pairs in $\mathcal{F}$ and $\mathcal{G}$, respectively.

Algorithm 6.1 outlines the process of associating WBANs with miners. The algorithm begins by initializing association variables, waiting lists, and candidate lists in lines 1-3. Preference lists $\mathcal{P}_p(\mathbb{M}, \mathbb{G})$ and $\mathcal{P}_m(\mathbb{P}, \mathbb{G})$ are then created for WBANs and miners, respectively, while satisfying constraints in Eqs. (6.19a) and (6.19c) (line 4). In each iteration of the allocation process, miners find a set of (p, g) pairs, denoted as $\mathfrak{D}_m$, that maximize their utility while satisfying constraint in Eq. (6.19b) (line 6). If $\mathfrak{D}_m$ is empty for all miners, the algorithm terminates (lines 7-8). For each pair in $\mathfrak{D}_m$, the miner applies for association and updates its candidate list (lines 10-12). WBAN p adds the (m, g) pair to its waiting list (line 13). For each WBAN with a non-empty waiting list (line 14), the WBAN accepts the (m, g) pair if constraint in Eq. (6.19b) is satisfied and updates the relevant variables accordingly (lines 16-21). Otherwise, WBAN rejects and removes the (m, g) pair from the waiting list and continues the process (lines 22-25). This process repeats until all WBANs are associated, or some miners still have non-empty candidate lists (lines 5-26).

Algorithm 6.1: WMA Algorithm

Input: $\mathbb{P}$, $\mathbb{M}$, $\mathbb{G}$, $\mathcal{Z}^g_{p,m}(\mathrm{h})$, $\mathcal{S}_m(\mathrm{h})$, $\mathfrak{B}^g_{p,m}(\mathrm{h})$, $\mathcal{Q}_m(\mathrm{h})$, $\mathfrak{V}_{p,m}$, $\mathfrak{V}_{min}$, $\forall p \in \mathbb{P}, \forall m \in \mathbb{M}, \forall g \in \mathbb{G}$

Output: Association $\mathbb{Y}$

$\mathbb{Y} = \varnothing, Y^g_{p,m}(\mathrm{h}) = 0, \forall p \in \mathbb{P}, \forall m \in \mathbb{M}, \forall g \in \mathbb{G}$

$\forall p \in \mathbb{P}, \Psi(p) = \varnothing$, Waiting list $\mathfrak{M}_p = \varnothing$

$\forall m \in \mathbb{M}, \Psi(m) = \varnothing$, candidate list $\mathcal{F}_m = \mathbb{P} \times \mathbb{G}$

Create preference lists $\mathcal{P}_p(\mathbb{M}, \mathbb{G})$ and $\mathcal{P}_m(\mathbb{P}, \mathbb{G})$ of WBANs and miners, respectively while satisfying *constraints in Eqs.* (6.19a) *and* (6.19c)

while $\exists\, p : \Psi(p) = \varnothing$ *and* $\exists\, m : \mathcal{F}_m \neq \varnothing$ **do**

  Find the set of (p, g) pairs satisfying the *constraint in Eq.* (6.19b) as $\mathfrak{D}_m$, $\forall m$

  if $\forall m \in \mathbb{M}, \mathfrak{D}_m = \varnothing$ **then**

    return $\mathbb{Y}$

  else

    for *every* $(p, g) \in \mathfrak{D}_m$ **do**

      Miner m applies for (p, g)

      Miner m removes (p, g) from the candidate list, $\mathcal{F}_m = \mathcal{F}_m \backslash \{(p, g)\}$

      WBAN p adds (m, g) to its waiting list, i.e., $\mathfrak{M}_p \leftarrow \mathfrak{M}_p \cup \{(m, g)\}$

  for *every WBAN* p *with* $\mathfrak{M}_p \neq \varnothing$ **do**

    repeat

      Find the most preferred (m, g) pair in $\mathfrak{M}_p$

      if *constraint in Eq.* (6.19b) *is satisfied for* m **then**

        WBAN p accepts (m, g) pair and rejects others in $\mathfrak{M}_p$

        Update $Y^g_{p,m}(\mathrm{h})$ and $\mathbb{Y}$ for all pairs in $\mathfrak{M}_p$ `// constraint in Eq.` (6.19d)

        Set $\mathfrak{M}_p$ empty, i.e., $\mathfrak{M}_p = \varnothing$

        break

      else

        WBAN rejects and removes (m, g) from waiting list

        $\mathfrak{M}_p \leftarrow \mathfrak{M}_p \backslash \{(m, g)\}$

        $\mathcal{F}_m = \varnothing$

        continue

    until $|\mathfrak{M}_p|$ **times**;

6.3.1.2 Analysis of WMA Algorithm

To ensure the stability of the association algorithm, it is crucial to avoid the existence of Blocking Pairs (BPs) in the associations. If the association is unstable, a WBAN might be willing to change its association if favorable to the WBAN. Such a network with

unstable associations results in unsatisfactory and unreliable associations. Therefore, for a stable WMA, it is necessary to satisfy the condition of the nonexistence of BPs. We formally define a BP as follows:

Definition 6.2 *BP: For every WBAN p, a pair $(p,(m',g'))$ is defined as a BP if the following conditions are satisfied:*

- *p associated with (m'',g'') pair.*
- *Miner m' is able to associate with WBAN p by satisfying constraint in Eq.* (6.19b) *of problem* ***P4****.*
- *There exist another candidate association $(p,(m',g'))$: $\mathcal{Z}^{g'}_{p,m'}(\mathrm{h}) > \mathcal{Z}^{g''}_{p,m''}(\mathrm{h}), \forall m'$, $m'' \in \mathbb{M}, \forall g', g'' \in \mathbb{G}$.*

Definition 6.2 indicates that the WBAN desires to change the association, implying instability in the association. Further, we define the stability of the WMA in the following.

Definition 6.3 (Stability) *WMA is stable if it doesn't contain BPs.*

As a result, we present Lemma 2 concerning the stability of the WMA formed by applying Algorithm 6.1.

Lemma 2 *WMA Algorithm gives stable association.*

Proof: To prove the stability of the WMA algorithm, we need to show that no BP exists. Let us consider a BP $(p,(m',g'))$ for WBAN p after its association with (m'',g''). According to Definition 6.2, $(p,(m',g'))$ should satisfy $\mathcal{Z}^{g'}_{p,m'}(\mathrm{h}) > \mathcal{Z}^{g''}_{p,m''}(\mathrm{h})$. As per Algorithm 6.1, if WBAN p accepts the (m',g') pair, it implies that the utility obtained by associating with (m',g') is higher than the utility obtained by associating with (m'',g''). However, WBAN p fails to form an association with (m',g') only if its utility with (m',g') is higher than the utility obtained from the association with (m'',g''). This contradicts with $(p,(m',g'))$, i.e., $\mathcal{Z}^{g'}_{p,m'}(\mathrm{h}) > \mathcal{Z}^{g''}_{p,m''}(\mathrm{h})$. Therefore, no BP exists after

applying Algorithm 6.1 to form associations between WBANs and miners, which proves the Lemma. □

Theorem 6.2 *Time complexity of Algorithm 6.1 is* $O(MP^2G)$.

Proof: Algorithm 6.1 iteratively forms associations between WBANs and miner-reward level pairs. Initialization of variables (lines 1-3) takes constant time, i.e., $O(1)$. Creating preference lists of WBANs and miners using Eqs. (6.21) and (6.22) take time complexity of $O(MG \log MG)$ and $O(PG \log PG)$, respectively. Since the number of WBANs is larger than the number of miners, the time complexity of line 4 is $O(PG \log PG)$. Finding the set of (p, g) pairs for each miner takes time complexity of $O(PG)$ in the worst-case (line 6). Therefore, line 6 takes $O(MPG)$ time complexity. Lines 7-8 take $O(M)$ and lines 9-13 take $O(PG)$. For each WBAN p, lines 15-26 repeat MG times in the worst-case. Thus, lines 14-26 take $O(PMG)$ time complexity. Since the number of iterations in Algorithm 6.1 depends on the number of WBANs, i.e., P (lines 5-26), the overall time complexity of Algorithm 6.1 is $O(MP^2G)$. □

This concludes Stage 1, i.e., the association between WBANs and miner-reward level pairs. Following the association, an efficient blockchain based FL for smart healthcare system begins (see Fig. 6.2), as discussed in the following.

6.3.2 Stage 2: Efficient blockchain based FL

The proposed blockchain based FL model comprises two components: *(i)* Blockchain for distributed model weight sharing, and *(ii)* Local model training by WBANs using their local data. After the association (i.e., Stage 1), each WBAN trains a shared model using j precision level. We denote the weights associated with the local model of WBAN p as $\mathbf{w}^{(p)}$. We introduce the loss function $loss(\mathbf{w}^{(p)}, \mathfrak{n}_p^d)$ of the model, which indicates the FL performance over an input sample[8]. Local model training at WBAN

[8]Various learning problems use different loss functions, such as cross-entropy, mean squared error, and log-likelihood [145].

p using its data $\mathbb{D}_p$ is defined as follows [146]:

$$\min_{\mathbf{w}^{(p)}} \mathcal{I}_p(\mathbf{w}^{(p)}) := \min_{\mathbf{w}^{(p)}} \frac{1}{D_p} \sum_{\mathfrak{n}_p^d \in \mathbb{D}_p} loss(\mathbf{w}^{(p)}, \mathfrak{n}_p^d). \tag{6.23}$$

Moreover, the FL process aims to minimize the global loss over the collection of all associated WBANs by finding the optimal weights $\mathbf{W}^I$, as follows:

$$\mathbf{W}^I = \arg\min_{\mathbf{W}} \frac{1}{|\mathbb{Y}|} \sum_{p \in \mathbb{P}} \sum_{m \in \mathbb{M}} \sum_{g \in \mathbb{G}} Y_{p,m}^g(\mathrm{h}) \mathcal{I}_p(\mathbf{w}^{(p)}), \tag{6.24}$$

where $\mathbf{W}$ represents the weight of the global model, and $|\mathbb{Y}|$ denotes the number of associations, which is equal to the number of WBANs participating in the FL process. Eq. (6.24) is solved using the Stochastic Gradient Descent (SGD) algorithm through multiple communications between WBANs and miners. However, WBANs are generally low energy-constrained devices and are unable to train local FL models. To reduce the energy consumption for local model computation and transmission, we use QNN with fixed-point format rather than the standard 32-bit floating-point format [132], as described in Algorithm 6.2. We consider one bit to represent integer part and $(j-1)$ bits to represent fractional parts. Let ι be the smallest positive number that can be represented using j bits, where $\iota = 2^{-j+1}$. As a result, the range of numbers that can be represented with j bits lies between $[-1, 1-2^{-j+1}]$. For any weight $w \in \mathbf{w}$, the quantized weight using stochastic quantization scheme is given as [132]:

$$\mathfrak{Q}(w) = \begin{cases} \lfloor w \rfloor, & \text{with probability } \frac{\iota - w + \lfloor w \rfloor}{\iota}; \\ \lfloor w \rfloor + \iota, & \text{with probability } \frac{w - \lfloor w \rfloor}{\iota}, \end{cases} \tag{6.25}$$

where $\lfloor w \rfloor$ is the greatest integer multiple of ι less than or equal to w. The weight w is clipped between $[-1, 1]$, as:

$$clip(w) = \begin{cases} -1, & \text{if } w \leq -1; \\ 1, & \text{if } w \geq 1; \\ w, & \text{otherwise.} \end{cases} \tag{6.26}$$

In each global iteration, WBANs and miners communicate the local model weights multiple times (given in Eq. (6.30)). However, sharing model weights raises concerns about potential privacy leakage. To mitigate this risk, we use DP during local model training, which ensures that the output of a differentially private algorithm gives the same output with l error whether or not a local data sample is included in the algorithm's input. l is the privacy budget, i.e., the bound on the loss of privacy. We use a variant of DP introduced in [133], that satisfies (l, j)-DP, where j defines a bound that the privacy guarantee does not hold (which is a preferably very small positive number).

Definition 6.4 *A randomized algorithm $\mathbb{Z} : \mathfrak{Y} \rightarrow \mathfrak{X}$ with domain $\mathfrak{Y}$ and range $\mathfrak{X}$ satisfies (l, j)-DP if, for any two adjacent datasets $\mathfrak{I}'$ and $\mathfrak{I}''$ that differ by one data sample, and for any subset $\mathfrak{Z} \subseteq \mathfrak{X}$, following condition holds [133]:*

$$Pr[\mathbb{Z}(\mathfrak{I}') \in \mathfrak{Z}] \leq e^{\mathrm{l}} Pr[\mathbb{Z}(\mathfrak{I}'') \in \mathfrak{Z}] + \mathrm{j}. \tag{6.27}$$

Algorithm 6.2 initializes the model weights $\mathbf{w}^{(0)}$ (line 1), encrypts them, and adds them to the blockchain. Each WBAN downloads the encrypted model weights from its associated miner, decrypts them into $\mathbf{w}^{(0)}$, and initializes its local model weights (line 4). In each local iteration, the gradient of the loss $\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})$ is computed, and it is clipped using the $L2$ norm (line 6), as follows:

$$\mathrm{H}' = \Delta\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)}) / \max\left(1, \frac{||\Delta\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})||_2}{A}\right), \tag{6.28}$$

where $\mathbf{w}_{\mathfrak{Q}}^{(p,i)} = \mathfrak{Q}(\mathbf{w}^{(p,i)})$ is the quantized model weights. This clipping ensures that if $||\Delta\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})||_2 \leq A$, then $\Delta\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})$ is preserved, whereas if $||\Delta\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})||_2 > A$, gradient gets scaled down to be of norm A. Further, the Gaussian noise is added to the clipped gradient in order to protect privacy (line 7), as given below:

$$\mathrm{H}'' = \mathrm{H}' + \mathcal{N}(0, \sigma^2 A^2 \mathbb{I}), \tag{6.29}$$

where $\mathcal{N}(0, \sigma^2 A^2 \mathbb{I})$ is the Gaussian noise, with noise scale σ, gradient bound A, and identity matrix $\mathbb{I}$. Then, WBANs update the model weights at x-th ($\mathrm{x} \in [1, \mathfrak{K}_p]$) local iteration for optimizing the loss function (line 8) as follows [133]:

$$\mathbf{w}_{\mathfrak{Q}}^{(p,\mathrm{x}+1)} = \mathbf{w}_{\mathfrak{Q}}^{(p,\mathrm{x})} - \mathfrak{l}\mathrm{H}'', \tag{6.30}$$

where $\mathfrak{l}$ is the learning rate. After local model training at i-th global iteration, each WBAN uploads its local model weights to the associated miner for model aggregation (line 9). However, the uploaded model weights can reveal significant statistical patterns of the local dataset [126]. Therefore, WBANs encrypt the local model weights $\mathbf{w}_{\mathfrak{Q}}^{(p,i)}$ before transmitting them to the associated miner using the Paillier HE scheme [134], and the encrypted weights are denoted by $Enc(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})$. Thus, local model weights remain unknown to the miners, thereby preventing information leakage [126].

After receiving model weights from associated WBANs, miners aggregate the weights (line 11) as follows [68]:

$$Enc(\boldsymbol{w}_m^{(i+1)}) = \sum_{p\in\mathbb{P}} \sum_{g\in\mathbb{G}} Y_{p,m}^{g}(\mathrm{h}) \, \frac{D_p}{\mathcal{D}_m} \, Enc(\mathbf{w}_{\mathfrak{Q}}^{(p,i)}), \tag{6.31}$$

where $\mathcal{D}_m = \sum_{p\in\mathbb{P}, u\in\mathbb{G}: Y_{p,m}^{g}(\mathrm{h})=1} D_p$. Miners perform PoW to add the aggregated weights $Enc(\boldsymbol{w}_m^{(i+1)})$ to the blockchain for distributed model weight sharing (line 12). Then, the block containing the weights is broadcasted to all miners (line 13). Additionally,

Algorithm 6.2: Efficient blockchain based FL

Input: Training samples $\mathbb{D}_p$, learning rate $\mathfrak{l}$, $\mathcal{I}_p(\mathbf{w}_{\mathfrak{Q}}^{(p)})$, no. of global iteration I, gradient bound A, $\mathbb{Y}$.
Output: Optimal weights $\mathbf{W}^I$.

1 **Initialization:** Add initial weights $\mathbf{w}^{(0)}$ to blockchain
2 **for** *every global iteration* $i = 1, 2, \ldots, I$ **do**
    `// Local Model Training at WBANs`
3 **for** *every* $p \in \mathbb{P}, Y_{p,m}^{g}(\mathrm{h}) = 1$ **do** `// Perform in parallel`
4 Download and initialize model weights
5 **for** *every local iteration* $\mathrm{x} = 1, 2, \ldots, \mathfrak{K}_p$ **do**
6 Compute the gradient using Eq. (6.28)
7 Add noise to gradient using Eq. (6.29)
8 Update $\mathbf{w}_{\mathfrak{Q}}^{(p,\mathrm{x}+1)} = \mathbf{w}_{\mathfrak{Q}}^{(p,\mathrm{x})} - \mathfrak{l}\mathrm{H}''$
    `// Encryption at WBAN`
9 Upload $Enc(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})$ to associated miner
    `// FC-enabled Hospitals (Miners)`
10 **for** *every* $m \in \mathbb{M}$ **do**
11 Aggregate encrypted weights as $Enc(\boldsymbol{w}_m^{(i+1)}) = \sum_{p\in\mathbb{P}} \sum_{g\in\mathbb{G}} Y_{p,m}^{g}(\mathrm{h}) \frac{D_p}{\mathcal{D}_m} Enc(\mathbf{w}_{\mathfrak{Q}}^{(p,i)})$
12 Perform PoW to add $Enc(\boldsymbol{w}_m^{(i+1)})$ to blockchain
13 Broadcast the new block to all miners
14 Verify and add to blockchain
15 Aggregate encrypted weights from all miners: $Enc(\mathbf{W}^{(i+1)}) = \sum_{m\in\mathbb{M}} \frac{\mathcal{D}_m}{\mathscr{D}} Enc(\boldsymbol{w}_m^{(i+1)})$

miners verify and add the received weights from other miners in parallel (line 14). Finally, miners use the weights stored in the blockchain to compute the global model weights for the subsequent global iteration (line 15) as follows [68]:

$$Enc(\mathbf{W}^{(i+1)}) = \sum_{m\in\mathbb{M}} \frac{\mathcal{D}_m}{\mathscr{D}} Enc(\boldsymbol{w}_m^{(i+1)}), \tag{6.32}$$

where $\mathscr{D}$ is the total data samples, i.e., $\mathscr{D} = \sum_{m\in\mathbb{M}} \mathcal{D}_m$.

After the global model aggregation, each WBAN downloads the global model weights, decrypts them, and updates its local weights accordingly. Subsequently, the WBANs encrypt and upload the updated local weights to their associated miners. This iterative

process continues for each global iteration (lines 2-15). Finally, the FL process obtains the optimal weights as $\mathbf{W}^I$.

6.3.2.1 Analysis of proposed Algorithm 6.2

This section presents an analysis of privacy protection, communication cost, and HE in the proposed framework.

Theorem 6.3 *Proposed efficient blockchain based FL framework is privacy preserved.*

Proof: In the proposed framework, we employ Paillier HE to improve privacy and security. The Paillier HE scheme is based on the Deterministic Composite Residue Assumption (DCRA), which has not been broken by any polynomial-time algorithm as of now [18]. The local model weights uploaded to miners are encrypted, and global model aggregation is achieved using homomorphic operations, i.e., no decryption is required by the miners. This ensures that all model weights on miners remain encrypted, i.e., miners cannot access any model weights without the secret key, thus preserving the privacy of WBAN users. Furthermore, the blockchain provides a robust and tempered-resistant framework for sharing model weights. Thus, the privacy of WBAN users can be protected. □

Theorem 6.4 *Communication cost of Algorithm 6.2 is* $O(I|\mathbf{w}|(|\mathbb{Y}| + M^2))$.

Proof: We analyze the communication cost of Algorithm 6.2 by considering the number of model weights. Let $|\mathbf{w}|$ be the number of weights in a local model. In FL, both uploading and downloading local model weights require $|\mathbf{w}|$ communications. Therefore, communication per WBAN in each global iteration is $2|\mathbf{w}|$ [147]. As $|\mathbb{Y}|$ WBANs participate in the FL process, the communication required for all WBANs in each global iteration is $2|\mathbb{Y}||\mathbf{w}|$. Similarly, miners in the blockchain broadcast M aggregated models (line 13), and broadcasting $|\mathbf{w}|$ model weights require at least $(M-1)|\mathbf{w}|$ communication. Thus, communication for all miners in each global iteration is $M(M-1)|\mathbf{w}|$.

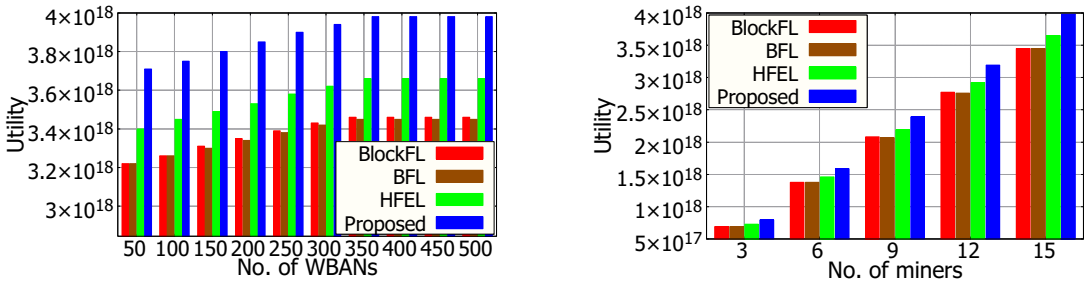
Since lines 2-15 iterate over I global iterations, the overall communication required in I global iterations is $I(2|\mathbb{Y}||\mathbf{w}| + M^2|\mathbf{w}| - M|\mathbf{w}|)$. As $|\mathbb{Y}| \gg M$ in general, the communication cost of Algorithm 6.2 can be expressed as $O(I|\mathbf{w}|(|\mathbb{Y}| + M^2))$. □

6.4 Performance Analysis

We consider [50-500] WBANs and [3-15] miners in our simulation. Unless stated otherwise, the global iteration I is set to 10, and the local iteration $\mathfrak{K}_p$ is set to 5. The bandwidth is set to 20 MHz [15], and the number of PRBs is taken as [5-15] [3]. The transmission power ϖ_p of WBANs is set to 100 mW [20]. The reward level g is taken between [0-1], and the unit cost $\mathfrak{y}(\mathrm{h})$ is set to 0.05. The parameters $\mathfrak{A}$ and z are taken as 3.27 pJ and 1.25, respectively [132]. The value of Q is set to 10^{18} units, while α_p varies between [0-1]. The local model size is taken as 3694.128 KB. Parameters $\mathfrak{P}_s$, $\mathfrak{P}_w$, and $\mathfrak{P}_o$ are taken as 20.64×10^6, 76961, and 480, respectively [132]. The value of $\mathfrak{x}_m$ is taken between [22-30], and the number of data samples D_p is taken as 837. The parameters j and h_{max} are set to 8 and 32, respectively [132]. The proposed framework is implemented using Python 3.9 and Tensorflow 2.0 on a Windows 10 Home PC with Intel® Core™ i7-10750H @ 2.60 GHz processor and 16 GB of memory. To simulate sensor and WBAN data, we use the ECG data from the MIT-BIH arrhythmia dataset [148], comprising 26,490 data samples with 5 classes. Our proposed model uses QNN with an SGD optimizer, comprising 4 dense layers with 256,

Table 6.1: Simulation parameter setting

Parameters	**Values**
M, P	[3-15], [50-500]
Iterations	$I = 10, \mathfrak{K}_p = 5$
Bandwidth [15]	20 MHz
$\mathfrak{S}_{p,m}, \mathfrak{p}_{p,m}$ [3]	[13-20] dB, [5-15]
ϖ_p [20], g	100 mW, [0-1]
$\mathfrak{A}$, z [132], $\mathfrak{o}_p$	3.7 pJ , 1.25, 50
$\mathfrak{l}, \mathfrak{j}, A, \sigma$	$0.001, 10^{-5}, 1, 0.25$
Q, α_p	10^{18} units, [0-1]
$\mathfrak{w}_p, \mathfrak{y}(\mathrm{h})$	0.05 unit, 0.05 unit
Model weight size	3694.128 KB
$\mathfrak{P}_s, \mathfrak{P}_w, \mathfrak{P}_o$ [132]	$20.64 \times 10^6, 76961, 480$
$\mathfrak{x}_m, D_p$	$[22 - 30]$, 837
$\mathrm{h}, \mathrm{h}_{max}$ [132], $\mathfrak{t}_1, \mathfrak{t}_2$	8, 32, 0.5, 0.5



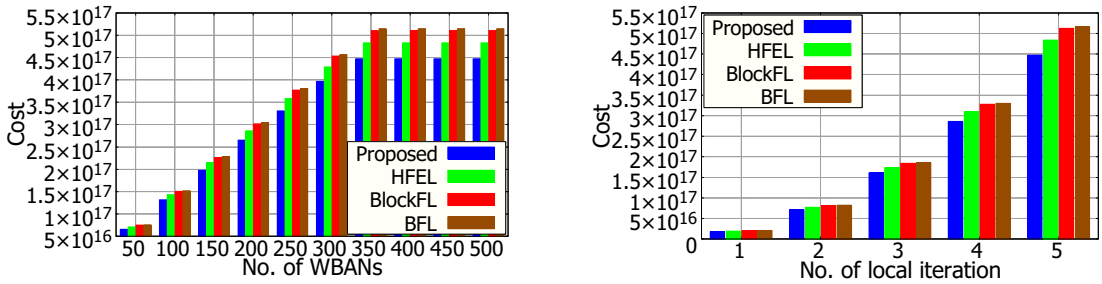
(a) Utility v/s WBANs **(b)** Utility v/s miners

Fig. 6.3. Utility analysis.

128, 64, 32, and 1 (output layer) neurons. Each dense layer is followed by a ReLu layer, and the learning rate is set to 0.001. Moreover, Table 6.1 shows the key parameters used in the experiment.

We compare our results with BlockFL [20], HFEL [68], and BFL [69] schemes on the same simulation parameters. Specifically, we compare our results with BlockFL, HFEL, and BFL since all these works consider user association and FL together, as shown in Table 2.4. Moreover, unlike other existing works in the literature, these works are closely related to our proposed method to the best of our knowledge. BlockFL and BFL utilize random association for matching devices to miners. Moreover, HFEL scheme employs a stable edge association algorithm to match devices with edge servers. We consider the devices used in BlockFL, HFEL, and BFL as WBAN users, and the same neural network is utilized across all three schemes. Moreover, computation and communication resources between WBAN users and miners are fixed to ensure a fair comparison with HFEL.

Utility Analysis: Fig. 6.3 compares the utility of the proposed scheme with BlockFL, HFEL, and BFL. The proposed scheme outperforms BlockFL, HFEL, and BFL, achieving 15.1%, 9.03%, and 15.35% more utility on an average, respectively. The reason is that BlockFL and BFL schemes randomly assign WBANs to miners without considering their utility, while HFEL considers the preferences of edge servers when al-



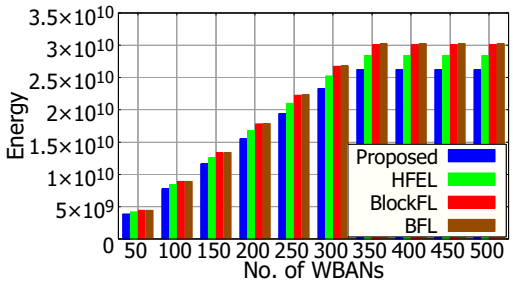
(a) Cost v/s WBANs **(b)** Cost v/s local iteration

Fig. 6.4. Cost analysis.

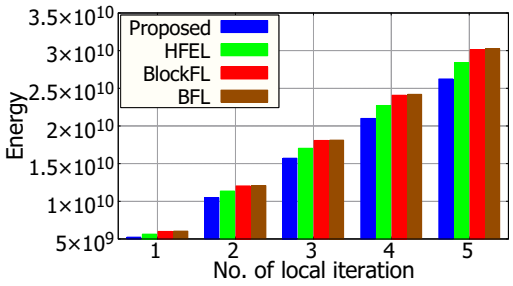
locating miner-reward level pairs to WBANs. This leads to higher energy consumption for WBANs and, consequently, lower utility. In contrast, the proposed scheme considers various parameters, such as energy, rewards, and revenue, and allocates WBANs and miner-reward pairs by minimizing energy consumption, leading to higher utility. Moreover, the utility becomes constant as the number of WBANs exceeds 350 (Fig. 6.3a), as no more WBANs can be associated without violating the constraints of formulated problem **P4**. Moreover, we observe that the utility increases with the number of miners, as can be seen from Fig. 6.3b.

Cost Analysis: Fig. 6.4 compares WBAN users' cost in the proposed scheme with BlockFL, HFEL, and BFL under various settings. We observe that the proposed scheme incurs lower costs than that of BlockFL, HFEL, and BFL (Fig. 6.4a). It is because the proposed scheme considers different parameters and allocates WBANs and miner-reward pairs by minimizing energy consumption. In contrast, BlockFL, and BFL randomly assign WBANs without considering cost, and HFEL only considers WBAN users' preferences when assigning miner-reward level pairs to WBANs, resulting in higher costs and lower utility. In Fig. 6.4b, we observe that the cost increases with the number of local iterations because more computation is required, resulting in higher costs.

Energy Analysis: Fig. 6.5 compares the energy consumption of the proposed

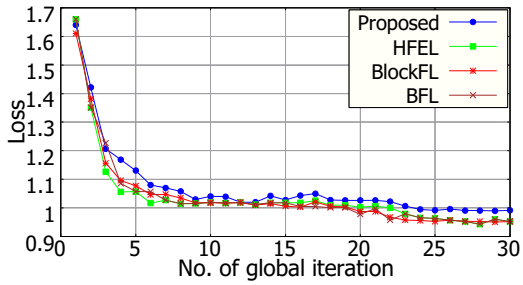


(a) Energy v/s WBANs

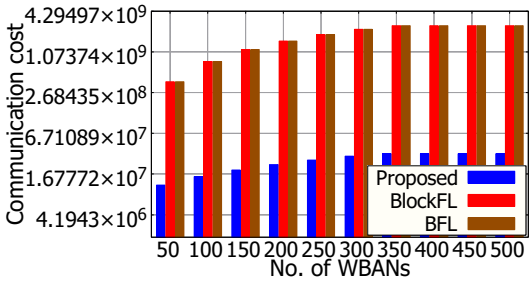


(b) Energy v/s local iteration

Fig. 6.5. Energy analysis.



(a) Loss



(b) Communication cost

Fig. 6.6. Loss and communication cost analysis.

scheme with BlockFL, HFEL, and BFL. The proposed scheme consumes 12.87%, 7.6%, and 13.18% less energy on an average than that of BlockFL, HFEL, and BFL, respectively. The reason is that the proposed scheme considers different parameters and allocates WBANs and miner-reward pairs by minimizing energy consumption. In contrast, BlockFL and BFL randomly assign WBANs without considering the energy consumption of WBANs, while HFEL considers the preferences of edge servers when assigning miner-reward level pairs to WBANs, resulting in higher energy consumption. Moreover, we observe an increase in energy consumption due to the growing computational requirements as the number of WBANs and local iterations increases, as can be seen from Figs. 6.5a and 6.5b.

Loss and Communication Cost Analysis: Fig. 6.6a compares the test loss achieved by the proposed scheme with BlockFL, HFEL, and BFL. As the number

Table 6.2: Analysis of HE

Operation	Local model size	Transmission time
Before encryption	76.961 KB	2.81 msec
After encryption	3694.128 KB	122.82 msec

of global iterations increases, the test loss for all schemes improves, and the gap between the different schemes decreases. The proposed blockchain based FL achieves a test loss comparable to the other three schemes. However, the energy consumption of BlockFL, HFEL, and BFL is much higher than that of the proposed scheme (see Fig. 6.5). Moreover, HFEL and BFL did not consider incentives for participating in the FL process and privacy-preserving techniques during model training. In contrast, the proposed scheme maintains good model performance and provides incentives to encourage WBANs to join the FL process while reducing energy consumption. Moreover, the proposed scheme employs privacy-preserving techniques to protect the privacy of the model weights, which is not the case in BlockFL, HFEL, and BFL.

Fig. 6.6b compares the communication cost of the proposed scheme with BlockFL and BFL. The results demonstrate that the proposed scheme incurs lower communication costs than that of BlockFL and BFL. This is because the proposed scheme aggregates the weights from associated WBANs and adds them to the blockchain as a block, reducing the overall communication. In contrast, BlockFL and BFL add all model weights from associated WBANs individually to the blockchain, leading to higher communication costs. We did not compare the proposed scheme with HFEL as HFEL did not consider blockchain in its work. Moreover, the communication cost remains constant as the number of WBANs increases beyond 350, as assigning more WBANs violate the constraints of problem **P4**.

Analysis of Homomorphic Encryption: We analyze the impact of HE regarding the local model size and transmission time of WBANs' data, as shown in Table 6.2. It is observed that the employment of HE leads to an increase in the local model

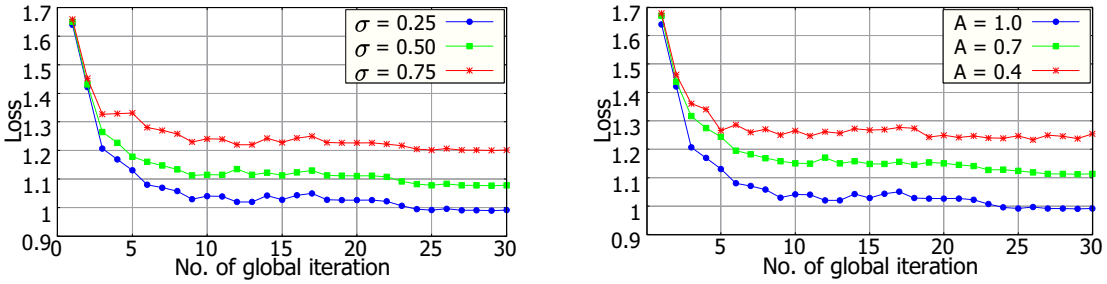
Table 6.3: Impact of HE on energy and cost

$\mathbb{P}$	Energy		Cost	
	With HE	**Without HE**	**With HE**	**Without HE**
100	7759159416	7759159389	132266113286922000	132266113286921998.65
150	11638739123	11638739083	198399169930383000	198399169930382997.98
200	15518318831	15518318777	264532226573844000	264532226573843997.31
250	19397898539	19397898472	330665283217306000	330665283217305996.63
300	23277478247	23277478166	396798339860767000	396798339860766995.96
350	26225958825	26225958731	447059462909797000	447059462909796995.45
400	26225958825	26225958731	447059462909797000	447059462909796995.45

size due to the encoding process intrinsic to Paillier HE [137], resulting in a subsequent elongation of the data transmission time for WBANs. Nevertheless, the transmission overhead brought about by integrating HE in the proposed framework is minimal (i.e., in milliseconds).

Table 6.3 examines the impact of HE on the energy consumption and the cost of WBANs. From the table, it is evident that the energy consumption and the cost of WBANs in the proposed scheme with HE are slightly higher than those in the proposed scheme without HE. The reason for this slight variation is the increased local model size resulting from the integration of HE before its transmission to miners. Consequently, this leads to a higher transmission time, subsequently elevating energy consumption and cost. Furthermore, an increase in energy and cost is also observable as the number of WBANs grows, and it becomes constant when the number of WBANs exceeds 350. This situation arises due to the impossibility of associating more WBANs while still adhering to the constraints outlined in optimization problem **P4**.

Impact of Differential Privacy: Fig. 6.7a examines how DP affects the test loss achieved by the proposed scheme across different noise scales ($\sigma = 0.25, 0.50, 0.75$). With an increase in the noise scale, the loss of the proposed scheme also escalates, illustrating that introducing additional noise influences the performance of the model. Fig. 6.7b illustrates a comparison of the test loss across different gradient bounds ($A = 0.4, 0.7, 1.0$). As the gradient bound diminishes, the loss of the proposed scheme



(a) Noise scale analysis **(b)** Gradient bound analysis

Fig. 6.7. Impact of noise scale and gradient bound on loss.

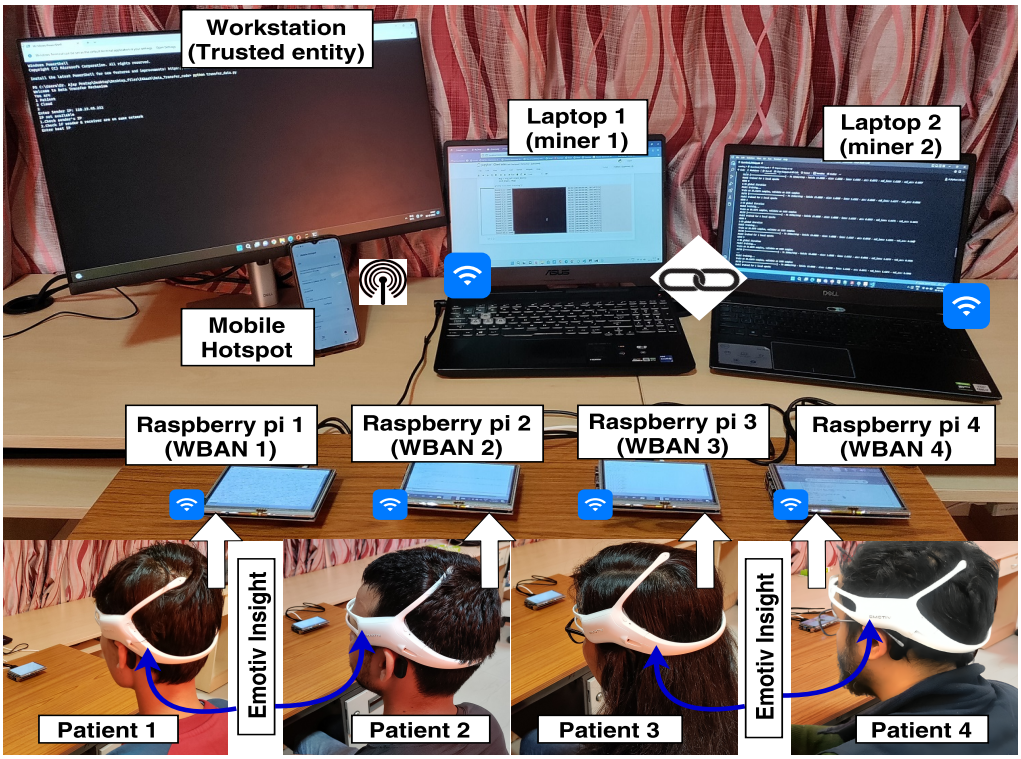


Fig. 6.8. Prototype setup.

grows, signifying that a reduced gradient bound disrupts the desired gradients of the model weights.

Prototype Model: We consider a workstation as the trusted entity, two laptops as miners, and four Raspberry Pis along with the Emotiv Insight as WBANs, as shown in Fig. 6.8. Workstation, Raspberry Pis, and laptops are connected using a 4G mobile hotspot. Emotiv Insight is a wearable device that has sensors placed on the scalp

Table 6.4: Hardware specifications

Devices	Specification
Raspberry Pi	**Model:** Raspberry Pi 4 Model B, **SOC:** Broadcom BCM2711, Cortex-A72 (ARM-v8) 64-bit SoC, **CPU:** 1.5 GHz 64-bit quad-core ARM Cortex- A72 CPU, **RAM:** 8GB LPDDR4 SDRAM, **WiFi:** Dual-band 802.11 b/g/n/ac wireless LAN
Emotiv	**Model:** EMOTIV INSIGHT, **Sensors:** EEG (5 channels: AF3, AF4, T7, T8, Pz), Motion sensor 4.10 GHz, **Connectivity:** Bluetooth Low Energy
Laptops	**Model:** Asus Tuf, 11th Gen Intel(R) Core(TM) i7-11600H @2.90GHz, **RAM:** 16 GB **Model:** Dell G3, 10th Gen Intel(R) Core(TM) i7-10750H @2.60GHz, **RAM:** 16 GB
Workstation	**Model:** Dell Precision 3640 Workstation, **Processor:** 11th Gen Core-i7 -10700 CPU (8 Core(s)) @4.10 GHz, **RAM:** 32 GB

and behind the ears to capture the electrical signals generated by the brain. The workstation assigns Raspberry Pis to miners by executing Algorithm 6.1. Then, the efficient blockchain based FL model (Algorithm 6.2) executes between Raspberry Pis and laptops using the collected data from Emotiv Insights. Moreover, the details of each device are given in Table 6.4.

Fig. 6.9 shows the utility obtained by the proposed scheme on various global iterations. The result shows that the utility achieved in the prototype is slightly lower than that of the simulation. The reason is that the prototype implementation used a 4G mobile hotspot for weight sharing between raspberry pi and laptops, unlike the 5G network used in the simulation[9]. Moreover, raspberry pis and laptops used in the prototype implementation are not

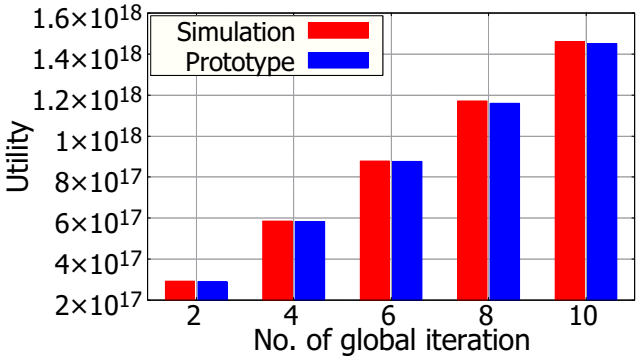


Fig. 6.9. Utility comparison.

[9]With the use of 5G in prototype implementation, higher data transmission rates between WBANs and UAVs, along with reduced latency, would ensure lower energy consumption and higher utility, effectively reducing the performance gap between the simulation result and the prototype result.

dedicated devices as considered in the simulation set-up, leading to higher transmission time. However, the simulation and prototype implementation curves are similar, showing the proposed scheme's applicability in real-world settings.

6.5 Summary

This chapter presented a blockchain based FL framework for smart healthcare, focusing on energy efficiency and privacy preservation, where WBANs collaboratively train FL models. Formulated an optimization problem that maximizes system utility while considering energy, WBAN incentives, miner revenue, and FL loss, altogether. The formulated problem is solved using stable matching and QNN combined with DP and HE to protect patient's privacy. Moreover, blockchain technology facilitates the decentralized sharing of model weights. Real-world experiments validate the framework, yielding an average of 15.1%, 9.03%, and 15.35% improvements over existing methods. However, this chapter focused on developing a blockchain-based FL framework for smart healthcare, considering incentives for WBANs to participate in the FL process based solely on the size of the contributed health data. Relying solely on data volume as the basis for incentives may lead to an imbalanced system, neglecting essential factors such as user reputation, data quality, and operational costs. Furthermore, the current work addresses only a single FL model, limiting its applicability in scenarios that require the parallel training of multiple FL models. Therefore, the next chapter tackles these challenges by exploring a more comprehensive incentive mechanism for WBAN user selection in scenarios involving multiple FL models.