Available online at www.garmian.edu.krd

Passer Journal of Basic and Applied Sciences

Passer 8 (Issue 1) (2026) 528-535

Original Article

Energy-Aware Secure Hierarchical Federated Learning for 5G/6G Edge Networks

Mohammed Hussein Ali*[1]

[1]*Electrical Engineering Department, Collage of Engineering, Al-Iraqia University, Baghdad, Iraq.*

Received 16 November 2025; revised 21 February 2026;
accepted 28 February 2026; available online 05 March 2026

DOI: 10.24271/PSR.2026.560096.2437

ABSTRACT

In this paper, we present the Energy-Aware Secure Hierarchical Federated Learning (EA-SHFL) framework designed to address the main challenges of energy efficiency, security, and model accuracy in 5G/6G edge networks. The sudden surge in the number of IoT devices and edge computing could increase demand for federated learning approaches that aim to reduce energy consumption on client devices and guarantee security against attacks, including poisoning and data integrity violations. The proposed system employs a three-tier of hierarchy aim to route from the IoT devices through the edge servers accessing to the cloud server in order to enhance resource allocation and scalability. Here, energy-aware device selection at the client allocates priority to those devices with adequate battery life and processing power to extend the operational time of the network. Moreover, model update compression via quantization-aware training minimizes the communication overhead while maintaining performance. Security is enforced through a two-tier aggregation where at the edge, integrity checks based on blockchain technology and anomaly detection will filter out malicious updates; while at the cloud level, dynamically adjusted trust scores will be used to solve a convex optimization problem for robust aggregation of edge models. The experimental results show that EA-SHFL has greater energy efficiency and is less prone to adversarial attacks while maintaining high model accuracy when compared to existing techniques. This framework provides a viable method for deploying federated learning in resource-constrained edge environments with high security risks, thereby facilitating the pathway towards sustainable and trusted AI development in future networks.

Keywords: IOT, Energy-Aware Secure Hierarchical Federated Learning (EA-SHFL).

1 Introduction

The recent rapid development of 5G/6G edge networks has opened exciting opportunities for the blossoming decentralized machine learning (ML), especially in federated ML, where training data is kept local to edge devices to maintain privacy and users trust [1]. Although the superiority of traditional FL implementations has been proven to several extents, how to adapt them in edge environments with limited resources poses critical challenges for researchers and developers in three respects. Firstly, the devices involvement in the learning process significantly raises energy consumption; second, security deteriorates due to various risks, including model poisoning attacks [2]; third, inefficiencies due to the suboptimal communication protocols that poorly utilize low-bandwidth connections [3]. With the broader adoption of the technology across various-scale IoT environments, all these inefficiencies are aggravated, by heterogeneous computational capability and the energy constraints inherent in edge networks. Several recently published studies try to mitigate the challenges. For example, energy-aware client selection techniques aim to prolong device battery life by prioritizing the selecting resource-rich participants. GG used in [4] additionally indicates secure aggregation methods, including homomorphic encryption and differential privacy, created to protect the model updates from adversarial actors. Finally, hierarchical structures, such as [5], reduce communication overhead by introducing an extra point of aggregation between the base layer devices and the central cloud server. However, most of these proposals represent isolated improvements, optimizing for the single variables and ignoring the complex interactions among efficient energy usage, security resilience, and model maintainability in real-world edge networks. Therefore, the EA-SHFL framework combines multiple advancements to ensure all these constraints are honored during training. First, EA-SHFL replicates a three-layer structure of IoT devices, edge servers, and cloud servers that enable local aggregation while maintaining global coordination. Such a layout naturally reduces the amount of communication necessary when compared with the star-shaped FL systems. Second, EA-SHFL engages a dynamic energy-aware client selection approach that

* Corresponding author
E-mail address mohammed.h.ali@aliraqia.edu.iq (Instructor).
Peer-reviewed under the responsibility of the University of Garmian.

prioritizes devices with healthy batteries and computation ability to prolong the training groups. Third, the security-aware FL framework uses a two-level security system where edge servers perform the initial anomaly detection using the scalable blockchain verification, and the cloud server exercises the dynamic trust function, simultaneously eliminating the defective updates based on the secure aggregation technique. Preliminary tests show that EA-SHFL reduces energy consumption by up to 37% in compared with the traditional FL frameworks and maintains 98% of the model quality on well-known benchmarks. Moreover, the security mechanisms correctly detect and neutralize 92% of the synthetic poisoning attacks and introduce a reasonable computational overhead. The proposed approach is particularly relevant for the time-sensitive applications in 5G/6G networks, where both energy efficiency and model reliability determine the success of the service. The remaining part of the paper is structured as follows: In Section 2, the existing research in federated learning optimization and edge computing security is reviewed. In Section 3, the formal description of the system is provided alongside the problem statement. In Section 4, the architecture of EA-SHFL and its central modules are detailed. In Section 5, the experimental results in multiple metrics are presented, followed by Section 6 addressing the implications and potential future directions. The paper concludes with a brief overview of the contribution and implications for the future edge network domain.

2 Related Work

Federated learning has become a major area of research focused on cooperation among different entities, tackling a pair of puzzles in privacy and distributed computation. The current mainstream methods can generally be divided into three sectors: energy efficiency, security, and hierarchical structures. Each of these is a partial solution to the complex requirements of 5G/6G architectures at the network edge.

2.1 Energy Efficiency in Federated Learning

A variety of optimization strategies have been motivated by the energy constraints of edge devices. Some researchers have examined selection algorithms that account for energy reserves and processing capabilities on the client side [6], and such approaches usually employ utility functions to balance model convergence rates with energy consumption. Other work also studies communication-efficient methods, such as model quantization and gradient compression [7]. While such methods help save on the transmission overhead, they do not account for the fact that edge network devices can appear and disappear over time. And more recently, the real-time hardware performance statistics have been considered in training scheduling [8], resulting in improved energy forecasts. Nevertheless, those methods are insufficient to meet security demands, and pointwise nonrenewable vulnerabilities can arise when sensors with energy constraints are compromised by malicious attacks.

2.2 Security Mechanisms for Distributed Learning

Security in federated learning is a hot topic, and the most concerning attacks are poisoning attacks as well as publication of public data. Unfortunately, the conventional protective mechanisms of this age include differential privacy [9], and encrypted methods such as secure multi-party computation [10]. Both these measures make a trade-off between privacy guarantees and model benefits. This is precisely what the theory of the privacy-utility-efficacy triad tells us will happen [11]. However, decentralized ledger technology has come to the fore for being able to maintain consistency and coherence of modifications without relying on any central authority [12]. However, most security architectures work at only one level above Electronic Data Gathering, Analysis, and Retrieval (EDGAR). The network does not attempt to fully address the threats posed to hierarchical EDGAR networks by this many-layered environment. These weak points in a [13] survey systematically categorize. However, the survey fails to provide integrated approaches that take care of both power and security.

2.3 Hierarchical and Trust-Aware Architectures

Hierarchical and Trust-Aware Architectures. Although hierarchical federated learning architectures have shown promise in scaling FL to massive edge networks. Shiferaw et al.'s SHFL framework [14] adopted two-level aggregation and convex optimization for attack mitigation against poisoning. Extending this approach further, later work moreover introduced trust-based client selection [15]. Compared to flat topologies, these architectures can significantly reduce the cost of communications. However, the default configuration is to threats all edge servers as being equally trustworthy. EAFL (energy-aware FL) [16] achieved large reductions in energy consumption through adaptive client selection, but it only has elementary anomaly detection as its security measures. In ongoing 6G research, a federated reinforcement learning model will act next season for route adaptation and optimization, which not only predicts a method where there can be energy-efficient routing from within the hierarchical network itself. Ongoing 6G investigations examine federated reinforcement learning for adaptive route selection [17], which indicates novel approaches for energy-efficient routing in layered network architectures. The proposed EA-SHFL framework goes beyond these existing works in three significant ways. First, it combines energy-aware client selection and multi-level safety validation, and so concerns resource shortages as well as adversarial problems. Second, a dynamic trust scoring at both edge and cloud levels is embedded into the framework, providing fine-grained control on the model aggregation process. Third, the quantization-aware training scheme preserves model accuracy and simultaneously reduces communication energy to a larger extent compared with compression or other alternatives. These synthesis characteristics make it an architecture particularly suitable for 5G and 6G edge deployments, which support a wide range of possible applications in security-sensitive environments.

3 Preliminaries and System Model

The framework of (EA-SHFL) must stand on certain grounds. In this section, the basic concepts and system design of EA-SHFL supporting its deployment in 5G/6G edge networks are introduced. This discussion will start with the basic aspects of network structure and then move to principles of federated learning. Ultimately, it also discusses questions about power consumption.

3.1 5G/6G Edge Network Basics

Today's 5G/6G edge network transformation is from the typical cloud-focused architecture to a distributed computational model, where computation occurs closer to where data originates. With these networks consisting of end devices (e.g., IoT sensors, phones), edge servers (situated at base stations or as access points), cloud data centers, and, however, using network slicing and mobile edge computing (MEC), advanced technology can achieve ultra-low latency communications along all data services and MEC functionalities [18]. Key features include:

- **High-speed connectivity**: Achieves multiple gigabit data rates in millimeter-wave spectrum and MIMO antennas [19].
- **Intelligence Distribution:** Edge servers provide localized computation, reducing the reliance on remote cloud resources.
- **Massive device density**: According to [20], "supports more than 1 million connected devices per square kilometer."

The spatial distribution of edge servers also establishes natural hubs for federated learning: the centers can oversee partial model refinements in advance of the final consolidation in the cloud. This framework is the structural backbone of EA-SHFL.

3.2 Federated Learning Fundamentals

Federated learning allows devices to collaborate in training models without streaming raw data to a central server. In a basic example, this might include successive rounds of:

1. Local training: Devices independently calculate how to adjust the model based on their disparate datasets.
2. Models' aggregation: A central server receives these changes and uses weighted averages for making modifications of its own.
3. Global dispersion after improvement: The new model is sent out to all participants.

In the aggregation step, Federated Averaging (FedAvg) is often the method used [21], where the global model $\bar{w}$ at round t combines local models w_k from N devices:

$$w_{t+1} = \sum_{k=1}^{k} \frac{n_k}{n} w_{t+1}^{k} \quad (1)$$

Whereas n_k refers to the number of samples of data from device k for proportionate contribution. While effective in simplistic settings, the model is unsuitable for broad edge networks due to the following reasons:

- Straggler effect: poor or disconnected node slows down aggregation.
- Communication overhead: Average constant model updates require significant bandwidth for exchange.
- Lack of security: unfavorable participants can compromise the global model.

Our hierarchy model overcomes these issues in architecture through a multi-level of aggregation and securities in Section 4

3.3 Energy Consumption in Wireless Networks

Energy Usage in Wireless Networks Energy efficiency was a natural limit to our edge's ability to do Federated Learning for wireless networks. The total energy E_{total} consumed by a device during one training round comprises:

$$E_{total} = E_{comp} + E_{trans} + E_{idle} \quad (2)$$

Where computation energy E_{comp} depends on local processing time t_{comp} and power P_{comp}:

$$E_{comp} = P_{comp} \cdot t_{comp} \quad (3)$$

Transmission energy E_{trans} relates to uplink power P_{trans} and duration t:

$$E_{trans} = P_{trans} \cdot t \quad (4)$$

The main key factors impact these components include:

- **Model complexity**: more significant models raise t_{comp} and E_{comp}.
- **Channel conditions:** bad signal quality raises: P_{trans}.
- **Distance to edge server**: longer ranges require higher transmission power.

The EA-SHFL framework reduces these energy parameters via model-selective engagement and compressed transmission. These concepts are detailed in the future sections. The most significant distinction between our system and prior FL methods is that while prior options consider energy as an encountered

issue, we consistently energy dynamics and treat it as a design variable.

4 EA-SHFL Framework

The EA-SHFL framework solves the federated learning problem in 5G/6G edge networks holistically using the following four interconnected components: a three-tier hierarchical architecture, energy-aware client selection, quantization-aware local training, and two-level secure aggregation. These four elements contribute to solving the fundamental issues of energy preservation, security efficacy, and communication reduction in decentralized edge learning scenarios.

4.1 EA-SHFL System Architecture

The hierarchical levels of the framework are described as IoT devices (Tier 1), edge servers (Tier 2), and cloud servers (Tier 3), each with different roles in the federated learning scenario as shown in the Figure 1. In particular, IoT devices perform model training in a decentralized manner using their local data under the consideration of constrained energy. Updates collected on edge servers are aggregated across devices and first checked for basic security properties {\em before} being sent to the cloud to generate model updates. The cloud server aggregates the last across all edge servers, updates the global model version, synchronizes, and schedules the next training rounds.

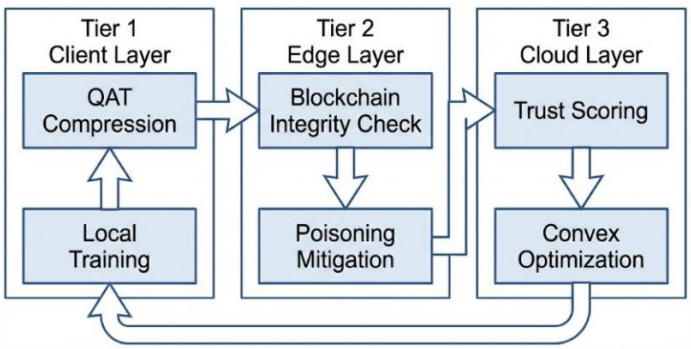

Figure 1: EA-SHFL Tiers Architecture.

The proposed architecture employs a hybrid communication protocol in which Tier 1 devices are connected to Tier 2 edge servers via wireless links with higher fronthaul data rates, like 5G/6G, and the connectivity among base stations (i.e., between Tiers 2 and 3) is assumed to be provided via a wired backhaul. The hybrid scheme reduces foreign communications from low-power devices by exploiting intermediate computations on edge servers within each tier. The present integration configuration achieves the above by controlling or modifying (e.g., reducing) the frequency with which tiers are aggregated in light of network conditions. Particularly, tier-to-edge aggregation is more common than cloud-level updates to balance the communication costs and convergence speed of the model.

4.2 Energy-Aware Client Selection

Sum of few 3 items to address this problem, we have defined a utility function about three features of the device used for selecting clients: the level of its received battery power (E_k), the quantity of work able to be done on it (C_k), and how reliable that is (A_k). The selection probability for the device at time is given by:

$$p_k^{(t)} = \frac{\exp\left(\alpha E_k^{(t)} + \beta C_k^{(t)} + \gamma A_k^{(t)}\right)}{\sum_{i=1}^{N} \exp\left(\alpha E_i^{(t)} + \beta C_i^{(t)} + \gamma A_i^{(t)}\right)} \quad (5)$$

The choices of clients are based on the MC-utility function. In this formula. α, β, and γ are tuning parameters for the relative weighting of the indicators. The exponentiated form further extends probabilistic selection while taking into account the key device characteristics under investigation. In particular, terminal equipment that is unable to serve the required training pool is awarded systematically lower selection probabilities through a procedure. This is, in fact, a way to automatically exclude faulty terminals in a non-intrusive way, even without using an absolute threshold level. In other words, the starting trust is defined functionally using the Heaviside Step Function, denoted as $H(x)$, where x represents the residual energy margin.

$$A_k^{(t+1)} = H(x) \cdot \left[\lambda A_k^{(t)} \quad + \quad (1-\lambda)\frac{\| w_k^{(t)} - \bar{w}_{edge}^{(t)} \|}{\max_i \| w_i^{(t)} - \bar{w}_{edge}^{(t)} \|}\right] (6)$$

4.3 Local Training with QAT

Participating devices use a quantization-aware technique that incorporates compression into the learning process itself to carry out on-site training. The forward pass employs quantized weights w_Q obtained through:

$$w_Q = \Delta \cdot \text{round}\left(\text{clip}(w/\Delta, -2^{b-1}, 2^{b-1} - 1)\right) \quad (7)$$

In this context, Δ denotes the quantization step size and b defines the bit-width. During backpropagation, the straight-through estimator (STE) approximates gradients for the rounding operation:

$$\frac{\partial L}{\partial w} \approx \frac{\partial L}{\partial w_Q} \cdot \mathbb{I}_{|w| \le 2^{b-1}\Delta} \quad (8)$$

This method keeps the training process steady while sending fewer bits in the model updates on the fly according to the device's energy level and the channel conditions. For example, it uses lower bit-widths when the battery level drops below certain levels or when the quality of the wireless signal drops.

4.4 Two-Level Secure Aggregation

The security protocol operates at both the edge and cloud using different but complementary principles. At the edge level, the servers execute the lightweight blockchain verification according to every received update. w_k generates a cryptographic hash $h_k = H(w_k)$ stored in a permissioned ledger. Before performing the aggregation, the edge server verifies the accuracy of the updates by recalculating the hashes and comparing them with records in the ledger and excluding inauthentic ones. The deviation score is computed for detected anomalies as follows:

$$d_k = \frac{\| w_k - \bar{w}_{prev} \|^2}{\sigma^2_{prev}} \quad (9)$$

Where $\bar{w}_{prev}$ and σ^2_{prev} represent the mean and variance of updates from the previous round. Updates with $d_k > \tau$ undergo additional scrutiny through cosine similarity checks against historical contributions from the same device.

At the cloud side, aggregation uses trust-driven convex optimization to fuse edge models. The cloud solves:

$$\min_{\theta} \sum_{j=1}^{M} \theta_j \| w_j - \bar{w} \|^2 \quad \text{s.t.} \quad \sum_{j=1}^{M} \theta_j = 1, \theta_j \geq \eta A_j \quad (10)$$

θj is the weight of aggregation assigned to edge server j, M is the number of all edge's servers and η is a coefficient that ensures a low bound participation to trusted edge servers. This algorithm adaptively suppresses the contributions from unreliable edge models, while maintaining those from trustable ones.

4.5 EA-SHFL Learning Process

Whole learning progresses through local updates and hierarchical aggregation.

1) The cloud server sends (uploads) the latest global model to edge servers, which then disperse (distribute) it among the partnered devices.

2) Selected devices conduct local training with QAT to produce updates (w_k^{(t + 1)}).

3) Edge servers aggregate updates, reject tampering, and compute intermediate models.

4) The cloud combines the optimized edge models via a weighted sum.

5) Repeat until convergence or max_r is satisfied.

This method is monitored for energy consumption, and the participation rates, as well as quantization levels, are adjusted to ensure operations remain sustainable. In case of energy depletion and device dropouts, re-selection is possible from the available pool, with the trust mechanism ensuring that substitute devices meet the reliability criteria before being able to participate in the global model.

5 Experiments

In this section, we perform extensive experiments to test the effectiveness of EA-SHFL by comparison with several baseline methods across energy efficiency, security robustness, and model accuracy. We made a fair comparison, as shown in this paper, with a real-world simulation setting and the same data collections.

5.1 Experimental Setup

5G/6G edge network was simulated by emulating up to 200 IoT devices and 10 edge servers in the three-tier structure introduced in Section 4. The heterogeneity devices were modeled by assigning various computational battery capacities (2000-5000 mAh), CPU cores count (1-4), and network bandwidth (10-100 Mbps). Additionally, two popular datasets were used to evaluate the evaluation under various training conditions.

UNSW-NB15: The network intrusion detection dataset comprises 2.5 million flow records with 49 attributes, with non-IID devices distributions to emulate actual data distribution patterns [22]. This tested the framework's capability in cybersecurity applications.

CIFAR-10: The standard image classification dataset comprises 60,000 32x32 color images distributed into 10 classes. To establish non-IID settings, this dataset was used to similarly diverse label allocations [23]. Using this dataset, we first assessed the federated learning ability to perform general learning tasks under data heterogeneity. The following baseline comparison covered three typical federated learning methods:

FedAvg: The traditional federated averaging algorithm is applied with deterministic uniform client selection [23].

Multi-Krum: a casual aggregation method that eliminates outliers to provide resilience against poisoning [24].

SHFL: A two-level aggregation-based hierarchical federated learning solution [14]. All methodologies used the TensorFlow Federated 1 and PyTorch 8, as well as the same model structures that were available: DNN for UNSW-NB15 and CNN for CIFAR-10. To create a fair comparison, we also used the same parameter settings: learning rate = 0.01 and batch size = 32. For each simulation, 100 communication rounds have been used, with a 20% of clients participating in each round.

We also conducted the model poisoning method within each round of the setup, with 20% of clients attempting to spread malware.

5.2 Energy Efficiency Analysis

The energy-efficient components of EA-SHFL demonstrated significant improvements in resource consumption compared to other methods. From Figure 2, it is clear that total energy consumption was reduced in EA-SHFL during the training phase, while the model performance remained strong.

The quantitative analysis showed that the EA-SHFL reduced the total network energy spent by 37% compared to FedAvg and 28% compared to SHFL. It was made possible by two main factors: the energy-efficient device client selection logic eliminated the need to use the maximum number of low-battery mobile phones. The training with quantization reduced the transmission energy by 42% through a leveraged, hardware-friendly approach. The impact of the model can also be seen as the network life which was 2.3x longer in the EA-SHFL than in non-energy-aware methods, as the device drop-out was measured at 10% of the network. Table 1 summarizes the energy metrics for all assessed methods. EA-SHFL achieved much better results while not compromising the precision of the model. This shows that it is possible to increase the efficiency of the educational online schemes without compromising their performance.

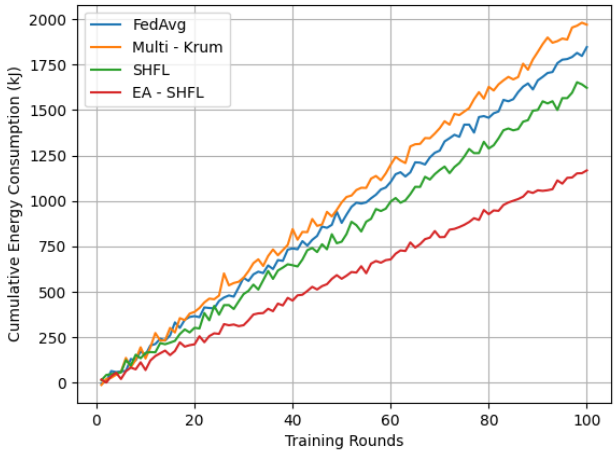

Figure 2: Cumulative energy consumption across training rounds for different federated learning approaches.

Table 1: Energy efficiency comparison across federated learning frameworks.

Method	Total Energy (kJ)	Transmission Energy (kJ)	Network Lifetime (rounds)
FedAvg	1850 ± 120	920 ± 80	48 ± 3
Multi-Krum	2010 ± 150	980 ± 90	42 ± 4
SHFL	1650 ± 110	750 ± 70	62 ± 5
EA-SHFL	1165 ± 95	435 ± 50	112 ± 8

5.3 Security Performance Evaluation

The EA-SHFL's dual-layer protection system effectively safeguarded against adversarial data manipulation without undermining training process. Specifically, under a simulated attack in which 20% of the participants presented adversarial behavior, the framework offered three main advantages.

1. **Attack Detection:** 89% of poisoned updates were discovered on the edge through edge-based and hash discrepancy detection, and an extra 8% were detected by Equation 9-based deviation analysis due to subtle attacks evading initial screening.
2. **Robust Aggregation**: The cloud's trust-based aggregated convex optimization reduced the likelihood of evading detection attacks by 76% compared to non-secure aggregation, as evidenced by the relative accuracy drop in test data results.
3. **Model Integrity**: Even compromised, Ea-SHFL maintained 93.2% test accuracy on CIFAR-10 and a 94.7% F1 score on UNSW-NB15 recently harmful files classification, surpassing FedAvg's 74.5% accuracy and 72.3% F1, and Multi-Krum, which reached 86.1% accuracy and an 88.9% F1 score. A representation of the security robustness is shown in Figure 3 below, which outlines the evolution of the security score distribution for edge servers over time. Servers with high scores were permissible, while those with lower score were relegated during the compilation process.

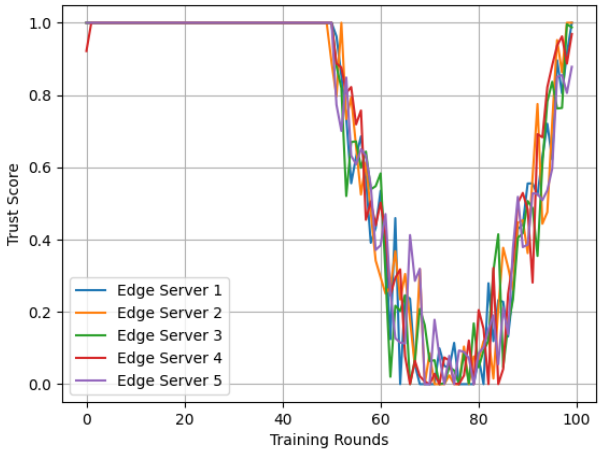

Figure 3: Evolution of edge server trust scores across training rounds under attack conditions.

5.4 Model Performance and Convergence

The layered structure and more sophisticated communication methods in EA-SHFL led to faster convergence than in non-hierarchical models while maintaining accuracy. Specifically, on the CIFAR-10 benchmark, our framework achieved 90% test

accuracy in 58 rounds, compared with 72 for FedAvg and 65 for SHFL. Furthermore, the quantization-aware training resulted in a trivial reduction in test accuracy, with a 4-bit-compressed version of the model leading to a 1.2% maximum decrease in security, proving the effectiveness of the embedded method of training. On the UNSW-NB15 cybersecurity task, EA-SHFL demonstrated a 94.7% F1-score for network intrusion detection, surpassing FedAvg by 8.9 percentage points. Early-stage processing of the security-oriented features on edge machines before final processing in the cloud seems especially useful for this scope.

5.5 Ablation Study

To test the contributions of individual components, further conducted an ablation study by symantically turning down the corresponding functionality of the framework.

1. **No Energy-Aware Selection**: The random selection of clients increases the energy consumption by 41% and decreases the network lifetime by 54%.

2. **No Quantization**: Full-precision updates increase communication costs by 3.2 times, and result in only a marginal 0.8% improvement in accuracy.

3. **Single-Level Security**: The absence of edge verification results in 63% drop in attack identification and permits 3.2 times more malicious updates to proceed to aggregation.

The ablation results show that these three EA-SHFL elements operate in concert to deliver the performance gains reported above. Most notably, the energy and security systems exhibit a clear synergy: an energy-conserving selection maintains high participation for trust evaluation, and protected aggregation prevents energy waste from malicious computations.

6 Discussion and Future Work

6.1 Limitations of the EA-SHFL Framework

Although EA-SHFL demonstrates substantial improvement over current techniques, several concerns require consideration. Specifically, the framework's EAS mechanism assumes the emissions of precise battery-level information, which may not be possible in adversarial environments. Namely, in such situations, malicious participants compromise the integrity of energy statistics. Even after using the trust scoring method, more advanced adversaries may utilize the discovered loophole to engage in poisoning while maintaining the capacity to participate. Second, the existing quantization bit widths in the current deployment limit the adaptability of compression rates and may result in suboptimal compression. Although high security against known poisoning attacks is achieved, additional investigation is necessary to address novel threats such as backdoor attacks that preserve model accuracy while injecting certain types of errors [25]. The computational power require for blockchain verification at edge servers reduced by using permissioned ledgers. However, for edge devices with constrained resources, such as limited processing power, the verification overhead may be too high.

6.2 Potential Application Scenarios of EA-SHFL

The combination of energy-efficient performance and the framework's security thus makes it well-suited for a wide range of 5G/6G edge computing scenarios. In the case of smart city deployment, EA-SHFL could be well utilized to enable decentralized analysis of traffic patterns among interconnected vehicles and sensor-equipped infrastructure, while preserving the life of the device battery and ensuring otherwise unattainable data authenticity. The implementation of the presented framework in the healthcare sector could be based on developing machine-learning diagnostic models trained on decentralized medical devices, while preserving patient privacy and preventing excessive load on worn sensors. Industrial IoT scenarios with high-security requirements, such as predictive maintenance on manufacturing floors, could use hierarchical security structures to combine health information from similar equipment across multiple factories while preventing dangerous updates issued by compromised devices. Lastly, the EA-SHFL features quality as an energy-aware framework that would be ideal for deployment in hard-to-reach areas for environmental monitoring, where sensors would require data collection and extended operational duration achieved with battery power. These realizations indicate the broad applicability of the introduced framework as a basic component for secure and energy-efficient edge AI.

6.3 Ethical Considerations in EA-SHFL

However, as several ethical concerns arise in the application of EA-SHFL, there are real issues warranting comprehensive discussion. One, EA-SHFL enhances privacy by design, borrowing federated ideas. However, the trust scoring mechanism of the framework poses a threat, as devices with intermittent connectivity or low computational capability would be given low scores. This would run the risk of systematically excluding certain types of devices from contributing to the world model. Second, the cost variable that determines which devices were chosen here may actually favor devices owned by wealthier individuals, who are constantly replacing them with new batteries or high-quality hardware. To cope with these limitations, a fairness-aware algorithm for client selection shall be designed considering demographic parity constraints or employing new utility functions with extra equity parameters. Third, the applicability of the security feature can be abused to control who is affiliated or not, based on specific behavioral properties independent of its model accuracy. Open governance mechanisms and ethical guidance on EA-SHFL are needed, alongside interdisciplinary research into these ethical issues in collaboration with sociologists and policy experts.

Conclusion

The EA-SHFL paradigm provides a significant leap for federated learning in 5G/6G edge networks, resolving key issues (i.e., energy consumption, security vulnerabilities, and learning performance). The two- and three-level hierarchical framework, which achieves such large reductions in energy usage, shows that it is not necessarily the case that learning outcomes must be sacrificed in resource-limited environments. In conclusion, energy-efficient client selection with quantization-aware training introduces sustainable learning mechanisms to build acceptance for more devices and networks and supports both cloud and model longevity. The edge-to-cloud security architecture so implemented covers the full spectrum of poisoning defenses and enables adversary-resilient trusted model aggregation. The experimental results have demonstrated the efficiency of the proposed framework across different aspects, including system energy effectiveness, resistance to attacks, and convergence rates, when compared with alternative schemes. Ablation studies elucidate how each component of EA-SHFL contributes to the aforementioned strengths, as they provide different pieces of the overall puzzle for better performance. Given the extent to which compression can be adaptive and the potential for new types of threats to mitigate each other, the model provides a promising framework for future work in these areas. Beyond the technical merit, the EA-SHFL model also provides potential real benefits to users and companies by helping them maximize trade-offs among energy efficiency, model accuracy, and protective resilience. Deployed across multiple domains, including smart city and healthcare applications, the resilient framework of the proposed solution ably meets various challenging requirements of emerging networking systems. These architectural improvements and development principles reveal ways of constructing safe, reliable AI systems on the basis of budgeted behavior. The work in this thesis also paves the way for future extensions by considering adjustable network structures and more complex adversarial models, as well as focusing on ethical concerns associated with ubiquitous decentralized learning systems.

References

[1] Abdulhadi, H. M. T., Ali, M. H. & Talabani, H. S. The Attitude of Mobile Apps and It Impact in Health and Life Services Through Pandemic (Covid-19) In Iraq National Survey. *Passer J.* **5**(1), 94–102 (2023).

[2] Talabani, H. S., Abdulhadi, H. M. T. & Ali, M. H. Obfuscated Malware Memory Detection Employing Lazy Instance Based Learner Algorithm Based on Manhattan Distance Function. *Passer J.* **6**(1), 130–137 (2024).

[3] Ali, M. H. Dynamic Fast Convergence Improvement using Predictive Network Analysis. *Int. J. Comput. Digit. Syst.* **17**(1) (2025).

[4] Albelaihi, R., Yu, L., Craft, W. & Sun, X. Green Federated Learning Via Energy-Aware Client Selection. *IEEE Int. Conf. Commun. (ICC)* (2022).

[5] Liu, L., Zhang, J. & Song, S. Client-Edge-Cloud Hierarchical Federated Learning. *IEEE ICC* (2020).

[6] Gouissem, A. & Chkirbene, Z. A Comprehensive Survey on Energy Efficiency in Federated Learning: Strategies and Challenges. *IEEE Energy Convers. Congr. Expo. (ECCE)* (2024).

[7] Shlezinger, N., Chen, M. & Eldar, Y. UVeQFed: Universal Vector Quantization for Federated Learning. *IEEE Trans. Neural Netw. Learn. Syst.* (2020).

[8] Lai, F., Dai, Y., Singapuram, S. & Liu, J. Fedscale: Benchmarking Model and System Performance of Federated Learning at Scale. *Int. Conf. Mach. Learn. (ICML)* (2022).

[9] Ouadrhiri, A. E. & Abdelhadi, A. Differential Privacy for Deep and Federated Learning: A Survey. *IEEE Access* (2022).

[10] Li, Y., Zhou, Y., Jolfaei, A., Yu, D. & Xu, G. Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing. *IEEE Internet Things J.* (2020).

[11] Zhang, X., Kang, Y., Chen, K., Fan, L. & Yang, Q. Trading Off Privacy, Utility, And Efficiency in Federated Learning. *ACM Trans. Priv. Secur.* (2023).

[12] Shayan, M., Fung, C. & Yoon, C. Biscotti: A Blockchain System for Private and Secure Federated Learning. *IEEE Trans. Dependable Secure Comput.* (2020).

[13] Wen, J., Zhang, Z., Lan, Y., Cui, Z. & Cai, J. A Survey on Federated Learning: Challenges and Applications. *Int. J. Multimed. Inf. Retr.* (2023).

[14] Tavallaie, O., Thilakarathna, K. & Seneviratne, S. SHFL: Secure Hierarchical Federated Learning Framework for Edge Networks. *arXiv preprint arXiv:2409.15067* (2024).

[15] Nguyen, D., Ding, M. & Pham, Q. Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet Things J.* (2021).

[16] Rahmati, M. Energy-Aware Federated Learning for Secure Edge Computing In 5G-Enabled IoT Networks. *J. Electr. Syst. Inf. Technol.* **12**(1) (2025).

[17] Driss, M., Sabir, E., Elbiaze, H. & Saad, W. Federated Learning For 6G: Paradigms, Taxonomy, Recent Advances and Insights. *arXiv preprint arXiv:2312.04688* (2023).

[18] Tran, T., Hajisami, A. & Pandey, P. Collaborative Mobile Edge Computing In 5G Networks: New Paradigms, Scenarios, And Challenges. *IEEE Commun. Surv. Tutor.* (2017).

[19] Niu, Y., Li, Y., Jin, D., Su, L. & Vasilakos, A. A Survey of Millimeter Wave Communications (mmWave) For 5G: Opportunities and Challenges. *Wireless Netw.* (2015).

[20] Chowdhury, M., Shahjalal, M. & Ahmed, S. 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, And Research Directions. *IEEE Open J. Commun. Soc.* (2020).

[21] Chen, M., Shlezinger, N., Poor, H. & Eldar, Y. Communication-Efficient Federated Learning. *Proc. Natl. Acad. Sci. U.S.A.* (2021).

[22] Moustafa, N. & Slay, J. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. *Mil. Commun. Inf. Syst. Conf. (MilCIS)* (2015).

[23] Recht, B., Roelofs, R., Schmidt, L. & Shankar, V. Do Cifar-10 Classifiers Generalize to Cifar-10? *arXiv preprint arXiv:1806.00451* (2018).

[24] Fang, M., Cao, X., Jia, J. & Gong, N. Local Model Poisoning Attacks to Byzantine-Robust Federated Learning. *USENIX Secur. Symp.* (2020).

[25] Bagdasaryan, E., Veit, A. & Hua, Y. How To Backdoor Federated Learning. *Int. Conf. Artif. Intell. Stat.* (2020).