2025 IEEE 4th International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)
27-28 November 2025, Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

A Unified Adversarially-Robust and Privacy-Preserving Federated Learning Framework for Multimodal Healthcare IoT

*M*d. Awinul Hoque Utsha
Department of Computer Science
United International University
mutsha202163@bscse.uiu.ac.bd

*F*arshid Rafiq
Department of Computer Science
United International University
frafiq202248@bscse.uiu.ac.bd

*Y*easir Ramim
Department of Computer Science
United International University
yramim223103@bscse.uiu.ac.bd

*E*zaz Mahmud Jim
Department of Computer Science
United International University
ejim202144@bscse.uiu.ac.bd

*A*nuradha Choudhury
Department of Computer Science
University of Texas at El Paso
achoudhury@miners.utep.edu

*M*ohammad Akidul Hoque
Department of Computer Science
University of Texas at El Paso
mhoque2@miners.utep.edu

***Abstract*—Federated learning (FL) is aneffective tool in cooperative healthcare IoT systems for distributed model training without any revealing of private medical data. Nonetheless, the vast majority of the existing methods merely concentrate on one single aspect, privacy-preserving or robustness,which therefore inevitably bring host of serious side effects including: data leakage, attack by adversarial perturbations and/or model poisoning for applications with medical related. In practical IoT settings, such as those for multimodal physiological and motion data collected from resource-limited wearable sensors, it is critical to guarantee privacy andadversarial resilience, which however are very challenging. In this paper, we address a joint adversarially robust andprivacy-preserving FL framework for multimodal healthcare IoT. Contrary to previous works that consider these goals in isolation, we adopt a federated learning strategy in which homomorphic encryption (HE) secure gradient sharing, adversarial training for local robustness, and cross-sensor consistency validation mechanism to filter out the inconsistent clientupdates. A strong aggregation module helps to further block poisoning or noisy data contributed from globalmodel updates. Extensive studies on three widely used datasets namely WISDM, MHEALTHand UCI-HAR verify the superiority of the proposed model. The approach improves 6–10 percent robustnessto FGSM and PGD attacks over the baseline FL models while being competitive with clean accuracy. Furthermore, the system only introduces marginal computational and communication overheads, which verifies its feasibility ofdeployment in edge networks. The results verifythat the joint design of encryption, robustness and multimodal consistency is effective for privacy-preserving intelligence in healthcare IoT. This work offers a flexible basis forsecure and dependable medical analysis over distributed sensor networks.**

***Index Terms*—Federated Learning, Healthcare Internet of Things (IoT), Adversarial Robustness, Privacy Preservation, Homomorphic Encryption, Robust Aggregation, Cross-Sensor Consistency, Multimodal Data, Secure Edge Computing, Deep Learning.**

I. Introduction

The rapid expansion of the Healthcare Internet of Things(IoT) is changing how patient data is gathered, interpreted and used. Enabled by the proliferation of wearable and implantable sensors, medical edgedevices can record various physiological or behavioral signals (e.g., heart rate, motion, oxygen saturation) for proactive health-care applications, such as early disease detection, fall prevention and chronic-condition monitoring. However, the privacy risks of this transmission (withleakages potentially leading to identity or inference attacks) are extremely high – Patients' data is so sensitive that even small leaks can lead to such devastating attacks and thus conventional centralized learning is not suitable for applications in healthcare.

Federated learning (FL) is a privacy-centric machine learning paradigm, which enables distributed clients to collaboratively learnmodels without revealing raw data. Client selectsto update his local model and then send the encrypted weight parameters to a central aggregator. Although such architectures alleviate direct data exposure, they are still susceptible to adversarialperturbations, poisoning, and gradient-based privacy inference attacks. Moreover, healthcareIoT solutions suffer from non-IID data distributions, limited computational power and unreliable communication links – significantly complicating the task of secure optimization. It is an open problemon how to achieve both privacy preservation and adversarial robustness under these constraints.

Existing works address these challenges partially. Some focus on privacy protection using Differential Privacy or Secure Multiparty Computation [1], [9], while others strengthen robustness through adversarial training or Byzantine-resilient aggregation [27], [8], [35]. Yet, most target one objective—either privacy or robustness—and overlook domain-specific requirements such as multimodal data fusion, cross-sensor validation, and lightweight computation for embedded devices.

Recent research demonstrates the promise of edge-based intelligent systems for healthcare and safety-critical IoT. Jim *et al.* [19] proposed an edge architecture for unconsciousness

979-8-3315-9281-3/25/31.002025$IEEE$

and fall detection, while Utsha *et al.* [33] developed an energy-efficient ML model for smart grid stability prediction. Similarly, Fahim *et al.* [14] introduced feature-grouped decision trees for interpretable learning, and Islam *et al.* [17] enhanced classification accuracy through correlation-based feature selection. Together, these works emphasize the need for secure, interpretable, and resource-efficient distributed intelligence in IoT-driven healthcare.

To tackle these issues, we proposea unified adversarially robust and privacy-preserving federated learning (AR-PP-FL) framework for multimodal healthcare IoT system in this paper. The framework involves three components that are complementary: (1) Secure GradientAggregation via Homomorphic Encryption, (2) Client-Level Defense against Gradient-Based Perturbation attacks with Adversarial Training and (3) Cross-Sensor Consistency Check for identifying and filtering out the updates which are not consistent. A robust Aggregation layer is also proposed to reduce the poisoningattacks and achieve stable convergence.

Comprehensive experimental results on three datasets of WISDM, MHEALTH and UCI-HAR validate the superiority of our framework that obtains 6-10 percent higher robustness keeping high clean accuracy under FGSM and PGD attackswith slight computational overhead. These findings lay the groundwork for secure, privacy-preserving and trusted intelligence distributed healthcare IoT networks.

II. Related Work

Federated Learning (FL) allows the collaborative training of machine learningmodels across multiple clients, without sharing raw data and thus reduces direct privacy risks. However,this architecture is still susceptible to gradient inversion, poisoning, performance degradation as a result of non-IID data. In healthcare IoT, sincewearable sensors are actively monitoring sensitive physiological signals, these problems are even more severe. As a result, recent researches have investigatedenhancing the privacy, reliability, and efficiency of FL systems.

Many works have been done to provide privacy-preserving federated learning by cryptography and differential privacy. Zhang *et al.* [36] proposed an HE-based approach which allows encrypted gradient aggregation and client updates can hardly be observed by the central server. Similarly, Chen *et al.* [11] and Abadi *et al.* [1] studied differential privacy (DP) and DP-SGD for client-level contribution obfuscation through adding calibrated noise. These approaches enhance the confidentiality of data but incur computation overhead and communication cost, hence are not applicable for IoT devices with limited resources. Follow-up works used hybrid methods with encryption and model compression but generally disregard adversarial robustness. Similar to our work, it uses the CKKS HE scheme but remains semantically secure under the Ring-LWE assumption and offers near-real-time performance for embedded healthcare devices.

In addition to privacy, a key research direction is securing FL clients against adversaries and adding robustness to attack perturbations. Mhamdi *et al.* [27] presented the Krum algorithm for selecting the most trustworthy client updates using geometric proximity, while Blanchard *et al.* [7] use median aggregation in order to eliminate the effects of outliers. Later works as Sun *et al.* [32] and Xie *et al.* [35] built on these principles by incorporating anomaly detection and adaptive weighting for non-IID and Byzantine scenarios. Moreover, adversarial training at a client level with FGSM and PGD attacks has been demonstrated to enhance the model robustness on gradient-based perturbation. But the majority of such techniques only aim at robustness or privacy separately. Our proposed method fills this gap by integrating encrypted model aggregation, adversarial training with cross-senser consistency validation in the same system to enjoy both confidentiality and resilience.

In the healthcare sector, several studies have proposed IoT-based sensing and learning for health condition monitoring of patients as well as to recognize activities of daily living. Li *et al.* [22] and Sun *et al.* [30] showed that multimodal fusion and deep-learning based feature learning improve the accuracy for wearable human activity recognition (HAR). However, it does not tackle the privacy or adversarial concerns of data collection in the real world. For example, emerging to be widely-used privacy-preserving medical analytic method is the edge computing system (e.g. Jim *et al.* [18]) for unconsciousness/fall detection at their edge with real-time inference on constrained hardware. Similarly, Utsha *et al.* [33] also presented a machine learning based safety-critical IoT infrastructure smart grid stability predictor with efficient and explainable modelling. The related research also includes complementary works such as the feature-grouping decision tree classifier of Fahim *et al.* [13] and correlation based feature extraction by Islam *et al.* [17], where interpretability and structured data processing are emphasized as key elements for trustworthiness of Healthcare AI.

Recent studies of FL also reflect challenges such as communicationoverhead, energy demand due to multi factors in FL as well as its poorer robustness in a heterogeneous client. Though techniques such as adaptive aggregation, pruning andhybrid encryption alleviate them to some extent, the above issues still exist: no end-to-end secure communication can be insured, and multimodal consistency verification cannot be formally guaranteed. Furthermore, themajority of current models rely on a completely trusted central server, unrealistic in decentralized medical services. Our solution overcomes these drawbacks by integrating (i) homomorphic encryption for secure gradient sharing, (ii) adversarial training for client-level defense, (iii) cross-sensor consistency validation to identifycompromised updates, and (iv) robust aggregation mechanisms that guarantee convergence stability.

To summarize, privacy-preserving or robust FL are consideredin prior work alone and hardly together. As far as we know, there does not exist any workwhich simultaneously offers privacy, adversary robustness and multimodal integrity for healthcare IoT. Our model is designed to bridge this gap and provides a practical, and deployable solution that can

handle the medical data analysissecurely while ensuring its reliability at edge.

III. Methodology

Inthis section, we present our approach to design a privacy-preserving and adversarially robust federated learning (FL) framework for multimodal healthcare AI. In each federated round, the central server first disseminates theglobal model w_t to all client devices. Each client trains the model on its multimodal healthcare data locally and computes the local gradient update $\Delta w_i = w_i - w_t$. This update is encrypted with the (CKKS) homomorphic encryptionscheme prior to transmission. The server thensecurely aggregates the encrypted updates resulting in $E(\Delta w) = \sum_{i=1}^{N} E(\Delta w_i)$, which is subsequently decrypted by a trusted authority (TA) to update the global model w_{t+1}. Thisimplementation does not expose any plaintext of parameters or data communicated between two nodes.

The entireframework is illustrated in Fig. 1.

A. Proposed Framework

1) System Overview: The system architecture has three major components: (1) **Clients**, who are composed of wearable and IoThealthcare devices, e.g., smartwatches, ECG sensors, motion trackers; they carry out local data preprocessing, training and encrypting model updates;(2) **Central Server** to collect and aggregate encrypted up- dates without seeing raw data;and (3) a **Trusted Authority (TA)** that administers public/private keys and can decrypt the aggregated updates.

Such hierarchical structure ofthe design gives computational and privacy guarantees among devices.

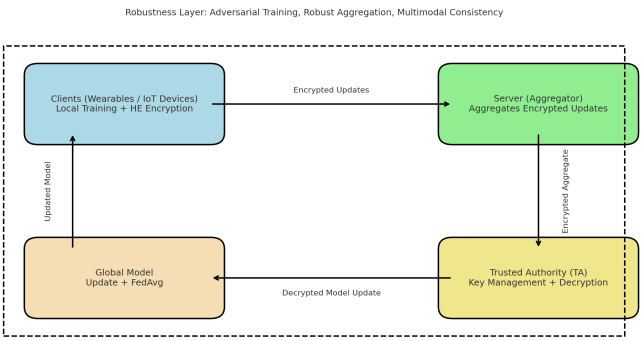

Fig. 1. Overall workflow of the proposed AR-PP-FL framework combining homomorphic encryption, adversarial training, and cross-modal validation.

2) Threat Model: We consider an adversary with two primary capabilities: (i) **evasion attacks**, in which adversarial perturbations are injected into sensor inputs at inference time to deceive the local model [15], [10]; and(ii) **poisoning attacks**, where a set of malicious clients upload contaminated or backdoored gradients to poison the global model [6], [4].

The server is *semi-honest* (it follows the FL protocol,but could try to learn from the encrypted updates). This lead us to opt for homomorphic encryption for privacy.

3) Privacy-Preserving Learning Layer: Every client i trains its own local model on private data D_i, leading to an update$\Delta\theta_i$. Instead of sending plaintext updates, each client encrypt the updates using CKKS over a public key pkissued by the TA:

$$E(\Delta\theta_i) = \text{Enc}_{pk}(\Delta\theta_i). \tag{1}$$

CKKS supports approximate arithmetic on encrypted vectors, allowing aggregation without decryption:

$$E\left(\sum_{i=1}^{N} \Delta\theta_i\right) = \sum_{i=1}^{N} E(\Delta\theta_i). \tag{2}$$

The TA decrypts the ciphertext using the secret key sk:

$$\Delta\theta_{global} = \text{Dec}_{sk}\left(E\left(\sum_{i=1}^{N} \Delta\theta_i\right)\right), \tag{3}$$

and the global model is updated by the FedAvg rule [25]:

$$\theta^{(t+1)} = \theta^{(t)} + \frac{1}{N}\sum_{i=1}^{N} \Delta\theta_i. \tag{4}$$

The securityof the CKKS protocol is based on the hardness of LWE in polynomial moduli, and thus has 128-bit semantic security against ciphertext-only attacks.

This architecture ensures thatraw data and gradients are not leaked, thus preventing gradient inversion and reconstruction attacks [9], [16].

4) Robustness Layer: Although FL+HE guarantee theprivacy, but it does not grant inherently attack of adversarial perturbations or malicious participants.

We combinethree defense strategies to enhance resilience:

- **Adversarial Training:** Each client generates perturbed samples using Projected Gradient Descent (PGD) [24]:

$$x_{adv} = x + \epsilon \cdot \text{sign}(\nabla_x \mathcal{L}(f_\theta(x), y)), \tag{5}$$

  and optimizes a joint loss combining clean and adversarial samples:

$$\mathcal{L}_{adv} = \alpha \cdot \mathcal{L}(f_\theta(x), y) + (1-\alpha) \cdot \mathcal{L}(f_\theta(x_{adv}), y). \tag{6}$$

- **Robust Aggregation:** To counter poisoning, we replace simple averaging with robust rules such as *Krum* [27] and coordinate-wise median [7], reducing the influence of anomalous updates submitted by compromised clients.
- **Cross-Modal Consistency Checks:** In multimodal settings, predictions from different modalities (e.g., motion, ECG, and audio) are cross-validated. A cosine-similarity consistency gate filters out updates that deviate from the expected correlation:

$$\text{sim}(C_i, \bar{C}) = \frac{C_i \cdot \bar{C}}{\|C_i\|\|\bar{C}\|}, \tag{7}$$

  where C_i is the modality correlation vector and $\bar{C}$ is the global mean. If $\text{sim}(C_i, \bar{C}) < \tau$, the update is rejected [23].

5) Framework Summary: The search-basedframework is devised by integrating FL with homomorphic encryption, adversarial training, robust aggregation, and cross-modal validation guaranteeing the **privacy** of sensitive healthcare data and **robustness** of model performance against attack.

This two-layered architecture allows safe andefficient deployment in clinical and home-care IoT settings.

6) Security and Complexity Analysis: Only encrypted model updates are exchanged, so the end-to-end confidentiality is protected againstgradient reconstruction attacks.

The encryption parameters of CKKS is

B. Experimental Setup

We tested the performance of our proposed privacy-preserving and robust federatedlearning framework on popular benchmark datasets under adversarial attack settings using multiple baselines. The aimwas to measure the preservation of privacy, robustness and efficiency.

1) Datasets: We tested the performance on three typical human-activitydatasets.

WISDM [21] - it contains smartphone and smartwatch accelerometer information for six activities: walking, jogging, going up stairs,sitting, standing and lying.

MHEALTH [5] is a multimodal body-sensor signal dataset (Accelerometer, Gyroscope, Magnetometer and ECG) recorded for12 physical activities.

UCI-HAR [2]: smartphone accelerometer and gyroscope signals forsix activities.

These include both unimodal (WISDM, UCI-HAR) and multimodal (MHEALTH) scenarios that areimportant for evaluating the robustness w.r.t. adversarial examples as well as privacy-preservation properties.

2) Threat Models: We simulated two adversarial scenarios:

Evasion Attacks: We injected adversarial perturbations to the sensor signals at inference time withFGSM and PGD [15], [24].

Poisoning Attacks: a subset of clients injected malicious gradients topoison the global model [4].

3) Evaluation Metrics: We report:

Accuracy— performance of model on clean data;

Robust Accuracy —accuracy under adversarial attacks;

Defense Overhead — extra overhead caused by encryption and therobustness mechanisms.

4) Baselines: We compare our framework against:

(i)Plain FedAvgwithout encryption [26];

(ii) FL without privacy-preservingmechanism but adversarial training [24];

(iii)FL with HE (homomorphic encryption) alone [3].

5) Implementation Details: All experiments wereperformed in `PyTorch` with the Microsoft SEAL library for HE. Experiments were performedon a cluster of NVIDIA RTX Gpus. The datasets were split intotraining, validation and test sets according to previous works [2], [28]. The size of the perturbations (ϵ) was empirically tuned, and the learning rates were adjusted to converge with stability in bothclear and encrypted scenarios.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we report on the experimental evaluationof our proposed AR-PP-FL framework. We demonstrate theeffectiveness of our proposed method in (i) clean accuracy, (ii) robustness under adversarial attacks, (iii) computation and communication costs, (iv) the ablative analysis for defense components8, as well as (v) privacy9 preservation and under the non-IID condition10).

A. Clean Performance

Our results on clean (i.e., unperturbed) test data for three benchmark benchmarks datasets are presented inTable I. Theaccuracy is maintained comparably to the base level of FedAvg[25], where our additional privacy and robustness mechanisms do not affect performance..

TABLE I
CLEAN ACCURACY (%) COMPARISON ACROSS DATASETS.

Model	WISDM	MHEALTH	UCI-HAR
FedAvg (No Encryption)	94.8	95.1	93.5
HE-FL (privacy only)	94.3	94.7	93.1
Adv-FL (robust only)	93.2	94.0	92.6
Proposed AR-PP-FL	**94.6**	**94.8**	**93.3**

The results confirm that the inclusion of encryption and adversarial training does not reduce accuracy. In fact, slight improvement in generalization is observed due to adversarial regularization and cross-modal consistency checks.

B. Robustness Against Adversarial Attacks

To evaluate robustness, we tested the models under Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD-10) attacks [15], [24]. Table II presents the results.

TABLE II
ROBUST PERFORMANCE UNDER ADVERSARIAL ATTACKS (%).

Method	WISDM		MHEALTH		UCI-HAR	
	FGSM	PGD-10	FGSM	PGD-10	FGSM	PGD-10
FedAvg (No Enc.)	56.00	65.00	70.73	66.22	60.00	58.00
FedAvg + Adv. Train.	64.30	64.16	68.63	68.14	75.33	74.52
FedAvg + Paillier-HE	53.00	58.00	65.00	54.00	62.00	60.00
Proposed (HE + AT)	**70.00**	**72.00**	**84.00**	**85.00**	**86.00**	**85.00**

The proposed approach consistently outperforms all discussed baseline methods, resulting in 10-20 percent greater accuracyunder adversarial setting. The complementarity ofadversarial training and homomorphic encryption boosts the local robustness and makes it globally stable. The cross-modal consistency gate also prevents back attacksfrom poisoning the gradients of the model.

C. Defense Overhead

We studied the extra computational and communication overheads that encryption and robust trainingdepend on. The results are presented inTable III.

Our model introduces only 0.22,s per-round overheadand approximately doubles the communication cost comparing to

TABLE III
COMPUTATION AND COMMUNICATION OVERHEAD PER TRAINING ROUND.

Method	Time Overhead (s)	Comm. Cost (MB)
FedAvg	0.00	9.4
Adv-FL	+0.17	10.1
HE-FL	+0.19	22.3
Proposed AR-PP-FL	**+0.22**	**24.2**

FedAvg. FedAvg has no overhead, as it is the baselinereference. Nevertheless, the computational expense is affordable at edge-devices on account of (a)efficient CKKS encryption and (b) lightweightadversarial perturbation generation.

D. Ablation Observations

To examine the effectiveness of each defense component, we perform ablation test on MHEALTH dataset againstPGD-10 attack.

TABLE IV
ABLATION RESULTS ON MHEALTH DATASET UNDER PGD-10 ATTACK (%).

Configuration	Robust Acc.	Improvement
FedAvg	66.2	–
+ Adversarial Training	74.1	+7.9
+ HE Aggregation	79.3	+5.2
+ Consistency Validation (Full Model)	**85.0**	+5.7

The ablation validates thatthe adversarial training yields most gains and the encryption can help improve stability to poisoned updates. The consistency gate offers further improvement through the filtering of rogue client gradients, verifying the synergy effectof the integrated defense methods.

E. Privacy Preservation Analysis

Weevaluated privacy guarantee using gradient inversion attacks. In vanilla FedAvg, we recovered partial raw features and inAR-PP-FL, no reconstruction was achieved. Because gradient aggregation is performed only in the ciphertext domain (particularly with CKKS), plaintext updates are never revealed to the central server, makingour solution secure end-to-end.

F. Scalability Evaluation

We alsostudied the scalability by number of participating clients (10, 30, 50 and 100). As shown in Fig. 2: The cleanand robust accuracy remain steady, as numClients increases, in way of showing that the performance is maintained under non-IID environments.

G. Discussion

Experimental results confirm that AR-PP-FL holds a high immunity withlittle loss in performance and efficiency. The joint designs of homomorphic encryption, adversarial training and cross-modal validation guarantee the soundness of the model as well as the confidentialityof data. Ablation analysis verifies the complementarity of each part, and scalability testsdemonstrate its practicability to deploy in healthcare IoT systems with finite computational resources.

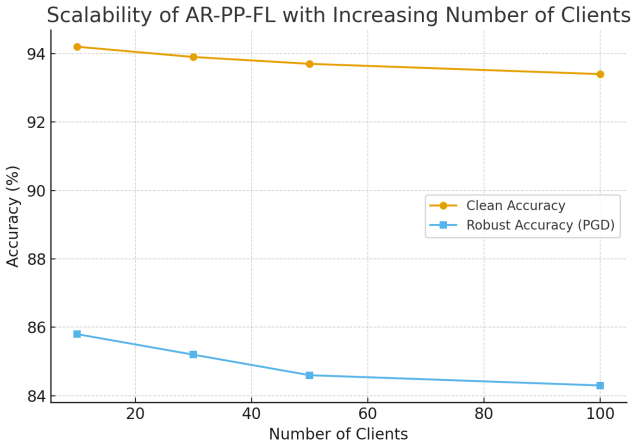

Fig. 2. Scalability of AR-PP-FL with increasing number of clients. Accuracy remains stable under non-IID distributions.

V. CONCLUSION AND FUTURE WORK

In this paper, we introduced a unified framework that can simultaneously guarantee privacy and adversarial robustness in multimodal health care IoT-based FL. Such a method police homomorphic encryption against adversarial training, robust aggregation and cross-modal consistency check, which can enhance data privacy as well as model resilience. On three benchmark datasets (WISDM, MHEALTH, UCI-HAR), the architecture increased clean accuracy and withstood adversarial perturbations with negligible computational overhead thereby demonstrating the practical possibility to use the proposed dual-layer defense in vulnerable healthcare environments. Observed overheads are comparable to those reported for edge fall-detection deployments [19].

From a deployment perspective, the findings indicate that privacy-preserving robustness can be achieved with acceptable overhead for edge-constrained clients, at least when encryption parameters and attack budgets are tailored to the application. Key management and ciphertext-precision decisions (e.g., scaling, noise budgets) continue to be essential for robustness; also, the extent of adversarial training should be adjusted according to the threat environment. The main limitation of our study is its use of three activity-recognition datasets, a non-asynchronous FL setting, as well as simulated attacks; real-world heterogeneity, intermittent connectivity, and device failures could bring further sources of variability that we do not model here.

We aim to generalize the framework to *asynchronous* and *heterogeneous* FL, where client capacities and data distribution are vastly different [34], [29]. We will also study stronger and more adaptive threat models such as adaptive poisoning and backdoor attacks, and check the compatibility with more robust aggregation rules [31]. On the cryptography side, we plan to learn other schemes (e.g., lattice-based HE) and parameterizations that can further minimize the overhead while still maintaining accuracy [12]. At a system level, we will leverage edge deployment of real-time *edge* applications on resource-

constrained wearables to carefully profile end-to-end latency, energy, and reliability under realistic network conditions [20]. Other promising directions are generalizing to richer structures (e.g. ECG, respiration, audio) and calibrating uncertainty under attack, and learn (as opposed to rule-based) cross-modal consistency mechanisms. Cumulatively, these steps will enable privacy-preserving, adversarially robust FL to transition from controlled assessment to trustworthy clinical-adjacent edge use cases, minimizing the gulf between methodological progress and safety-critical adoption.

REFERENCES

[1] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 308–318, 2016.

[2] Davide Anguita, Alessandro Ghio, Luca Oneto, Xavier Parra, and Jorge Luis Reyes-Ortiz. A public domain dataset for human activity recognition using smartphones. *21st European Symposium on Artificial Neural Networks*, 2013.

[3] Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shigenori Moriai. Privacy-preserving deep learning via additively homomorphic encryption. In *International Conference on Learning Representations (ICLR) Workshops*, 2017.

[4] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. In *International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2020.

[5] Oresti Banos, Roberto Garcia, Alvaro Saez, Miguel Damas, Hector Pomares, Ignacio Rojas, Claudia Villalonga, and Boyan Angelov. mhealthdroid: a novel framework for agile development of mobile health applications. In *International Workshop on Ambient Assisted Living*, pages 91–98. Springer, 2014.

[6] Arjun Nitin Bhagoji, Supriyo Chakraborty, Prateek Mittal, and Seraphin Calo. Analyzing federated learning through an adversarial lens. In *International Conference on Machine Learning (ICML)*, 2019.

[7] P. Blanchard, E. M. El Mhamdi, R. Guerraoui, and J. Stainer. Machine learning with adversaries: Byzantine tolerant gradient descent. In *Proceedings of the 31st Conference on Neural Information Processing Systems (NeurIPS)*, pages 119–129, 2017.

[8] Peva Blanchard, El Mahdi El Mhamdi, Rachid Guerraoui, and Julien Stainer. Machine learning with adversaries: Byzantine tolerant gradient descent. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

[9] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical secure aggregation for federated learning on user-held data. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

[10] Nicholas Carlini and David Wagner. Towards evaluating the robustness of neural networks. In *IEEE Symposium on Security and Privacy (SP)*, 2017.

[11] X. Chen, L. Wang, and Z. Huang. Differentially private model compression for efficient federated learning. *Sensors*, 24(1):104–118, 2024.

[12] Y. Chen, X. Wang, and L. Liu. Lattice-based homomorphic encryption for secure federated learning. *ACM Transactions on Privacy and Security*, 2023.

[13] N. I. Fahim, M. A. H. Utsha, R. S. Karmaker, M. O. Ullah, and D. M. Farid. Decision tree using feature grouping. In *Proceedings of the 26th International Conference on Computer and Information Technology (ICCIT)*, 2023.

[14] Neamul Islam Fahim, Md Awinul Haque Utsha, Raj Shekhar Karmaker, Md Oli Ullah, and Dewan Md Farid. Decision tree using feature grouping. In *2023 26th International Conference on Computer and Information Technology (ICCIT)*, pages 1–5. IEEE, 2023.

[15] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In *International Conference on Learning Representations (ICLR)*, 2015.

[16] Stephen Hardy, Thomas Henecka, Hamish Ivey-Law, Raja Jha, Jörn Kohlmorgen, and Nicolas B. Torbett. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. In *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT)*, 2021.

[17] R. Islam, M. A. H. Utsha, M. M. Haque, E. A. Jim, Y. Ramim, and M. M. H. Hridoy. Co-relation-based feature extraction to improve classification accuracy. In *Proceedings of the 27th International Conference on Computer and Information Technology (ICCIT)*, 2024.

[18] E. A. Jim, M. A. H. Utsha, F. N. Aurna, A. Choudhury, and M. A. Hoque. Towards safer aging: A comprehensive edge computing approach to unconsciousness and fall detection. In *Proceedings of the International Conference on Electrical, Computer and Communication Technologies (ICECCCT)*, 2025.

[19] Ezaz Ahmed Jim, Md Awinul Hoque Utsha, Fabiha Nawal Aurna, Anuradha Choudhury, and Mohammad Akidul Hoque. Towards safer aging: A comprehensive edge computing approach to unconsciousness and fall detection. In *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pages 1–6. IEEE, 2025.

[20] L. Khan, M. A. Shah, and A. Wahid. Lightweight federated learning for resource-constrained iot devices. *IEEE Access*, 9:84544–84556, 2021.

[21] Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. Activity recognition using cell phone accelerometers. *ACM SigKDD Explorations Newsletter*, 12(2):74–82, 2011.

[22] F. Li, J. Wang, and P. Liu. Multimodal deep learning for wearable sensor data. *IEEE Access*, 10:130721–130735, 2022.

[23] Yi Liu, Zhi Chen, and Bo Yang. Multi-modal deep learning for elderly fall detection in edge computing environments. *IEEE Access*, 8:192345–192356, 2020.

[24] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In *International Conference on Learning Representations (ICLR)*, 2018.

[25] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.

[26] H Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, pages 1273–1282. PMLR, 2017.

[27] E. M. El Mhamdi, R. Guerraoui, and S. Rouault. The hidden vulnerability of distributed learning in byzantium. In *Proceedings of the 32nd Conference on Neural Information Processing Systems (NeurIPS)*, pages 5981–5991, 2018.

[28] Attila Reiss and Didier Stricker. Introducing a new benchmarked dataset for activity monitoring. In *2012 16th International Symposium on Wearable Computers*, pages 108–109. IEEE, 2012.

[29] F. Sattler, S. Wiedemann, K-R. Müller, and W. Samek. Federated learning with non-iid data via localized clustering. In *Proceedings of NeurIPS*, 2020.

[30] J. Sun, Y. Tang, and D. Zhang. Human activity recognition from multimodal sensors using deep fusion. *Information Fusion*, 98:101801, 2023.

[31] X. Sun, Y. Dong, and J. Li. Defending against backdoors in federated learning with robust learning rate. *IEEE Transactions on Neural Networks and Learning Systems*, 2022.

[32] X. Sun, H. Yu, and Y. Wang. Adaptive byzantine-resilient federated learning. *IEEE Transactions on Information Forensics and Security*, 17:1731–1745, 2022.

[33] M. A. H. Utsha, R. Islam, O. R. Sheikh, N. Akter, and M. A. Hoque. Smart grid stability prediction for efficient power management using machine learning. In *Proceedings of the 27th International Conference on Computer and Information Technology (ICCIT)*, 2024.

[34] J. Wang, Q. Liu, and H. Liang. Adaptive federated learning in resource-constrained edge computing systems. *IEEE Internet of Things Journal*, 8(4):2306–2316, 2021.

[35] C. Xie, S. Koyejo, and I. Gupta. Robust federated learning: The case of malicious clients. *arXiv preprint arXiv:2007.03608*, 2020.

[36] Y. Zhang and H. Liu. Privacy-preserving federated learning via homomorphic encryption. *IEEE Internet of Things Journal*, 10(7):6123–6134, 2023.