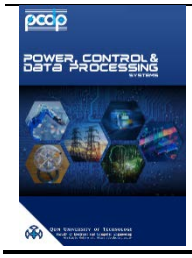
DOI: 10.30511/pcdp.2025.2062825.1027 - ISSN: 3060-8376 - Vol 2(4), 2025



POWER, CONTROL AND DATA PROCESSING SYSTEMS

Available Online at: https://pcdp.qut.ac.ir/

# Enhancing Security in Federated Solar Panel Fault Detection: Evaluating Robust Aggregation Methods Against Malicious Client Attacks

**ARTICLE INFO**

***Article Type***
Original Research

***Authors***
Keyvan Kazemi[1]

[1] School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, Iran,
keyvan.kazemi@ut.ac.ir

**** Correspondence***
*Address*: School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, Iran.
*Phone*: -
*Fax*: -
keyvan.kazemi@ut.ac.ir

***Article History***
Received: June 05, 2025
Accepted: August 08, 2025
ePublished: December 01, 2025

**ABSTRACT**

Renewable energy, particularly solar energy, is critical for sustainable development, yet maintaining solar panel efficiency requires timely and accurate fault detection. Federated learning has emerged as a promising solution by enabling decentralized model training while preserving data privacy. However, conventional aggregation methods such as FedAvg are vulnerable to adversarial attacks, where malicious clients poison model updates and severely degrade performance. In this paper, we present an enhanced federated transfer learning framework for solar panel fault detection that leverages a pre-trained VGG-16 model for effective feature extraction and incorporates robust aggregation techniques to defend against model poisoning. Specifically, we simulate a poisoning attack scenario by introducing malicious clients that inject Gaussian noise into their updates, and we evaluate two robust aggregation methods—Krum and coordinate-wise median—against this threat. Experimental results demonstrate that while standard FedAvg yields a final test accuracy of only 19.21\% with an exorbitantly high loss, the Krum and coordinate-wise median methods achieve significantly improved performance, with final test accuracies of 70.62\% and 72.88\% and test losses of 1.3161 and 0.7926, respectively. Notably, these results are closely aligned with the performance of federated learning without attack, which achieves 74\% accuracy with a final loss of 0.82, and centralized learning, which reaches 75\% accuracy with a loss of 0.85. These findings underscore the critical importance of robust aggregation in securing federated learning frameworks for solar panel fault detection, providing a scalable and privacy-preserving solution even in adversarial environments.

**Keywords:** Solar Panel Fault Detection, Federated Learning Security, Robust Aggregation, Adversarial Attacks, Model Poisoning.

# 1 Introduction

The increasing global energy demand, coupled with growing environmental concerns and the finite nature of fossil fuel reserves, has accelerated the adoption of renewable energy technologies [1]. Among these, solar energy has emerged as a key contributor, with photovoltaic (PV) systems playing a crucial role in sustainable energy infrastructure [21]. As solar panel installations expand to meet rising energy needs [2], ensuring their operational efficiency remains a significant challenge due to performance degradation caused by environmental stressors and equipment faults [3].

Reliable fault detection in PV systems is essential for optimizing energy yield and minimizing maintenance costs. Common failure modes such as microcracks, hot spots, and partial shading can lead to power losses of up to 30% if left undetected [6]. Recent advancements leverage deep learning techniques, including convolutional neural networks (CNNs) for infrared image analysis [4] and IoT-enabled monitoring systems [5]. While centralized approaches have demonstrated high accuracy [8], they present inherent challenges related to data privacy and scalability.

Federated learning (FL) has emerged as a transformative approach in distributed machine learning, enabling collaborative model training without sharing raw data [17]. This paradigm is particularly beneficial for solar fault detection, where privacy concerns and the geographical dispersion of PV systems pose significant constraints on centralized methodologies [15, 34]. To improve FL's performance in data-limited environments, transfer learning techniques utilizing pretrained vision models are integrated, facilitating robust feature extraction while reducing computational demands on client devices [9]. Unlike conventional FL approaches that primarily focus on data aggregation [19], federated transfer learning (FTL) introduces model personalization mechanisms that address data heterogeneity and annotation limitations across distributed clients [20].

Despite its advantages, the decentralized nature of FL introduces vulnerabilities to adversarial attacks, compromising model integrity and the reliability of energy production [27]. In solar fault detection systems, malicious clients can execute model poisoning attacks by injecting manipulated local updates, which is particularly concerning given the critical nature of energy infrastructure [30]. One such attack involves Gaussian noise injection, where adversaries introduce additive noise $\mathcal{N}(\mu, \sigma^2)$ into their model updates, obscuring fault signatures in infrared images [29]. This attack poses several challenges: (1) Noisy gradients can mask early-stage panel degradation, delaying essential maintenance actions; (2) Reduced fault detection accuracy leads to undiagnosed efficiency losses, impacting energy production; (3) The stealthiness of the attack enables gradual performance deterioration, evading conventional anomaly detection mechanisms [28]. Traditional aggregation methods such as FedAvg are particularly susceptible to these attacks due to their equal weighting of all client updates, irrespective of their reliability [31].

To counteract these threats, robust aggregation schemes tailored for solar fault detection scenarios are employed. The Krum algorithm enhances resilience by selecting the most representative client updates based on pairwise Euclidean distances between gradient vectors, effectively filtering out poisoned updates [32]. Additionally, coordinate-wise median aggregation provides further robustness by computing the median value for each model parameter independently across clients, mitigating the impact of skewed noise distributions [33].

To address these challenges, an enhanced federated transfer learning framework for solar panel fault detection is proposed. The approach leverages a pretrained VGG-16 model for efficient feature extraction and integrates robust aggregation techniques to mitigate adversarial threats. A poisoning attack scenario is simulated by introducing malicious clients injecting Gaussian noise into their model updates. The effectiveness of two robust aggregation methods—Krum and coordinate-wise median—is evaluated under these conditions. Experimental results show that these methods significantly improve resilience against attacks compared to standard approaches. Notably, their performance remains close to that of federated learning without attacks and centralized learning, demonstrating the robustness of these techniques in ensuring secure and reliable federated learning. These findings highlight the importance of robust aggregation in providing a scalable and privacy-preserving solution in adversarial settings.

**The contributions of this study are as follows:**

- A realistic adversarial scenario is formulated by simulating model poisoning through Gaussian noise injection, reflecting stealthy attack behaviors in federated environments.
- Robust aggregation methods—Krum and coordinate-wise median—are integrated into the federated learning process and examined for their effectiveness in mitigating adversarial impacts.
- A comprehensive experimental evaluation is conducted, comparing centralized learning, federated learning without attack, and federated learning under adversarial conditions. The analysis includes the performance of three aggregation strategies, highlighting their relative robustness and effectiveness in maintaining model performance under malicious client behavior.

The remainder of this paper is organized as follows: Section II presents the proposed federated transfer learning framework, describing its architecture, the integration of VGG-16 for feature extraction, and the incorporation of robust aggregation techniques to enhance security against adversarial attacks. Section III outlines the experimental setup and provides a comprehensive analysis of the results, including dataset de-

tails, model architecture, federated learning implementation, and a comparative evaluation of robust versus non-robust aggregation methods under both adversarial and non-adversarial conditions. Finally, Section IV concludes the paper by summarizing the key contributions, highlighting the impact of robust aggregation on federated learning security, and discussing potential avenues for future research.

# 2 Proposed Framework

## 2.1 Problem Formulation

The objective is to classify solar panel images into predefined categories using a decentralized dataset distributed across multiple clients. Each client $i$ holds a subset $D_i$ of the global dataset $D = \bigcup_{i=1}^{n} D_i$, where $n$ is the total number of clients. This distribution introduces challenges such as data heterogeneity, privacy preservation, and potential adversarial interference. In our framework, some clients may behave maliciously by injecting noise into their model updates, thereby undermining the integrity of the aggregated global model and reducing fault detection performance.

## 2.2 Federated Learning

Federated learning (FL) enables collaborative model training across clients without sharing raw data, thereby preserving privacy. To improve performance in scenarios with limited labeled data, we integrate transfer learning by leveraging the pre-trained VGG-16 model for feature extraction. The model comprises a frozen convolutional feature extractor and trainable task-specific layers. Formally, the model output is given by:

$$p(y \mid x; \theta) = f_{\text{task}}\Big(f_{\text{conv}}(x; \theta_{\text{conv}}); \theta_{\text{task}}\Big). \tag{1}$$

where $\theta = \{\theta_{\text{conv}}, \theta_{\text{task}}\}$, $f_{\text{conv}}$ represents the feature extractor, and $f_{\text{task}}$ performs classification.

Each client $i$ minimizes its local cross-entropy loss:

$$L_i(\theta) = -\sum_{(x,y)\in D_i} \log p(y \mid x; \theta). \tag{2}$$

where $D_i$ is the local dataset for client $i$.

Local model parameters are updated using stochastic gradient descent (SGD):

$$\theta_i^{t+1} = \theta^t - \eta \nabla L_i(\theta^t). \tag{3}$$

where $\eta$ is the learning rate, and $t$ represents the global training round.

The global loss function is defined as:

$$L_{\text{global}}(\theta) = \sum_{i=1}^{n} \frac{|D_i|}{|D|} L_i(\theta). \tag{4}$$

where $|D_i|$ represents the number of samples at client $i$, and $|D|$ is the total number of samples.

The server updates the global model by aggregating the client updates:

$$\theta_{t+1} = \sum_{i=1}^{n} \frac{|D_i|}{|D|} \theta_i^{t+1}. \tag{5}$$

where $\theta_i^{t+1}$ represents the updated parameters from client $i$.

## 2.3 Model Poisoning Attack

Federated learning systems are vulnerable to adversarial attacks. In our framework, we simulate a model poisoning attack in which malicious clients perturb their local updates by injecting noise. For any model parameter $\theta$, a malicious client generates a poisoned update:

$$\theta' = \theta + \epsilon. \tag{6}$$

where $\epsilon \sim \mathcal{N}(0, \sigma^2)$ is Gaussian noise, and $\sigma$ is the standard deviation of the noise distribution.

This perturbation is intended to distort the aggregated global model, leading to reduced classification accuracy and increased overall loss.

## 2.4 Robust Aggregation Methods

To mitigate the effects of adversarial updates, we incorporate two robust aggregation techniques: Krum aggregation and coordinate-wise median aggregation.

### 2.4.1 Krum Aggregation

Krum aggregation enhances robustness by selecting the client update that is most consistent with the majority. For each client $i$, the Krum score is computed as:

$$s_i = \sum_{j \in S_i} \|\theta_i - \theta_j\|^2. \tag{7}$$

where $S_i$ is the set of $n - f - 2$ nearest updates to $\theta_i$, and $f$ represents the number of malicious clients.

The update with the smallest score $s_i$ is selected as the representative global update.

### 2.4.2 Coordinate-wise Median Aggregation

The coordinate-wise median method aggregates model parameters by computing the median for each coordinate across all client updates. For a given parameter $\theta$, the aggregated global parameter is given by:

$$\theta_{\text{global}} = \text{median}(\theta_1, \theta_2, \ldots, \theta_n). \tag{8}$$

where $\theta_1, \theta_2, \ldots, \theta_n$ are the corresponding parameters from the $n$ client updates.

This approach minimizes the influence of outlier values introduced by adversarial clients.

### 2.5 Framework Integration

The complete federated transfer learning framework integrates decentralized training with adversarial defense mechanisms as follows:

1. **Initialization:** The server initializes the global model $\theta_0$ using VGG-16 pre-trained weights.
2. **Federated Training:** For each global round $t$:
   (a) The server distributes the current global model $\theta_t$ to all clients.
   (b) Each client fine-tunes the model on its local dataset $D_i$ to obtain updated parameters $\theta_i^{t+1}$.
   (c) Malicious clients simulate a poisoning attack by injecting Gaussian noise into their updates (as per Equation 7).
   (d) The server collects all local updates and aggregates them using one of the following methods:
      - **FedAvg (Baseline):** Weighted averaging of client updates (Equation 5).
      - **Krum:** Selection based on the minimum Krum score (Equation 7).
      - **Coordinate-wise Median:** Aggregation via the median for each parameter (Equation 8).
   (e) The global model is updated to $\theta_{t+1}$ using the aggregated update.
3. **Convergence:** The training process continues until a predefined convergence criterion is met.

### 2.6 Advantages of the Proposed Framework

The proposed framework offers several key benefits:

- **Data Privacy:** Raw data remains on local clients, ensuring privacy.
- **Robustness:** The use of Krum and coordinate-wise median aggregation mitigates the impact of adversarial (poisoned) updates.
- **Scalability:** The decentralized approach supports large-scale deployment across distributed PV systems.
- **Enhanced Accuracy:** Integration of transfer learning via VGG-16 improves feature extraction and fault detection performance, particularly in data-limited scenarios.

This comprehensive framework provides a secure, scalable, and high-performance solution for decentralized solar panel fault detection, effectively addressing challenges related to data heterogeneity, privacy preservation, and adversarial attacks.

## 3 Experimental Setup and Results

### 3.1 Experimental Setup

The experiments were conducted using the following setup:

#### 3.1.1 Dataset Details

The dataset utilized in this study comprises solar panel images categorized into six distinct fault types: **Bird-drop**, **Clean**, **Dusty**, **Electrical-damage**, **Physical-Damage**, and **Snow-Covered**. This dataset, named "Solar Panel Images Clean and Faulty Images," is publicly available on Kaggle,[1] and consists of a total of 885 images, with an uneven distribution across the fault categories. To maintain consistency, all images were preprocessed and resized to a uniform resolution of $244 \times 244$ pixels. Fig. 1 presents a sample image from each category.

#### 3.1.2 Model Architecture

A fine-tuned VGG-16 model served as the foundational architecture for fault detection. The model was initialized with pre-trained ImageNet weights, with its top layers replaced by a Global Average Pooling layer, a Dropout layer with a rate of 0.3, and a Dense layer containing 6 output units, corresponding to the total number of classes in the dataset.

#### 3.1.3 Federated Learning Setup

The federated learning framework consists of a central server and seven distributed solar panel clients. Five of these clients store a subset of the dataset locally and participate in legitimate model training, while the remaining two act as malicious clients. The server manages the training process by collecting model updates from all clients, aggregating them, and distributing the updated global model back. The bidirectional communication ensures that data privacy is maintained, as raw client data never leaves local devices. However, the malicious clients do not perform genuine training; instead, they manipulate the received global model by injecting noise into the trainable parameters before sending poisoned updates back to the server, aiming to degrade overall model performance. In our setup, the noise is drawn from a Gaussian distribution with a mean of zero and a standard deviation of $\sigma = 0.5$, ensuring a controlled but impactful perturbation to the model updates in every training round. Fig. 2 illustrates the federated learning setup, highlighting the interaction of legitimate and adversarial clients.

[1] Available at: `https://www.kaggle.com/datasets/pythonafroz/solar-panel-images`

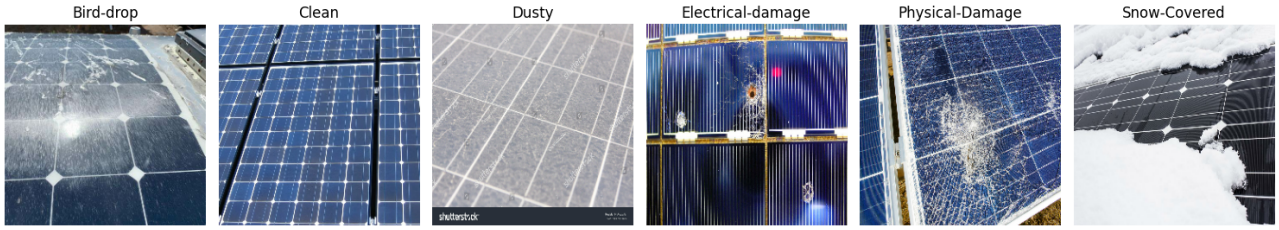



Figure 1: Representative images from each of the six classes in the dataset.

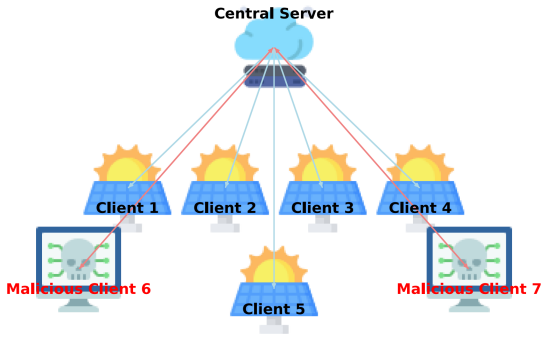



Figure 2: Federated learning setup for central server experiment...

## 3.2 Results and Discussion

This section presents the experimental results, analyzing the performance of centralized and federated learning in both benign and adversarial environments. The evaluation includes accuracy and loss trends across training rounds, highlighting the impact of adversarial attacks and the effectiveness of robust aggregation methods.

### 3.2.1 Centralized and Federated Learning Without Attack

To establish a baseline, we first evaluate the performance of centralized learning and federated learning in a benign setting, without adversarial interference. The centralized model, trained with full access to the dataset, achieves a final test accuracy of **75%** with a loss of **0.85**, demonstrating strong classification performance. In contrast, the federated learning model, where training occurs in a decentralized manner across clients, attains a closely comparable test accuracy of **74%** with a final loss of **0.82**, confirming the feasibility of federated learning in maintaining competitive accuracy while preserving data privacy. This slight performance gap is expected due to the decentralized nature of federated learning, where client updates are based on locally available data without full visibility into the global distribution.

Fig. 3 and Fig. 4 illustrate the accuracy and loss curves for centralized training, showing smooth convergence over training rounds. Similarly, Fig. 5 and Fig. 6 depict the performance trends for federated learning, demonstrating stable convergence behavior and minimal deviation from centralized results.

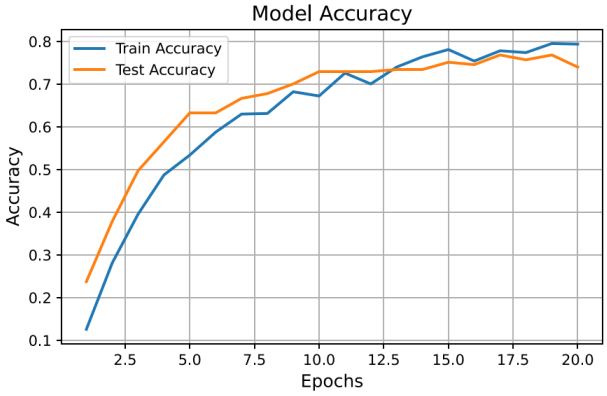



Figure 3: Test accuracy progression for centralized learning, showing steady improvement over training epochs.

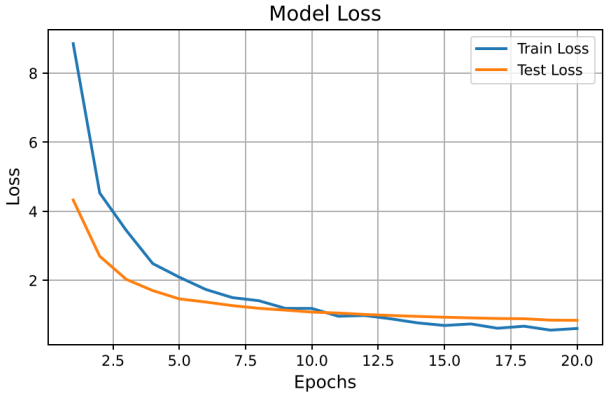



Figure 4: Test loss progression for centralized learning, indicating smooth convergence with minimal fluctuations.

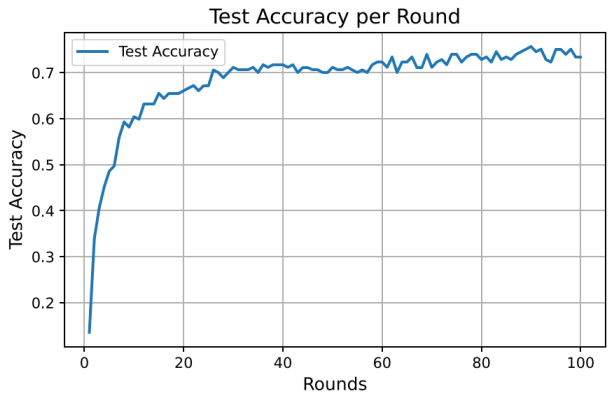



Figure 5: Test accuracy per round for federated learning without attack, demonstrating strong performance close to centralized learning.

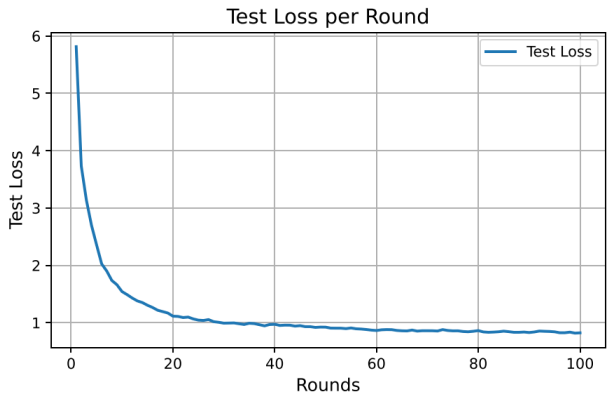



Figure 6: Test loss per round for federated learning without attack, highlighting stable model convergence.

### 3.2.2 Federated Learning Under Adversarial Attack

Next, we examine the impact of adversarial attacks on federated learning. When trained using the standard FedAvg aggregation method in the presence of two malicious clients injecting Gaussian noise, the global model suffers a severe degradation in performance, achieving only 19.21% final test accuracy with an excessively high loss. This highlights the vulnerability of FedAvg to model poisoning attacks. Since FedAvg aggregates all client updates without evaluating their reliability, poisoned model parameters from malicious clients are integrated directly into the global model. This lack of robustness causes the aggregated model to deviate significantly from the true gradient direction, leading to unstable training dynamics and degraded accuracy.

To mitigate this, we implement two robust aggregation methods: **Krum** and **coordinate-wise median**. The Krum aggregation method, which selects a client update closest to the majority, significantly improves model resilience, achieving a final test accuracy of **70.62%** with a test loss of **1.3161**. The coordinate-wise median method, which aggregates updates by computing the median for each parameter dimension, further enhances robustness, achieving the highest test accuracy of **72.88%** with a final test loss of **0.7926**. These results confirm the effectiveness of robust aggregation in mitigating adversarial interference while preserving classification performance.

Fig. 7 and Fig. 8 compare the performance of FedAvg, Krum, and coordinate-wise median aggregation under attack. The accuracy trends in Fig. 7 illustrate the severe degradation of FedAvg, while Krum and coordinate-wise median demonstrate significantly improved stability and learning progression. Similarly, Fig. 8 highlights the difference in loss behavior, where robust aggregation methods effectively limit model divergence.

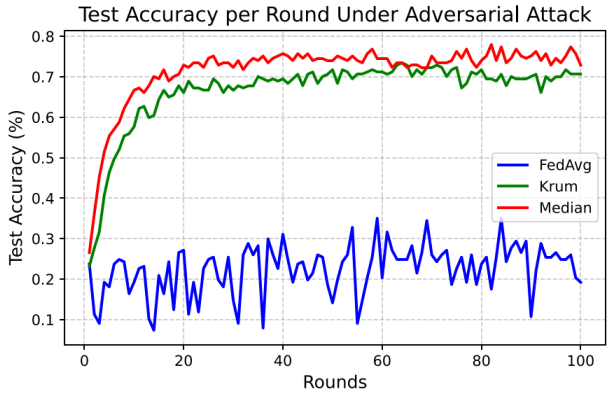



Figure 7: Test accuracy per round under adversarial attack, comparing the performance of FedAvg, Krum, and coordinate-wise median aggregation.

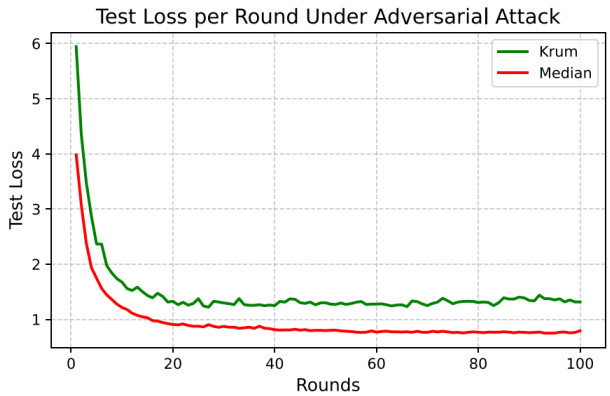



Figure 8: Test loss per round under adversarial attack, demonstrating the robustness of Krum and coordinate-wise median aggregation in stabilizing learning.

To summarize the impact of adversarial attacks and the effectiveness of robust aggregation techniques, Ta-

ble 1 presents a comparative analysis of test accuracy and loss across different training scenarios.

Table 1: Comparison of test accuracy and loss under different training conditions.

| Training Method | Accuracy (%) | Loss |
|---|---|---|
| Centralized (No Attack) | 75.00 ± 0.04 | 0.85 ± 0.01 |
| FedAvg (No Attack) | 74.00 ± 0.10 | 0.82 ± 0.02 |
| FedAvg (Attack) | 19.21 ± 1.20 | High |
| Krum (Attack) | 70.62 ± 1.34 | 1.3161 ± 0.08 |
| Median (Attack) | 72.88 ± 1.18 | 0.7926 ± 0.06 |

As seen in Table 1, FedAvg fails under adversarial conditions, while Krum and coordinate-wise median significantly improve resilience, restoring accuracy close to non-attacked federated learning. These findings reinforce the necessity of robust aggregation techniques in securing federated learning for solar panel fault detection, ensuring reliable performance in adversarial environments.

# 4 Conclusion

In this paper, a federated transfer learning framework was extended for solar panel fault detection, addressing the challenge of adversarial attacks in decentralized environments. A model poisoning scenario was simulated in which malicious clients injected Gaussian noise into their updates, leading to significant performance degradation under standard FedAvg aggregation. While federated learning without attack achieved a test accuracy of 74% with a final loss of 0.82, and centralized learning reached 75% accuracy with a loss of 0.85, FedAvg under attack dropped sharply to 19.21% accuracy with an excessively high loss. In contrast, robust aggregation methods significantly mitigated this effect: Krum achieved 70.62% accuracy with a final loss of 1.3161, and coordinate-wise median further improved performance to 72.88% accuracy with a loss of 0.7926. These results demonstrate that robust aggregation can restore federated learning performance to near non-adversarial levels while preserving data privacy and scalability. Despite these promising results, several avenues remain for future work. First, the current study focuses on model poisoning, where malicious updates directly manipulate model parameters. However, many real-world threats arise from data poisoning strategies—such as label flipping, backdoor injection, or adaptive attacks targeting data semantics. Future studies will explore these more sophisticated and subtle adversarial behaviors to broaden the threat model and validate the robustness of federated learning under diverse attack scenarios.Second, the dataset employed in this work though highly relevant to the solar fault detection domain is relatively niche in size. This constraint influenced the number of participating clients in our simulation. As part of future research, larger and more heterogeneous datasets will be incorporated, and experiments will be scaled to include more clients. This will help assess both the scalability and generalizability of the proposed framework under realistic federated deployment conditions.While Krum and coordinate-wise median were selected due to their popularity and computational simplicity, they represent only a subset of robust aggregation strategies. Future work will explore more advanced aggregation techniques and robust client selection methods. This expanded analysis will help identify aggregation or defense strategies that are best suited for specific attack types, system constraints, or application domains.

# Disclosure of Potential Conflicts of Interest

The Authors declare that there is no conflict of interest.

# References

[1] Seminario-Córdova, R. & Rojas-Ortega, R. Renewable energy sources and energy production: A bibliometric analysis of the last five years. *Sustainability.* **15**, 10499 (2023), https://doi.org/10.3390/su151310499

[2] Alliance, G., Presidency, C. & Others Tripling renewable power and doubling energy efficiency by 2030: Crucial steps towards 1.5° C. (IRENA: International Renewable Energy Agency,2023), https://coilink.org/20.500.12592/wpxr18

[3] Tong, D., Farnham, D., Duan, L., Zhang, Q., Lewis, N., Caldeira, K. & Davis, S. Geophysical constraints on the reliability of solar and wind power worldwide. *Nature Communications.* **12**, 1-12 (2021), https://doi.org/10.1038/s41467-021-26355-z

[4] Ledmaoui, Y., El Maghraoui, A., El Aroussi, M. & Saadane, R. Enhanced fault detection in photovoltaic panels using cnn-based classification with pyqt5 implementation. *Sensors.* **24**, 7407 (2024), https://doi.org/10.3390/s24227407

[5] Anish, B., Gokul, B., Harish, M., Kavin, P. & Others Solar Panel Fault Detection Using Internet of Things. *2024 International Conference On IoT Based Control Networks And Intelligent Systems (ICICNIS).* pp. 727-731 (2024), https://doi.org/10.1109/ICICNIS64247.2024.10823354

[6] Pathak, S., Patil, S. & Mishra, D. Enhancing Solar Panel Fault Detection: An Efficient Multidomain Feature Analysis Model with Entropy-Guided Saliency Map Segmentation.. *International Journal Of Intelligent Engineering & Systems.* **17** (2024), https://doi.org/10.22266/ijies2024.0831.25

[7] Pa, M., Uddin, M. & Kazemi, A. A Fault Detection Scheme Utilizing Convolutional Neural Network for PV Solar Panels with High Accuracy. *2022*

*IEEE 1st Industrial Electronics Society Annual On-Line Conference (ONCON)*. pp. 1-5 (2022), https://doi.org/10.1109/ONCON56984.2022.10126746

[8] Duranay, Z. Fault detection in solar energy systems: A deep learning approach. *Electronics*. **12**, 4397 (2023), https://doi.org/10.3390/electronics12214397

[9] Mittal, K., Gill, K., Chattopadhyay, S. & Singh, M. Innovative Solutions for Solar Panel Maintenance: A VGG16-Based Approach for Early Damage Detection. *2024 International Conference On Communication, Computing And Internet Of Things (IC3IoT)*. pp. 1-4 (2024), https://doi.org/10.1109/IC3IoT60841.2024.10550368

[10] Abdelmoula, I., Oufettoul, H., Lamrini, N., Motahhir, S., Mehdary, A. & El Aroussi, M. Federated learning for solar energy applications: A case study on real-time fault detection. *Solar Energy*. **282** pp. 112942 (2024), https://doi.org/10.1016/j.solener.2024.112942

[11] Luan, Z., Lai, Y., Xu, Z., Gao, Y. & Wang, Q. Federated learning-based insulator fault detection for data privacy preserving. *Sensors*. **23**, 5624 (2023), https://doi.org/10.3390/s23125624

[12] Zhao, L., Li, J., Li, Q. & Li, F. A federated learning framework for detecting false data injection attacks in solar farms. *IEEE Transactions On Power Electronics*. **37**, 2496-2501 (2021), https://doi.org/10.1109/TPEL.2021.3114671

[13] Liu, Q., Yang, B., Wang, Z., Zhu, D., Wang, X., Ma, K. & Guan, X. Asynchronous decentralized federated learning for collaborative fault diagnosis of PV stations. *IEEE Transactions On Network Science And Engineering*. **9**, 1680-1696 (2022), https://doi.org/10.1109/TNSE.2022.3150182

[14] Khan, R., Saeed, U. & Koo, I. FedL-STM: A Federated Learning Framework for Sensor Fault Detection in Wireless Sensor Networks. *Electronics*. **13**, 4907 (2024), https://doi.org/10.3390/electronics13244907

[15] Husnoo, M., Anwar, A., Haque, M. & Mahmood, A. Decentralized Federated Anomaly Detection in Smart Grids: A P2P Gossip Approach. *ArXiv Preprint ArXiv:2407.15879*. (2024), https://doi.org/10.48550/arXiv.2407.15879

[16] Lu, S., Gao, Z., Zhang, P., Xu, Q., Xie, T. & Zhang, A. Event-triggered federated learning for fault diagnosis of offshore wind turbines with decentralized data. *IEEE Transactions On Automation Science And Engineering*. **21**, 1271-1283 (2023), https://doi.org/10.1109/TASE.2023.3270354

[17] Zhao, H., Guo, Y., Wang, M., Fan, F., Zhang, H. & Ma, Y. A Federated Learning Model for Fault Diagnosis of IIoT Using a Modified PSO Algorithm Customized by Taguchi Method. *Proceedings Of The 2023 5th International Conference On Internet Of Things, Automation And Artificial Intelligence*. pp. 135-140 (2023), https://doi.org/10.1145/3653081.3653105

[18] Han, J., Zhang, X., Xie, Z., Zhou, W. & Tan, Z. Federated Learning-Based Equipment Fault-Detection Algorithm. *Electronics*. **14**, 92 (2024), https://doi.org/10.3390/electronics14010092

[19] Abdelmoula, I., Oufettoul, H., Lamrini, N., Motahhir, S., Mehdary, A. & El Aroussi, M. Federated learning for solar energy applications: A case study on real-time fault detection. *Solar Energy*. **282** pp. 112942 (2024), https://doi.org/10.1016/j.solener.2024.112942

[20] Guo, W., Zhuang, F., Zhang, X., Tong, Y. & Dong, J. A comprehensive survey of federated transfer learning: challenges, methods and applications. *Frontiers Of Computer Science*. **18**, 186356 (2024), https://doi.org/10.1007/s11704-024-40065-x

[21] Masoudi, M., Haghighi, M. & Rahimipour Behbahani, M. Optimal Operation of Solar Energy System integrated with Energy Storage Systems. *Power, Control, And Data Processing Systems*. **1** (2024), https://doi.org/10.30511/pcdp.2024.718345

[22] Monemi Bidgoli, M. & Ghani, R. Optimal Energy Management of Water-Energy Nexus in Multi-Carrier Systems Integrated with Renewable Sources. *Power, Control, And Data Processing Systems*. **1** (2024), https://doi.org/10.30511/pcdp.2024.718536

[23] Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., Xiong, H. & He, Q. A comprehensive survey on transfer learning. *Proceedings Of The IEEE*. **109**, 43-76 (2020), https://doi.org/10.1109/JPROC.2020.3004555

[24] Kairouz, P., McMahan, H., Avent, B., Bellet, A., Bennis, M., Bhagoji, A., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R. & Others Advances and open problems in federated learning. *Foundations And Trends® In Machine Learning*. **14**, 1-210 (2021), https://doi.org/10.1561/2200000083

[25] Etemadi, S. & Khashei, M. Survey of the loss function in classification models: Comparative study in healthcare and medicine. *Multimedia Tools And Applications*. **84**, 12765-12812 (2025), https://doi.org/10.1007/s11042-024-19543-8

[26] Afroz, P. Solar Panel Images Clean and Faulty Images. , https://www.kaggle.com/datasets/pythonafroz/solar-panel-images

[27] Nair, A., Raj, E. & Sahoo, J. A robust analysis of adversarial attacks on federated learning environments. *Computer Standards & Interfaces*. **86** pp. 103723 (2023), https://doi.org/10.1016/j.csi.2023.103723

[28] Pillutla, K., Kakade, S. & Harchaoui, Z. Robust aggregation for federated learning. *IEEE Transactions On Signal Processing*. **70** pp. 1142-1154 (2022), https://doi.org/10.1109/TSP.2022.3153135

[29] Yazdinejad, A., Dehghantanha, A., Karimipour, H., Srivastava, G. & Parizi, R. A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Transactions On Information Forensics And Security*. (2024), https://doi.org/10.1109/TIFS.2024.3420126

[30] Kumar, K., Mohan, C. & Cenkeramaddi, L. The impact of adversarial attacks on federated learning: A survey. *IEEE Transactions On Pattern Analysis And Machine Intelligence*. **46**, 2672-2691 (2023), https://doi.org/10.1109/TPAMI.2023.3322785

[31] Isik-Polat, E., Polat, G. & Kocyigit, A. ARFED: Attack-Resistant Federated averaging based on outlier elimination. *Future Generation Computer Systems*. **141** pp. 626-650 (2023), https://doi.org/10.1016/j.future.2022.12.003

[32] Colosimo, F. & De Rango, F. Median-krum: A joint distance-statistical based byzantine-robust algorithm in federated learning. *Proceedings Of The Int'l ACM Symposium On Mobility Management And Wireless Access*. pp. 61-68 (2023), https://doi.org/10.1145/3616390.3618283

[33] He, Y., Li, P., Ni, J., Deng, X., Lu, H., Zhang, J. & Yang, L. RSAM: Byzantine-Robust and Secure Model Aggregation in Federated Learning for Internet of Vehicles using Private Approximate Median. *IEEE Transactions On Vehicular Technology*. (2023), https://doi.org/10.1109/TVT.2023.3341637

[34] Kazemi, K. Federated Transfer Learning for Image-Based Solar Panel Fault Detection. *2025 12th Iranian Conference On Renewable Energies And Distributed Generation (ICREDG)*. pp. 1-5 (2025), https://doi.org/10.1109/ICREDG66184.2025.10966124