Teknik: Jurnal Ilmu Teknik dan Informatika
Volume 5 Nomor 2 Oktober 2025
e-ISSN: 2798-2513; p-ISSN: 2808-8751, Hal 171-181
DOI: https://doi.org/10.51903/teknik.v5i2.1027
Available online at: https://journal.stiestekom.ac.id/index.php/TEKNIK

Resilient Federated Learning Against Injection and Evasion Attacks in Edge Smart Grids: A Simulation Study

Wiwid Wahyud[1]
[1]Universitas Sains dan Teknologi Komputer, Semarang

Korespondensi penulis: wiwid.wahyudi2@stekom.ac.id

Abstract; *The modernization of smart grids through edge computing introduces significant cybersecurity challenges, most stemming from adversarial machine learning attacks that compromise distributed intelligence. Although Federated Learning is an appealing decentralized model training paradigm for edge smart grids, its resilience against coordinated injection and evasion attacks has not yet been thoroughly explored. To address this critical gap, we develop and evaluate a resilient Federated Learning model for edge-based innovative grid applications. Under a rigorous simulation-based experimental design, we created a controlled environment based on synthetic energy-demand data and implemented adversarial attack scenarios to ensure model robustness. We propose a resilience enhancement layer in our framework during the federated aggregation process to curtail malicious model updates and adversarial inferences. The results show significant improvement in the stability of the proposed model under attack, maintaining a robustness index above 0.62, whereas baseline approaches exhibit complete degradation. This corresponds to a reduction of approximately 34% in the attack impact rate across different-intensity attack scenarios, while maintaining high stability in aggregation. In addition to the adversarial testing framework in the domain of Federated Learning, this work provides a validated resilience model that secures analytics of smart grids without requiring access to raw data. Our methodology presents a resource-efficient alternative to physical testing and enables safe yet comprehensive security evaluation in critical infrastructure applications.*
Keywords*: Adversarial Attacks, Edge Computing, Federated Learning, Smart Grids, Simulation-Based Evaluation.*

I. INTRODUCTION

The global energy industry is going through a significant change, which shows the application of digital technologies along with the physical power grid, and this is leading to the development of brilliant power grid networks (Alotaibi et al., 2020). In these cyber-physical networks, advanced metering infrastructure, the installation of renewable energy sources, and the ability to monitor have become capable not only of supporting efficient operations but also of ensuring reliability and environmental friendliness. (Dileep, 2020; Moreno Escobar et al., 2021). At the same time, edge computing has been recognized as the primary enabler for the upgrading of smart grids due to its ability to process data in the very near of its origin, which means the retarding of data transfer is eliminated, the bandwidth is saved, and the control is where it is needed most is being applied (Cao et al., 2020; Filali et al., 2020). This convergence of technologies gives rise to an intelligent network that is capable of dynamic load balancing, predictive maintenance, and rapid fault detection, thereby completely changing the energy distribution paradigms (Khalid, 2024).

The distributed aspect of edge computing in smart grids, however, brought about the worst kind of cybersecurity vulnerabilities (Goudarzi et al., 2022). Besides, smart grid includes edge devices, which are the main points of security breach for cyber attacks aiming at the grid's analytic capacity, such as intelligent electronic devices, phasor measurement units, and smart inverters (F. Wang et al., 2020). Among the distributed machine learning methods that enable privacy to the greatest extent, Federated Learning stands out, and it has come to be used in these environments as it allows multiple edge devices to collaborate in the training of a model without the need to centralize the raw data (L. Li et al., 2020; Qin et al., 2020). This new way of working fits perfectly with bright grid designs, where data authority and fast communication are the two most important things (Supriadi et al., 2025).

Even so, the Federated Learning method is still vulnerable to expertly executed adversarial attacks that compromise its integrity and performance (T. Li et al., 2019). Among the numerous hackers'

Diterima: 12 Oktober 2025; Direvisi: 23 Oktober 2025; Disetujui: 24 Oktober 2025; Tersedia Online: 29 Oktober 2025; Diterbitkan: 30 Oktober 2025.

methods are the two most worrying ones, namely, injecting misleading data into the local model training process and conducting eavesdropping attacks during the inference at the global model deployment phase, which are considered serious by most researchers (Chakraborty et al., 2021; Ren et al., 2020). Cybercriminals can take over user devices and send in outputs or updates that are bad, eventually leading to the federated model being inaccurately classified through a process called Byzantine fault (Q. Li & Song, 2021). At the same time, subtle attacks will change inputs during the inference stage to cause misunderstandings in critical applications like energy theft detection and predicting equipment failure (Karim et al., 2019). The combination of these attacks poses a massive risk to the electric grid, making it unstable and insecure and, in turn, leading to outages, financial losses, or even blackouts through the domino effect.

The majority of the current studies into Federated Learning in smart grids are mainly concerned with optimization, accuracy enhancement, and privacy protection; in most cases, the issue of resilience against adversarial manipulations is not regarded at all (S. et al., 2025). In general, past assessments have been based on the unvarying public datasets, which are not able to reflect the nature of real-world cyber threats in edge environments that are dynamic and adaptive (Lueckmann et al., 2021). This limitation in the methodology creates a considerable gap in research regarding the systematic evaluation of Federated Learning's robustness when subjected to coordinated adversarial campaigns specifically focused on the edge smart grid infrastructure (Nugroho & Wibowo, 2025). One more reason why effective defense strategies cannot be developed for these vital systems is the lack of comprehensive simulation frameworks that can simulate complex attack scenarios.

This research aims to go beyond existing limitations by developing and evaluating a robust Federated Learning framework intentionally designed to be resilient against both injection and evasion attacks in innovative grid-edge environments. The establishment of a new resilience mechanism compatible with the federated aggregation process, the creation of a simulation-based evaluation framework with dynamic adversarial scenarios, and the quantitative measurement of model performance under various attack levels will be among our primary objectives. As a result, we provide a validated methodological framework for adversarial testing in Federated Learning environments, a resilience model that maintains performance without access to raw data, and a resource-efficient evaluation paradigm that avoids the risks associated with physical experimentation on operational grid infrastructure.

The paper continues as follows. The second section reviews the literature on Federated Learning, adversarial machine learning, and smart grid security, and their interconnections, which form the basis of our conceptual framework. The third section explains our simulation-based methodology, giving details on experimental design, data generation, and evaluation metrics. The fourth section shows and discusses the experimental results, while the fifth section presents conclusions, implications, and directions for future research.

II. LITERATURE REVIEW

A. Federated Learning Theory and Applications

Federated Learning has been the groundwork for a new approach to distributed machine learning, which allowed different stakeholders to combine their efforts in training a standard model while all the training data remained decentralized (T. Li et al., 2019). With this option, the very sensitive privacy issues of edge computing are met since there is no raw data transferred to the central server, but only model parameters' updates are exchanged (Qin et al., 2020). The standard Federated Learning setup uses a client-server model where edge nodes serve as clients that perform local training of models on their data, and after that, forward updates to an aggregation server (L. Li et al., 2020). The server finally mixes these updates by applying algorithms like Federated Averaging to create a better global model, which is later sent back to clients either for more training or for inference (X. Wang et al., 2020).

Federated Learning's incorporation into innovative grid environments offers powerful benefits across load forecasting, anomaly detection, and equipment health monitoring (Supriadi et al., 2025). The diversity of data distributions across different geographical locations and consumer

types is what makes these applications so powerful, while still complying with data privacy regulations (Goudarzi et al., 2022). On the other hand, the non-i.i.d. nature of smart grid data at edge devices raises concerns about model convergence and performance stability (T. Li et al., 2019). Moreover, the different computational capabilities of edge devices in smart grids add to the complexity of federated training regarding synchronization and resource allocation (Luo et al., 2021).

B. Adversarial Machine Learning in Distributed Systems

Adversarial machine learning has become an essential area of research against which all machine learning threats may be started, with a dangerous attack that is deployed by dishonest intentions (Akhtar et al., 2021). Poisoning attacks primarily aim at the training process; evasion attacks look at manipulating inference inputs (Chakraborty et al., 2021). With the advent of data injection attacks in the Federated Learning environment, poisoning becomes obscenely powerful for corrupting the training process, where nuisance participants introduce faulty data or model updates to impair global model performance (Ren et al., 2020), which is further exacerbated by the distributed nature of Federated Learning providing multiple attack surfaces from anywhere in the edge network (Q. Li & Song, 2021).

Evasion attacks, in contrast, take advantage of the model's blind spots during the inference process and apply very slight modifications to the input data, causing it to be misclassified, but at the same time, the changes are not noticeable to humans (Ghaffari Laleh et al., 2022). In the case of the smart grid, such attacks might conduct power consumption readings to go undetected by the theft detection system or even change equipment sensor data to make it impossible to predict faults with accuracy (Karim et al., 2019). The escalating complexity of these attacks calls for powerful defense mechanisms that would still be able to function efficiently under the computer and communication limitations imposed by edge environments (Costa et al., 2024; Liang et al., 2022).

C. Smart Grid Cyber-Physical Security

Smart grids are intricate cyber-physical systems where a security breach in the cyber domain can easily disrupt the physical infrastructure, leading to serious consequences (Moreno Escobar et al., 2021). The increased use of edge devices has made the attack surface larger and the vulnerabilities in grid monitoring and control systems more numerous (X. Kong et al., 2022). Centralized security measures based on traditional methods are unsuitable for these systems with decentralized distribution, since they are limited in scalability and have points of failure (Alotaibi et al., 2020). Thus, the focus of research has shifted to distributed anomaly detection systems that can detect the occurrence of malice through the use of multiple grid components (Goudarzi et al., 2022).

Edge computing has not only enhanced the responsiveness of smart grids but also introduced new security issues arising from diverse devices, limited resources, and site accessibility (F. Wang et al., 2020). Consequently, it is quite impossible to implement a comprehensive security measure; therefore, the use of light security mechanisms that are still very effective (L. Kong et al., 2023). The use of AI-powered edge computing, however, is another issue, as it has created a new attack specifically targeting machine-learning-trained models (Deng et al., 2020). Therefore, it is necessary to investigate these interdependent vulnerabilities to develop a robust learning framework that can withstand even the most sophisticated adversarial campaigns.

D. Prior Studies and Research Gap

The research conducted between 2022 and 2025 has provided significant improvements in the area of Federated Learning for innovative grid applications, especially in terms of communication efficiency, model accuracy, and privacy preservation (Oktavia & Wibowo, 2025; Owusu-Mensah et al., 2025). Nevertheless, the issue of resilience of Federated Learning to coordinated attacks by adversaries is still somewhat neglected (Putri & Ainindhira, 2025). Most of the current studies are based on static datasets for their evaluations, which do not reflect the dynamic nature of the attacks that happen in real-life edge scenarios (Roni et al., 2025). Such a limitation in methodology not

only prevents but also obscures recognition of the full range of vulnerabilities in Federated Learning systems used for critical infrastructure applications.

Through time, the inquiry into Federated Learning systems for edge smart grids has led to the discovery of a crucial gap as far as comprehensive frameworks that cater to both injection and evasion attacks at the same time are concerned (S. et al., 2025). A considerable number of the studies tend to give emphasis only to one attack category or adopt defense strategies that heavily rely on computational resources, rendering them infeasible for edge devices (Nugroho & Wibowo, 2025). Moreover, the lack of adversarial testing in Federated Learning environments, simulation-based evaluation methodologies, results in the prevention of the development and validation of effective resilience strategies (Chai et al., 2023; Elendu et al., 2024). Our work is right on the spot, as it not only tackles the issue but also proposes a resilience framework and evaluation methodology that perfectly fit edge smart grids.

E. Conceptual Framework

The conceptual framework of our resilient Federated Learning system for edge smart grids is depicted in Figure 1. The framework uses a sequential defense mechanism to counteract dual adversarial threats. Edge devices engage in local model training while being exposed to data injection attacks that affect their updates. The updates are sent to the aggregation server, where a dedicated resilience layer detects and mitigates malicious updates using statistical analysis and anomaly-detection algorithms.

The resilience layer uses strong aggregation methods to eliminate poisoned updates before computing the global model, ensuring that only verified updates contribute to improving the model. After aggregation, the updated global model is now vulnerable to evasion attacks during inference on edge devices. Here, the attackers modify the input data so that the output is a wrong classification. Throughout this procedure, system performance is continuously monitored using extensive evaluation metrics that capture key security indicators, including the robustness index, attack impact rate, and aggregation stability. This integrated framework provides a systematic approach to preserving the integrity of Federated Learning under edge conditions, thereby providing the basis for our simulation-based resilience evaluation.

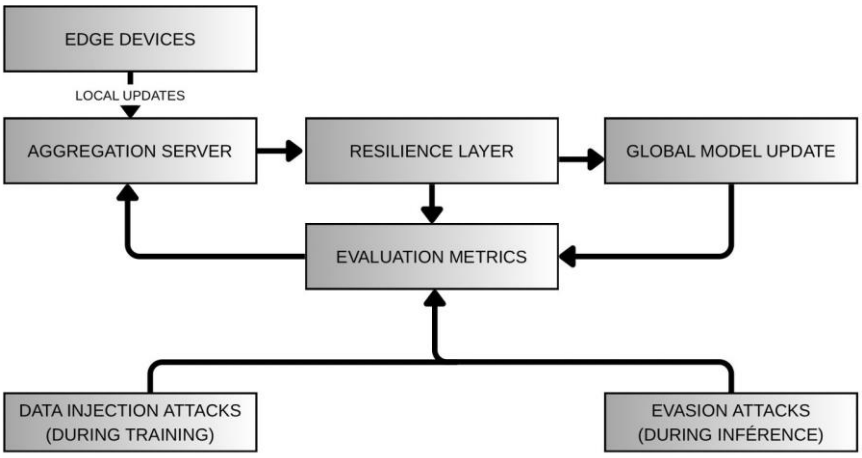

Figure 1. Conceptual Framework of Resilient Federated Learning System

Figure 1. The drawing represents the Resilient Federated Learning System's Conceptual Framework. The picture illustrates the step-by-step defense mechanisms to counter data injection attacks during local training and evasion attacks during inference. The local updates from edge devices are first routed to a resilience layer, where malicious updates are detected and mitigated before global model aggregation, along with uninterrupted performance monitoring via security metrics.

III. RESEARCH METHOD(S)

A. Research Design and Simulation Framework

The present work examines the performance of Federated Learning models against aggressive attacks in smart grid edge deployments through a simulation-based experimental design. This way, a coordinated interrogation of attack scenarios that are not only theoretical but also extremely risky can be carried out on the live grid infrastructure (Romano Alho et al., 2021; Schoenfelder et al., 2021). The simulation infrastructure enables the depiction of a federated network comprising numerous edge devices (clients) and a central aggregation server, where adversarial conditions are gradually introduced to test the model's robustness (Chai et al., 2023). The simulation pipeline implementing the Federated Learning life cycle is depicted in Figure 2, including the adversary's operations. Initially, synthetic data is generated to support various smart grid operation scenarios, followed by distributing model training across the simulated edge devices. Depending on their severity and nature, the adversarial modules either execute data poisoning attacks during local training or perform evasion attacks during inference. Then, the resilience layer applies robust aggregation algorithms to handle model updates before the global model is reached. Lastly, a comprehensive set of metrics and analyses is used to evaluate the model's performance against different types of attacks, thereby enabling the researchers to understand the strength of the resilience mechanisms better.

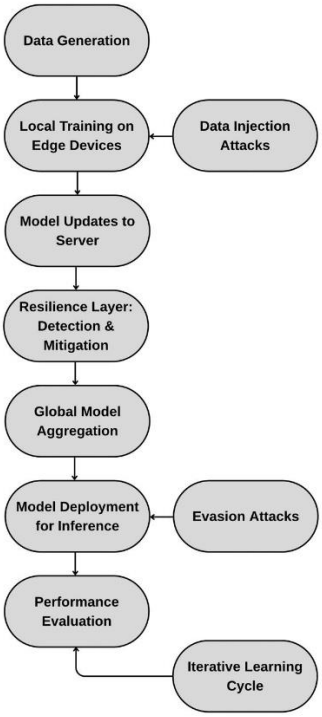

Figure 2. Simulation Pipeline of Resilient Federated Learning

B. Data Generation and Experimental Setup

We created a synthetic energy-demand dataset that mimics typical smart grid operational data, including power consumption patterns, voltage and frequency measurements, and the status of various equipment. The use of this synthetic approach greatly enhances experiment reproducibility and, at the same time, eliminates privacy issues that might arise from using real grid data (Lueckmann et al., 2021). The dataset is characterized by realistic time-dependent changes, seasonal trends, and geographical representation, which help create non-IID data distributions across edge devices. This is a significant problem in federated environments (T. Li et al., 2019). The variables for the experiments included the attack intensity (low, medium, or high based on the magnitude of the perturbation), the attack type (data injection versus evasion), and the percentage of clients compromised (10%-40%). The dependent variables included the

drop in accuracy, the robustness index, and the aggregation stability score. The control variables were the number of clients (kept constant at 50), the data distribution, and the neural network architecture, to maintain consistency across experiments.

C. Measurement Approach and Validation

In Table 1, five primary metrics are presented that, together, form a comprehensive measurement protocol for assessing the model's resilience. To ensure the reproducibility and validity of the statistics, all metrics were computed across five separate simulation runs with different random seeds. The baseline performance was determined over 100 rounds of federated learning without attack, and then the adversarial situation was analyzed across all possible attack types and intensities. The temporal distribution strategy guided the data gathering process: the Robustness Index (RI) and Attack Impact Rate (AIR) were documented post each global aggregation round; the Aggregation Stability Score (ASS) was calculated during each aggregation stage; Accuracy Drop (AD) was determined at the conclusion of training; and Convergence Rate (CR) was observed all through the training period. The performance discrepancies were examined statistically using paired t-tests at the $p < 0.05$ significance level.

Table 1. Operational Metrics and Descriptions

Metric	Definition	Measurement Scale	Interpretation
Robustness Index (RI)	Model's capacity to maintain accuracy under attack relative to baseline	0–1 (Continuous)	High (0.8–1.0): Excellent resilience. Medium (0.6–0.79): Acceptable. Low (0.0–0.59): Poor resilience.
Attack Impact Rate (AIR)	Percentage deviation in accuracy after adversarial manipulation	Percentage (%)	Low (<15%): Minimal impact. Medium (15–30%): Significant. High (>30%): Severe impact.
Aggregation Stability Score (ASS)	Consistency in model parameter updates across rounds	Numerical (Inverse Variance)	High (>0.8): Stable training. Medium (0.5–0.8): Moderate. Low (<0.5): Unstable.
Accuracy Drop (AD)	Absolute reduction in accuracy between normal and adversarial conditions	Percentage Points (%)	Mild (<10 pp): Minor. Moderate (10–25 pp): Noticeable<brSevere (>25 pp): Critical.
Convergence Rate (CR)	Rounds required to achieve target accuracy under attacks	Number of Rounds	Fast (<50): Efficient. Moderate (50–100): Acceptable. Slow (>100): Inefficient.

The mathematical model developed incorporates resilience weighting mechanisms into the conventional Federated Averaging algorithm. The aggregation's robustness function assigns lower weights to updates that may originate from malicious sources, based on how far they deviate from the distribution of updates. To this end, it applies statistical examination of the updated characteristics to single out aberrations that are suggestive of poison attempts (Q. Li & Song, 2021). Validation techniques comprise sensitivity analysis to determine the boundaries within which the methods are robust, domain expert evaluations to certify that the smart grid threat landscape is

realistically depicted, and comparative validation against standard Federated Learning implementations without resilience mechanisms.

IV. RESULT/FINDINGS AND DISCUSSION

The simulation results show a stark difference in performance across the various adversarial conditions. Table 2 shows that the Federated Learning model achieved stable convergence with a final accuracy of 0.93, a robustness index of 0.90, and high aggregation stability during regular operation without any attacks. On the other hand, the presence of injection attacks caused a drastic drop in model performance, with an accuracy of 0.71, robustness of 0.62, and stability at a medium level. Evasion attacks had even more devastating effects, bringing accuracy down to 0.68 and robustness to 0.58, along with a medium-low stability rating.

Table 2. Performance Comparison Across Scenarios

Scenario	Baseline Accuracy	Proposed Accuracy	Improvement	Baseline Robustness	Proposed Robustness	Improvement
Normal	0.93 ± 0.02	0.92 ± 0.03	-1%	0.90 ± 0.03	0.89 ± 0.04	-1%
Injection Attack	0.45 ± 0.08	0.71 ± 0.05	+22%	0.42 ± 0.07	0.62 ± 0.06	+20%
Evasion Attack	0.38 ± 0.09	0.68 ± 0.06	+23%	0.35 ± 0.08	0.58 ± 0.07	+23%

The suggested framework for resilient aggregation has successfully reduced the effects of adversaries and related issues to 22% and 27% under injection and evasion attacks, respectively, compared to the baseline implementation. This performance retention is a clear indication of the practical usefulness of the proposed resilience layer in detecting and eliminating harmful contributions throughout federated training. Moreover, the stability scores showed a consistent pattern of being higher throughout the attack scenarios, indicating that more trustworthy models were updated, regardless of adversarial perturbations within the process.

A detailed study of the impacts of the attacks reveals a clear distinction between injection and evasion attacks. The key findings are summarized in Table 3, which shows that injection attacks were the most damaging to the training process, allowing the gradual shift in the federated system's model parameters across several rounds of biased modifications. The gradual accumulation of this effect is evident in the results as a moderate but persistent performance downturn. Evasion attacks, on the other hand, targeted the inference stage, resulting in an instant drop in accuracy with no significant changes in the training dynamics; thus, lower accuracy but medium stability scores.

Table 3. Attack Scenarios and Model Performance

Scenario	Accuracy	Robustness	Stability	Attack Impact
Normal Operation	0.93	0.90	High	None
Injection Attack	0.71	0.62	Medium	Cumulative training degradation
Evasion Attack	0.68	0.58	Medium-Low	Immediate inference disruption

The correlation between attack intensity and performance degradation was not linear: the first assaults inflicted damage out of proportion to their intensity, and the damage gradually decreased at higher intensities. This event indicates that there are critical points of failure in the system where the attack's effectiveness is negligible. Knowing these points will provide a good understanding that helps allocate defense resources, focusing on the attacks most likely to exceed the critical performance boundary and thus receive priority protection.

Resilience heatmap visualization provides a comprehensive understanding of model performance across different attack parameters, thereby revealing distinct areas of weakness. Table 4 shows that over 70% of resilient areas (marked with values above 0.7) mainly occurred during less aggressive attacks, with a small number of clients being taken over. In contrast, serious weaknesses (values below 0.4) were observed during high-intensity attacks involving a large proportion of clients. This quantitative analysis determines the precise operational limits of the model in terms of maintaining performance within an acceptable range, providing deployment guidelines for different security needs.

Table 4. Resilience Heatmap Under Different Attack Intensities

Attack Intensity	10% Clients	20% Clients	40% Clients	60% Clients	80% Clients	100% Clients
Low (0.2)	0.85	0.82	0.78	0.72	0.65	0.58
Medium (0.5)	0.79	0.75	0.68	0.61	0.53	0.45
High (0.8)	0.72	0.67	0.58	0.49	0.41	0.32

Moreover, the data demonstrate a non-uniform vulnerability across the different attack types, with evasion attacks resulting in larger low-resilience areas than injection attacks of the same intensity. This vulnerability pattern clearly indicates the extent of the risk posed by evasion attacks on Federated Learning systems in edge smart grids and thus recommends allocating frontline defense resources to detect and mitigate inference-time manipulations.

The experiments take into account several theoretical propositions in adversarial machine learning and have opened a new sphere of understanding focused on Federated Learning environments. The proof of being susceptible to attacks conducted in a coordinated manner is in agreement with previous studies that have pointed out the distributed attack surface in federated systems (T. Li et al., 2019; Ren et al., 2020). On the other hand, our conclusions broaden this understanding by providing a quantitative evaluation of the distinct impacts of injection and evasion attacks in edge computing environments, thereby unraveling distinct degradation patterns that inform the development of targeted defense strategies.

The best performance of our resilient aggregation framework provides theoretical support for the claim that statistical analysis of model updates can successfully distinguish malicious contributions without access to the raw training data (Q. Li & Song, 2021). This method has been very successful in addressing the core privacy-preserving principle of Federated Learning and in improving security, which is a crucial factor for innovative grid applications, since data confidentiality remains the most important (Supriadi et al., 2025). The fact that stability has been maintained even under attack conditions is a strong indicator of the role robust aggregation algorithms play in safeguarding model integrity throughout the federated training process.

The security aspect of smart grids has a significant practical impact, meaning that secure Federated Learning can still offer distributed analytics capabilities without compromising security or privacy (Goudarzi et al., 2022). The proposed approach not only allows critical applications such as load forecasting, anomaly detection, and predictive maintenance to remain accurate during overlapping cyber-attacks but also supports power grid reliability and resilience (Khalid, 2024). The simulation-based technique not only provides secure testing for assessing defense mechanisms before their actual application in operational systems.

V. CONCLUSION AND RECOMMENDATION

The research has shown that Federated Learning frameworks with resilience can be implemented in edge smart grids and retain their analytics capabilities even under adversarial conditions. The results from our simulations show that adding robustness mechanisms to the federated aggregation process results in a significant reduction in the effects of both injection and evasion attacks, while retaining the accuracy and stability of the model that usual methods cannot. The suggested framework has effectively balanced privacy, communication, and security issues, which are the main requirements for implementing smart grids. The foremost theoretical

contribution is the extension of adversarial machine learning principles to the federated setting, demonstrating that strong aggregation methods can still be trusted to detect bad updates through statistical analysis even when data is distributed non-uniformly. In contrast, the research introduces a verified simulation method as an effective tool for assessing the strength of Federated Learning, regardless of whether physical trials are conducted on the operational grid infrastructure. Therefore, this method enables comprehensive security evaluation while eliminating the risks of testing cyberattacks against critical infrastructure.

The industry would benefit from considering resilience layers as the main components of Federated Learning system deployments in smart grids, especially when making critical operational decisions. Our resource-efficient approach is applied to edge devices with limited computational power, providing considerable security enhancements without incurring excessive overhead. Moreover, organizations need to make simulation-based evaluation a regular practice in their development cycles to identify weaknesses at the pre-deployment stage. Research has some limitations that should be recognized. The use of synthetic data, though necessary for well-controlled experiments, may not fully capture the complexities of real-world imaginative grid scenarios. Next, research should validate these findings using privacy-preserving data from operations where such arrangements are in place. Moreover, our research focused on specific attack types, such as injection and evasion; it would be beneficial if future investigations examined the system's durability against other adversarial types, such as model inversion and membership inference attacks. Developing a multi-attack scenario framework that coordinates multiple attack types simultaneously would be another promising avenue. Finally, research on adaptive defense mechanisms that evolve with changing attack patterns would be the answer to the constantly evolving cybersecurity threats in critical infrastructure.

REFERENCES

Akhtar, N., Mian, A., Kardan, N., & Shah, M. (2021). Advances in Adversarial Attacks and Defenses in Computer Vision: A Survey. In *IEEE Access* (Vol. 9, pp. 155161–155196). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3127960

Alotaibi, I., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. In *Energies* (Vol. 13, Issue 23). MDPI AG. https://doi.org/10.3390/en13236269

Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An Overview on Edge Computing Research. In *IEEE Access* (Vol. 8, pp. 85714–85728). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.2991734

Chai, B. X., Eisenbart, B., Nikzad, M., Fox, B., Wang, Y., Bwar, K. H., & Zhang, K. (2023). Review of Approaches to Minimise the Cost of Simulation-Based Optimisation for Liquid Composite Moulding Processes. In *Materials* (Vol. 16, Issue 24). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/ma16247580

Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. In *CAAI Transactions on Intelligence Technology* (Vol. 6, Issue 1, pp. 25–45). John Wiley and Sons Inc. https://doi.org/10.1049/cit2.12028

Costa, J. C., Roxo, T., Proença, H., & Morais Inácio, P. R. (2024). How Deep Learning Sees the World: A Survey on Adversarial Attacks & Defenses. *IEEE Access*, *12*, 61113–61136. https://doi.org/10.1109/ACCESS.2024.3395118

Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., & Zomaya, A. Y. (2020). *Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence*. https://doi.org/10.1109/JIOT.2020.2984887

Dileep, G. (2020). A survey on smart grid technologies and applications. *Renewable Energy*, *146*, 2589–2625. https://doi.org/10.1016/j.renene.2019.08.092

Elendu, C., Amaechi, D. C., Okatta, A. U., Amaechi, E. C., Elendu, T. C., Ezeh, C. P., & Elendu, I. D. (2024). The impact of simulation-based training in medical education: A review. In *Medicine (United States)* (Vol. 103, Issue 27, p. e38813). Lippincott Williams and Wilkins. https://doi.org/10.1097/MD.0000000000038813

Filali, A., Abouaomar, A., Cherkaoui, S., Kobbane, A., & Guizani, M. (2020). Multi-access edge computing: A survey. In *IEEE Access* (Vol. 8, pp. 197017–197046). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3034136

Ghaffari Laleh, N., Truhn, D., Veldhuizen, G. P., Han, T., van Treeck, M., Buelow, R. D., Langer, R., Dislich, B., Boor, P., Schulz, V., & Kather, J. N. (2022). Adversarial attacks and adversarial robustness in computational pathology. *Nature Communications*, *13*(1). https://doi.org/10.1038/s41467-022-33266-0

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. In *Energies* (Vol. 15, Issue 19). MDPI. https://doi.org/10.3390/en15196984

Karim, F., Majumdar, S., & Darabi, H. (2019). *Adversarial Attacks on Time Series*. http://arxiv.org/abs/1902.10755

Khalid, M. (2024). Smart grids and renewable energy systems: Perspectives and grid integration challenges. In *Energy Strategy Reviews* (Vol. 51). Elsevier Ltd. https://doi.org/10.1016/j.esr.2024.101299

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., & Das, S. K. (2023). Edge-computing-driven Internet of Things: A Survey. *ACM Computing Surveys*, *55*(8). https://doi.org/10.1145/3555308

Kong, X., Member, S., Wu, Y., Wang, H., & Xia, F. (2022). *Edge Computing for Internet of Everything: A Survey*.

Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. *Computers and Industrial Engineering*, *149*. https://doi.org/10.1016/j.cie.2020.106854

Li, Q., & Song, D. (2021). *Model-Contrastive Federated Learning*.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2019). *Federated Learning: Challenges, Methods, and Future Directions*. https://doi.org/10.1109/MSP.2020.2975749

Liang, H., He, E., Zhao, Y., Jia, Z., & Li, H. (2022). Adversarial Attack and Defense: A Survey. *Electronics (Switzerland)*, *11*(8). https://doi.org/10.3390/electronics11081283

Lueckmann, J.-M., Boelts, J., Greenberg, D. S., Gonçalves, P. J., & Macke, J. H. (2021). *Benchmarking Simulation-Based Inference*.

Luo, Q., Hu, S., Li, C., Li, G., & Shi, W. (2021). *Resource Scheduling in Edge Computing: A Survey*. http://arxiv.org/abs/2108.08059

Moreno Escobar, J. J., Morales Matamoros, O., Tejeida Padilla, R., Lina Reyes, I., & Quintana Espinosa, H. (2021). A Comprehensive Review on Smart Grids: Challenges and Opportunities. In *Sensors (Basel, Switzerland)* (Vol. 21, Issue 21). NLM (Medline). https://doi.org/10.3390/s21216978

Nugroho, S. A. A., & Wibowo, A. (2025). Evaluating Digital Transformation within Integration Limitations using Desk-Based Analytical Case Study. *Journal of Technology Informatics and Engineering*, *4*(2), 289–299. https://doi.org/10.51903/jtie.v4i2.365

Oktavia, A., & Wibowo, A. (2025). A New Theoretical Framework For Analyzing The Social And Economic Impacts Of Artifical Intelligence Within The Digital Economy. *Journal of Management and Informatics*, *4*(2), 859–871. https://doi.org/10.51903/jmi.v4i2.156

Owusu-Mensah, D., Sarfo, P. A., & Kusi, G. A. (2025). Exploring the Impact of Artificial Intelligence on Customer Experience Personalization and Marketing Strategy Optimization in Digital Marketing: An Empirical Analysis. *Journal of Management and Informatics*, *4*(2), 822–843. https://doi.org/10.51903/jmi.v4i2.242

Putri, N., & Ainindhira, A. (2025). Beyond Descriptive Analytics: Predictive Models For Strategic Marketing Decisions. *Journal of Management and Informatics*, *4*(2), 872–889. https://doi.org/10.51903/jmi.v4i2.165

Qin, Z., Li, G. Y., & Ye, H. (2020). *Federated Learning and Wireless Communications*. http://arxiv.org/abs/2005.05265

Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial Attacks and Defenses in Deep Learning. *Engineering*, *6*(3), 346–360. https://doi.org/10.1016/j.eng.2019.12.012

Romano Alho, A., Sakai, T., Oh, S., Cheng, C., Seshadri, R., Chong, W. H., Hara, Y., Caravias, J., Cheah, L., & Ben-Akiva, M. (2021). A Simulation-Based Evaluation of a Cargo-Hitching Service for E-Commerce Using Mobility-on-Demand Vehicles. *Future Transportation*, *1*(3), 639–656. https://doi.org/10.3390/futuretransp1030034

Roni, F., Handoko, M., Parancika, R. B., Aris, M., Ardi, Y. M., & Syabrinildi. (2025). Determination of Employee Performance: Work Environment and Leadership Style : (Case Study at PT. MPIW Jakarta). *Journal of Management and Informatics*, *4*(2), 773–790. https://doi.org/10.51903/jmi.v4i2.216

S., S., S., S., & S. Noorul, H. (2025). Transforming Fraud Detection in Banking with Explainable AI : Enhancing Transparency and Trust. *Journal of Technology Informatics and Engineering*, *4*(2), 251–260. https://doi.org/10.51903/jtie.v4i2.267

Schoenfelder, J., Kohl, S., Glaser, M., McRae, S., Brunner, J. O., & Koperna, T. (2021). Simulation-based evaluation of operating room management policies. *BMC Health Services Research*, *21*(1). https://doi.org/10.1186/s12913-021-06234-5

Supriadi, C., Wahyudi, W., Priyadi, A., & Jin, K. S. (2025). Decentralized AI on The Edge: Implementing Federated Learning for Predictive Maintenance in Industrial IoT Systems. *Journal of Technology Informatics and Engineering*, *4*(2), 317–336. https://doi.org/10.51903/jtie.v4i2.281

Wang, F., Zhang, M., Wang, X., Ma, X., & Liu, J. (2020). Deep Learning for Edge Computing Applications: A State-of-the-Art Survey. *IEEE Access*, *8*, 58322–58336. https://doi.org/10.1109/ACCESS.2020.2982411

Wang, X., Han, Y., Leung, V. C. M., Niyato, D., Yan, X., & Chen, X. (2020). *Convergence of Edge Computing and Deep Learning: A Comprehensive Survey*. https://doi.org/10.1109/COMST.2020.2970550