

RESEARCH ARTICLE

OPEN ACCESS

A COMPARATIVE SURVEY ON FEDERATED LEARNING AND SELF-LEARNING FOR PRIVACY PRESERVATION OF PARTICIPANTS' DATA IN TRANSACTIVE ENERGY SYSTEMS

Oluwaseun O. Tooki^{*1}, Olawale M. Popoola² and Mudasiru A. Saloro³

^{1,2}Department of Electrical Engineering, Faculty of Engineering and the Built Environment, Tshwane University of Technology, Pretoria, South Africa.

³Department of Electrical and Electronic Engineering, Faculty of Ground and Communication Engineering, Air Force Institute of Technology, Kaduna, Nigeria.

¹<https://orcid.org/0000-0002-3554-8004> , ²<https://orcid.org/0000-0002-9980-5241> , ³<http://orcid.org/0009-0009-5324-5662> 

E-mail: *TookiOO@tut.ac.za, PopoolaO@tut.ac.za, M.asoloro@afit.edu.ng.

ARTICLE INFO

Article History

Received: November 01, 2025

Reviewed: December 17, 2025

Accepted: April 10, 2026

Published: June 30, 2026

Keywords:

Federated Learning (FL),
Self-Learning (SL),
Privacy-Preservation,
Transactive Energy System
(TES).

ABSTRACT

Transactive Energy System (TES) has emerged as a promising paradigm for coordinating Renewable Energy generation, consumption, and delivery. However, participants' sensitive data transmitted over the network in the TES framework must be preserved against cyber-attacks as more Distributed Energy Resources (DERs) come online. This article aims to conduct a comparative survey of two Machine Learning (ML) techniques, Federated Learning (FL) and Self-Learning (SL), to determine which is most suitable for preserving participants' data privacy in TES, based on the existing literature. The performance of their models was evaluated with a focus on resilience and network stability. The work examines, predicts, and uncovers meaningful patterns in the application of FL and SL techniques around privacy preservation. Findings revealed that FL is the most appropriate choice, as it allows collaborative model training, unlike SL, which utilizes centralized data, exposing it to privacy risks. Furthermore, the efficiency of FL-based TES is superior because it eliminates communication delays and does not require sending the entire raw data to the central server. In conclusion, the research demonstrated that FL-based TES is secure and inherently decentralized. Hence, FL is suitable for preserving participants' data in TES.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

The geometric rise in the integration of distributed energy resources (DERs) at energy distribution and utilization levels, enhanced by advancements in smart metering, energy management, and Information and Communication Technology (ICT), has transformed conventional electricity consumers into prosumers. These prosumers can monitor and control their generation, consumption, and energy storage in real time, to facilitate energy cost savings [1]. Recently, peer-to-peer (P2P) Transactive Energy Systems (TES) have emerged as a new energy market model, promising a more thorough and effective utilization of available renewable production and DER flexibility by prosumers [2] [3]. It uses control and economic mechanisms to achieve a dynamic balance of energy supply and demand across the entire electrical grid, with value as a main operational metric [4].

TES can be further described as a group of connected peers that use prices and incentives to sustain economic benefits for participants [5]. TES permits trade of electricity in real-time based on their energy consumption and generation prediction [6]. It is an emerging solution with features to secure critical loads during generation deficits and support electrical infrastructure when transmission and distribution networks are non-operational, which may be due to natural disasters such as Hurricane Maria, which was recorded in 2017 in Puerto Rico, where 80% of the grid collapsed [7]. However, the rapid integration of Internet of Things (IoT) and the adoption of Intelligent edge devices for processing IoT data into energy systems bring about the unprecedented growth in the digitalization of the energy sector based on the data volume generated by participants [8] [9].

Nonetheless, there are security challenges associated with this advancement, which include data integrity, authentication, scalability, and privacy leakage (that is, personal information and energy consumption patterns of participants) [10]. Hence, this prompts the need to protect this data against the activities of adversaries and to leverage the potential of intelligent techniques in making rational choices regarding grid services [11]. Distributed Machine Learning (ML), such as Federated learning (FL) and Self-Learning (SL), has proved to be a promising technique that permits multiple entities, across edge devices, to train a distributed model without direct raw data sharing [12]. The FL's architecture enables collaborative and privacy-preserving training on ML models to [10] [11]. The choice of FL in recent times is based on its features and the distinctive training approach that permits training of local models in each agent, beyond the collection of the entire data from other agents to the main server [11]. It alleviates concerns about privacy protection, as only the updated parameters (gradients or weights) are transferred during model training [13]. FL was portrayed as a catalyst with the potential to resolve data privacy and security issues in [14]. A privacy-preserving FL scheme was presented for IoT intrusion detection [15]. Researchers are probing the application of FL.

Some of them include a Clustered Asynchronous FL (CAFL), which was proposed for Energy-Harvesting Smart Meters in P2P Energy Trading (ET) in [12]. Ref. [7] introduced a privacy-aware FL framework for DER analytics in constrained environments. Du et al. [16] presented an FL-assisted distributed energy optimization, while Mendes et al [17] suggested an FL framework for predicting net energy demand in TES. The role of FL in preserving the privacy of IoT devices was reported in [18], while centralized and decentralized architectures were compared in [19]. Ref. [20] reported three privacy threats in the FL central server: susceptibility, gradient leakage attacks, and collusion among participants. The authors further explored three privacy techniques —Homomorphic Encryption (HE), Differential Privacy, and Multi-party Computation — to address privacy issues. A survey of optimization methods in privacy-preserving FL with HE was reported in [21]. Privacy-preserving techniques were deployed by hybridizing FL with blockchain for telemedicine in [22], while Yin et al [23] presented a 5W-scenario-based taxonomy (Who, what, when, where, and why) to classify the potential privacy leakage risks in FL. Ref. [24] proposed a decentralized FL framework for consumers' privacy preservation and energy theft detection using HE.

An ML-based technique was proposed to address IoT privacy challenges in [25]. Federated Reinforcement Learning (RL) was reported for privacy-preserving integrated thermal and energy management of multi-connected hybrid EVs [26], while Federated Deep RL was introduced to address privacy-preserving issues in Energy Management Systems with shared energy storage for Smart houses [27]. A hybridization of FL and Transfer Learning (TL) was suggested for privacy-preserving HVAC systems [28], whereas privacy-preserving heterogeneous federated TL was reported in [29]. These analyses established recent advances in the application of FL in privacy preservation in energy systems. However, little or nothing has been extensively reported for TES. In summary, the key contribution of this work is to: (1) examine, predict, and uncover meaningful patterns in the application of FL and SL techniques around privacy preservation; (2) present a comparative analysis of these ML-based techniques to determine the best-suited for privacy preservation in TES for the network stability and resilience. The rest of the paper is organized as follows: Section II showcases the relevant research on privacy-preserving techniques in TES, and an overview of reported literature on FL and SL-based methods for privacy preservation in Energy Systems. In Section III, we evaluate the performance of FL and SL-based Models for privacy preservation in energy systems. Section IV focuses on the discussion and reported findings, while Section V is the Conclusion and future research outlook.

II. RELEVANT RESEARCH

II.1 PRIVACY-PRESERVING TECHNIQUES IN TES: OVERVIEW

Mechanisms must be put in place to protect participants' sensitive information in TES. Information such as data usage, asset ownership records, and market bid/ask prices. A privacy-preserving distributed coordination algorithm was introduced for protecting participants' data in TES in [6]. The authors' literature corroborates the existence of cryptographic techniques for data protection. Ref. [30] presented a cryptography-based method (HE-based algorithm) to address privacy and security concerns associated with TES deployment over insecure communication channels, protection of agents' bidding details, and quick detection of external injection of malicious data during market interactions. The authors employed Paillier encryption, Paillier digital signature, and Stamp concatenation techniques for privacy preservation.

Relatedly, Paillier cryptography and calibrated noise were proposed for confidentiality and privacy preservation, respectively [10]. The introduced privacy protection solution uses calibrated noise to facilitate fair transactions among participants and to conserve participant behaviour patterns. The authors achieved 41.07% privacy protection with the proposed solution. A blockchain-based privacy-preserving distributed algorithm with a smart contract to minimize the quantity of information exposed to other participants during ET using asymmetric cryptography for TES [31]. developed a decentralized P2P ET algorithm with two stages, on the blockchain, to preserve participants' privacy [32]. An FL-based framework was presented, utilizing local generation data obtained from a university, to predict the net demand of a building in TES settings [33].

II.2 FEDERATED LEARNING FOR PRIVACY PRESERVATION IN ENERGY SYSTEMS

In recent years, the application of FL for privacy preservation has become a centre for research. Liu et al. [12] proposed an energy-aware FL protocol to prioritize systems with adequate energy reserves dynamically, developed an adaptive dual-phase clustering strategy to mitigate preference inference attacks, and introduced a blockchain framework to establish a tamper-proof energy harvesting system in a P2P ET environment. The proposed CAFL resisted preference profiling attacks, confirming the model's robustness and its convergence under intermittent energy conditions. Consequently, similar research was reported. A FL-assisted distributed consensus approach was presented to forecast agents' local energy generation and demand for minimizing errors and improving forecast accuracy for net power demand prediction [16]. The authors further explored the proposed model to resolve the multi-agent distributed energy aggregation challenge in TES.

When comparing the prediction results obtained for FL forecasted (FLF) and Local Model forecasted (LMF), it indicates that FLF shows superiority over LMF with a greater accuracy of 1.36 times for April, for the first community (100 buildings), and 8 times for the second community (25 Buildings) for August. Relatedly, the same team of authors in [7] transitioned from applying FL for DER optimization to predicting net energy demand in the TES environment using FL in [17]. An FL architecture with two independent forecast systems, generation and demand systems, to facilitate collaborative learning among the buildings without sharing private data, and to support the management systems of TES. The authors introduced an auxiliary horizontal Federated TL (FTL) to enhance the forecast system. The buildings were divided into two groups of 100 and 25. The FTL was integrated by transferring the model weights between the servers responsible for the Groups. Group B realizes a better average of 0.07056 as against 0.09386 obtained by Group A. According to the authors, the FTL has the potential to enhance the forecast system's reliability.

Venkataramanan et al. [8] introduced an FL algorithm to forecast DER, transmitting a model of the consumption and generation patterns of 100 DERs for 24 hours without revealing consumer data. The work was evaluated using grid-specific performance metrics (load swings and load curtailment), while the simulation was validated using real data from the Pecan Street dataset. The research achieves a forecast with a root-mean-square error (RMSE) of 1.3 for 1000 IoT nodes and a 1.98 RMSE for real field data. However, the authors failed to establish that there is an existing trade-off between accuracy and privacy when using the FL approach. A comprehensive analysis of the application of FL in the energy sector, energy markets, and cybersecurity (fault detection, energy theft detection) was reported in [11]. Table 1 reflects FL applications in energy systems with their research significance, while Figure 1 illustrates the workflow of centralized FL.

Table 1. Application of FL in Energy Systems.

Ref.	FL	Research Significance
[12]	Clustered Asynchronous FL	Energy autonomy of smart meters and privacy preservation under intermittent communication conditions.
[7]	Privacy-aware FL using Fog model	Conceptualization of the FL framework using the Fog model for DER analytics
[16]	FL-assisted distributed consensus	To reduce errors in predicting net power demand
[8]	DER forecasting	DER forecasting and evaluation of grid-specific performance metrics (load swings and load curtailment)
[17]	Prediction of net energy demand	Predicting building temporal net energy demand

Source: Authors, (2026).

II.3 SELF- LEARNING FOR PRIVACY PRESERVATION IN ENERGY SYSTEMS

An SL-based adaptive framework, powered by the Soft Actor-Critic algorithm, was presented to enhance the energy management model, which resulted in a 45% energy reduction [34]. Wei et al [35] developed a novel SL parallel control technique to address the optimal control issue of discrete-time time-variant nonlinear systems. The adaptive dynamic programming-based SL method was utilized to ensure value function convergence and optimal policy. Ref. [36] proposed a SL control technique for decentralized winter-operated household ventilation systems for comfort and energy efficiency of occupants. The SL successfully learns the occupants' ventilation preferences. Zhou [37] reported a dynamic SL grid-responsive approach in enhancing energy flexibility and techno-economic needs of electrochemical batteries by adjusting off-peak grid charging power, thereby facilitating interactive energy networks in smart cities. A state SL approach was proposed to achieve distributed intelligent control in a multiple-reactor cascade operation, to capture the reactor's time-varying non-linear dynamics, and to enhance control performance [38]. The applicability of the technique was demonstrated in a cascaded zinc extraction process. An SL approach was presented to facilitate the decision-making process of a heterogeneous robot under uncertainty in [39].

III. PERFORMANCE EVALUATION OF FL AND SL-BASED MODELS ON PRIVACY PRESERVATION

When preserving the privacy of participants in TES, there must be a balance between privacy, model accuracy, and the efficiency of the algorithm [20]. In the review presented in [40], established that FL has been used in Renewable Energy (RE) for resource forecasting and that its local model surpasses other models in preserving data privacy. A Mathematical model was introduced to evaluate FL-based blockchain-enabled task scheduling to reduce energy consumption and delay by 41% and 28%, respectively [41]. An energy-aware architectural model was investigated and developed in [42]. Table 2 presents the performance evaluation of FL and SL models for privacy preservation.

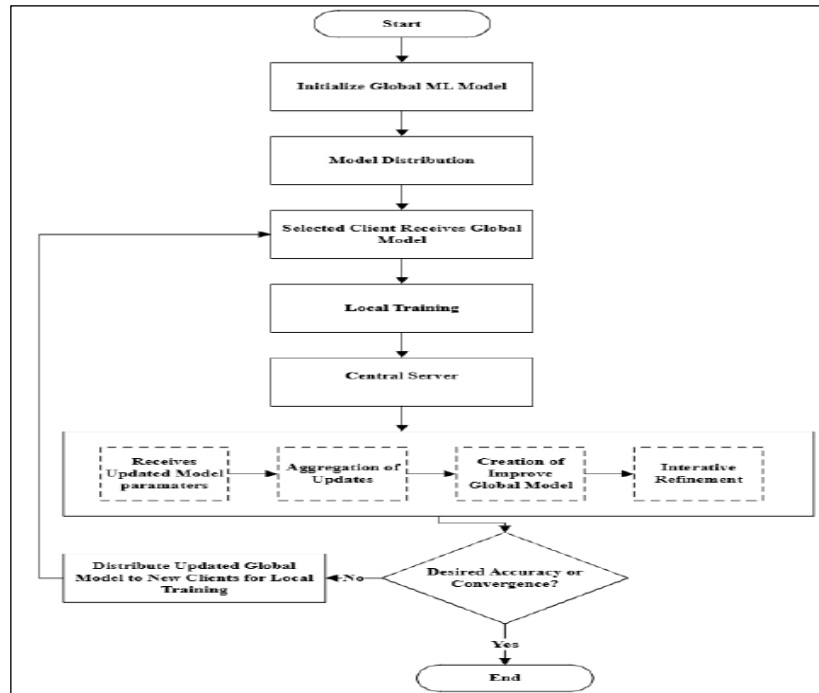


Figure. 1 Centralized FL Workflow
Source: Authors, (2026).

Table 2. Performance Evaluation of FL And SL Models.

Ref.	FL		Ref.	SL	
	Task	Performance		Task	Performance
[43]	Modeling of Distributed Anomaly Detection in Smart Grids (SGs)	Models performed effectively in terms of memory utilization	[38]	Distributed Intelligent Control	The model successfully decomposed a complex nonlinear control problem into sub-problems.
[44]	Modeling of Virtual Power Plant using multi-task FL for decentralizing the EMS processing	The results indicate that multi-pattern-multi-task FL is 41% better than the best-recorded models	[45]	SL-based model to iteratively learn the transition matrix when the pre-event and post-event states are unknown	The model demonstrates its suitability in solving practical problems in the energy sector
[46]	A privacy-preserving spatial-temporal adaptive personalized FL model for Multi-energy	The model achieves 14.86% effectiveness in terms of forecasting accuracy when compared with the baseline FL models.	[47]	SL-based model with an HE algorithm to mitigate privacy exposure threats	The model outperformed others as it shows better convergence speed and enhanced scalability features
[48]	Prevention of sensitive private data in short-term photovoltaic power forecasting using FL.	FL-based model surpasses others with improved Root Mean Square error of up to 10% in ensuring data security	[49]	Modeling of Possibilistic Model Checking using SL.	Achieved better learning performance.
[50]	FL-based secure model for energy optimization in SG	FL-based predictive model accurately forecasted RE generation and electric load in a privacy-oriented manner.			

Source: Authors, (2026).

IV. DISCUSSION AND FINDINGS

In the literature for privacy preservation in TES, blockchain-based techniques are the most widely utilized. Some of these techniques include HE-based algorithms, Paillier cryptography, and asymmetric cryptography. However, there is a limitation to these blockchain-based methods: the entire ET information stored on the network is available to all participants, thereby exposing users' data. Consequently, a malicious attacker may exploit this avenue for financial gain or espionage. In the application of SL in decentralized energy systems, a review of relevant literature shows that SL-based adaptive frameworks have been used to enhance energy management, whereas SL-based parallel control techniques were reported in resolving optimal control issues and for decentralized ventilation systems. Additionally, a dynamic SL grid-responsive approach was explored to enhance energy flexibility, while a state SL approach was proposed to achieve distributed intelligent control. The survey demonstrates that the SL technique is unsuitable for privacy preservation due to challenges, such as centralized vulnerabilities, data control, efficiency, and non-collaborative features, which prevent multiple participants from locally training a model. It was discovered that privacy-preserving techniques do not significantly affect the model's accuracy but may introduce computational and communication overhead. Furthermore, the survey shows that privacy-preserving techniques, such as FL, can optimize privacy, accuracy, and efficiency. However, one must carefully consider finding a balance between security and system performance. Consequently, all the reviewed articles on privacy-preserving techniques show that researchers have not explored the suitability of either FL or SL in TES, even though our findings established that FL is more suitable.

V. CONCLUSION AND FUTURE OUTLOOK

This survey successfully examined patterns in the application of FL and SL techniques for privacy preservation. Also presented is a comparative analysis of these ML-based techniques to determine the best fit for privacy preservation in TES to enhance network stability and resilience. The investigation reveals that FL offers robust privacy protections and supports decentralization as the data resides with participants during model training. In comparison with SL, which is centralized, all data are essentially aggregated into a main server for training. Therefore, raises concerns about the privacy and security of sensitive data. Its features allow TES participants to engage in ET without disclosing their private information. The research demonstrated that FL-based TES is secure and inherently decentralized, like P2P-based TES. Hence, FL's suitability in preserving participants' data. The work highlights the need for further research by exploring the integration of FL with Blockchain Technology to resolve emerging privacy issues in TES and to enhance efficiency and security. Additionally, challenges such as scalability and statistical heterogeneity require more attention. The contribution of this investigation will serve as a reference for future research.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Oluwaseun Tooki and Olawale Popoola.

Methodology: Oluwaseun Tooki, Olawale Popoola and Mudasiru Saloro.

Investigation: Oluwaseun Tooki, Olawale Popoola and Mudasiru Saloro.

Discussion of results: Oluwaseun Tooki, Olawale Popoola and Mudasiru Saloro.

Writing – Original Draft: Oluwaseun Tooki.

Writing – Review and Editing: Oluwaseun Tooki, Olawale Popoola and Mudasiru Saloro.

Resources: Oluwaseun Tooki and Olawale Popoola.

Supervision: Olawale Popoola.

Approval of the final text: Oluwaseun Tooki, Olawale Popoola and Mudasiru Saloro.

VII. ACKNOWLEDGMENTS

This work is based on the research supported wholly/in part by the National Research Foundation of South Africa (Grant Number: 150574), and Tshwane University of Technology - Faculty of Engineering and Built Environment and Centre for Energy and Electric Power.

VIII. REFERENCES

- [1] Y. Ye, Y. Tang, H. Wang, X. Zhang, and G. Strbac, "A Scalable Privacy-Preserving Multi-Agent Deep Reinforcement Learning Approach for Large-Scale Peer-to-Peer Transactive Energy Trading," *IEEE Trans Smart Grid*, vol. 12, no. 6, pp. 5185–5200, 2021.
- [2] O. O. Tooki, O. M. Popoola, and J. D. Pam, "Towards sustainable energy : Implementation framework for a decentralized peer-to-peer transactive energy system," *Aims Energy*, vol. 13, no. April, pp. 962–986, 2025, doi: 10.3934/energy.2025036
- [3] D. Sousa-Dias, D. Amyot, A. Rahimi-Kian, and J. Mylopoulos, "A Review of Cybersecurity Concerns for Transactive Energy Markets," *Energies (Basel)*, pp. 133–149, 2021, doi: 10.4324/9781315617213-17.
- [4] O. O. Tooki and O. M. Popoola, "A comprehensive review on recent advances in transactive energy system : Concepts , models , metrics , technologies , challenges , policies and future," *Renewable Energy Focus*, vol. 50, no. June, pp. 1–19, 2024, doi: <https://doi.org/10.1016/j.ref.2024.100596>.
- [5] O. O. Tooki and O. M. Popoola, "A systematic review on blockchain-based energy trading in a decentralized transactive energy system : Opportunities , complexities , strategic challenges , research directions," *Results in Engineering*, vol. 27, no. May, 2025, doi: <https://doi.org/10.1016/j.rineng.2025.106237>
- [6] F. R. Ranjbar, S. N. Ravadanegh, and A. Safari, "Transactive energy trading in distribution systems via privacy-preserving distributed coordination," *Appl Energy*, vol. 361, no. January, p. 122823, 2024, doi: 10.1016/j.apenergy.2024.122823.
- [7] A. Sundararajan, R. A. Bridges, M. Olama, and M. Ferrari, "A Privacy-Aware Federated Learning Framework for Distributed Energy Resource Analytics in Constrained Environments," in *IEEE PES Innovative Smart Grid Technologies (ISGT-LA)*, 2023, pp. 155–159. doi: 10.1109/ISGT-LA56058.2023.10328226.

- [8] V. Venkataramanan, S. Kaza, and A. M. Annaswamy, "DER Forecast Using Privacy-Preserving Federated Learning," IEEE Internet Things J, vol. 10, no. 3, pp. 2046–2055, 2023, doi: 10.1109/JIOT.2022.3157299.
- [9] O. Tooki and O. Popoola, "Intelligent-Based Techniques for Detection, Identification and Mitigation of Cyberattacks in Cyber-Physical Power Systems: A Review," 2024 IEEE PES/IAS PowerAfrica, PowerAfrica 2024, pp. 0–4, 2024, doi: 10.1109/PowerAfrica61624.2024.10759370.
- [10] V. Anil and S. L. Arun, "Security and Market Liquidity Enhanced Transactive Energy System for Residential End Users," IEEE Access, vol. 13, no. December 2024, pp. 24833–24851, 2025, doi: 10.1109/ACCESS.2025.3538330.
- [11] R. A. N. Zheng, A. Sumper, and S. Galceran-arellano, "Advancing Power System Services With Privacy-Preserving Federated Learning Techniques : A Review," IEEE Access, no. June, pp. 76753–76780, 2024.
- [12] Z. Liu et al., "Clustered Federated Learning for Energy-Harvesting Smart Meters in P2P Energy Trading," IEEE Transactions on Green Communications and Networking, pp. 1–12, 2025, doi: 10.1109/TGCN.2025.3591768.
- [13] Z. Liu, J. Guo, W. Yang, J. Fan, K. Lam, and S. Member, "Privacy-Preserving Aggregation in Federated Learning : A Survey," IEEE Trans Big Data, pp. 1–20, 2022, doi: 10.1109/TBDATA.2022.3190835.
- [14] R. S. Peres and A. Manta-costa, "Implementing Privacy-Preserving and Collaborative Industrial Artificial Intelligence," IEEE Access, no. July, pp. 74579–74589, 2023, doi: 10.1109/ACCESS.2023.3296143.
- [15] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of Things Intrusion Detection : Centralized , On-Device , or Federated Learning ?," no. December, pp. 310–317, 2020.
- [16] Y. Du, N. Mendes, S. Rasouli, J. Mohammadi, and P. Moura, "Federated learning assisted distributed energy optimization," IET Renewable Power Generation, no. August, pp. 2524–2538, 2024, doi: 10.1049/rpg2.13101.
- [17] N. Mendes, J. Mendes, J. Mohammadi, and P. Moura, "Federated learning framework for prediction of net energy demand in transactive energy communities," Sustainable Energy, Grids and Networks, vol. 40, no. August, 2024, doi: <https://doi.org/10.1016/j.segan.2024.101522>.
- [18] T. Alam and R. Gupta, "Federated Learning and Its Role in the Privacy Preservation of IoT Devices," Future Internet, pp. 1–22, 2022, doi: <https://doi.org/10.3390/fi1409024>.
- [19] J. Chen, H. Yan, Z. Liu, M. I. N. Zhang, H. U. Xiong, and S. Yu, "When Federated Learning Meets Privacy-Preserving," ACM Comput Surv, vol. 56, no. 12, 2024.
- [20] J. Lu, "Survey on Privacy-Preserving Techniques for Federated Learning," in Proceedings of the 2nd International Conference on Data Science and Engineering (ICDSE 2025), Science and Technology Publications, 2025, pp. 40–46. doi: 10.5220/0013677800004670.
- [21] Q. Xie, S. Jiang, L. Jiang, Y. Huang, and Z. Zhao, "Efficiency Optimization Techniques in Privacy-Preserving Federated Learning With Homomorphic Encryption : A Brief Survey," IEEE Internet Things J, vol. 11, no. 14, pp. 24569–24580, 2024.
- [22] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, "Healthcare Analytics A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine," Healthcare Analytics, vol. 3, no. February, 2023.
- [23] X. Yin, Y. Zhu, and J. Hu, "A Comprehensive Survey of Privacy-preserving Federated Learning : A Taxonomy , Review , and Future Directions," ACM Comput Surv, vol. 54, no. 6, 2021.
- [24] X. Wang et al., "Decentralized Privacy-Preserving Electricity Theft Detection for Distribution System Operators," IEEE Trans Smart Grid, vol. 15, no. 2, pp. 2179–2190, 2024, doi: <https://doi.org/10.1109/TSG.2023.3313771>.
- [25] S. El-gendy, M. S. Elsayed, and A. Jurecut, "Privacy Preservation Using Machine Learning in the Internet of Things," Mathematics, no. M1, pp. 1–35, 2023.
- [26] A. Khalatbarisoltani, J. Han, M. Saeed, C. Liu, and X. Hu, "Privacy-preserving integrated thermal and energy management of multi connected hybrid electric vehicles with federated reinforcement learning," Appl Energy, vol. 385, no. August 2024, 2025, doi: <https://doi.org/10.1016/j.apenergy.2025.125386>.
- [27] D. Choi, "Privacy-Preserving Energy Management of a Shared Energy Storage System for Smart Buildings : A Federated Deep Reinforcement Learning Approach," Sensors, 2021, doi: <https://doi.org/10.3390/s21144898> Academic.
- [28] Z. Wang, G. S. Member, P. Yu, and G. S. Member, "Privacy-Preserving Regulation Capacity Evaluation for HVAC Systems in Heterogeneous Buildings Based on Federated Learning and Transfer Learning," IEEE Trans Smart Grid, vol. 14, no. 5, pp. 3535–3549, 2023, doi: <https://doi.org/10.1109/TSG.2022.3231592>.
- [29] D. Gao, Y. Liu, A. Huang, C. Ju, H. Yu, and Q. Yang, "Privacy-preserving Heterogeneous Federated Transfer Learning," in IEEE International Conference on Big Data, 2019, pp. 2552–2559.
- [30] Y. Lu, J. Lian, S. Member, and M. Zhu, "Transactive Energy System Deployment Over Insecure Communication Links," IEEE Transactions on Automation Science and Engineering, vol. 21, no. 3, pp. 2677–2688, 2024, doi: 10.1109/TASE.2023.3267034.
- [31] I. Smart, "Privacy-Preserving Transactive Energy Management," IEEE Internet Things J, vol. 8, no. 14, pp. 11463–11475, 2021, doi: 10.1109/JIOT.2021.3051323.
- [32] Q. Yang and H. Wang, "Blockchain-Empowered Socially Optimal Transactive Energy System : Framework and Implementation," IEEE Trans Industr Inform, vol. 17, no. 5, pp. 3122–3132, 2021, doi: 10.1109/TII.2020.3027577.
- [33] P. Moura and R. Salles, "Federated Learning Enabled Prediction of Energy Consumption in Transactive Energy Communities," in 2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2022, pp. 0–4. doi: DOI: 10.1109/ISGT-Europe54678.2022.9960350.
- [34] A. Masoud, A. Haider, and K. Moghaddasi, "Self-learning adaptive power management scheme for energy-efficient IoT-MEC systems using soft actor-critic algorithm," Internet of Things, vol. 31, no. March, p. 101587, 2025, doi: 10.1016/j.iot.2025.101587.

- [35] Q. Wei, L. Wang, J. Lu, and F. Wang, "Discrete-Time Self-Learning Parallel Control," *IEEE Trans Syst Man Cybern Syst*, vol. 52, no. 1, pp. 192–204, 2022, doi: 10.1109/TSMC.2020.2995646.
- [36] N. Carbonare, T. Pflug, C. Bongs, and A. Wagner, "Design and implementation of an occupant-centered self-learning controller for decentralized residential ventilation systems," *Build Environ*, vol. 206, no. July, p. 108380, 2021, doi: 10.1016/j.buildenv.2021.108380.
- [37] Y. Zhou, "A dynamic self-learning grid-responsive strategy for battery sharing economy — multi-objective optimisation and posteriori multi-criteria decision making," *Energy*, vol. 266, no. November 2022, p. 126397, 2023, doi: 10.1016/j.energy.2022.126397.
- [38] S. Yin, Y. Li, Z. Feng, B. Sun, and H. Liang, "Distributed Intelligent Control Method Based on State Self-Learning and Its Application in Cascade Processes," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 10533–10545, 2025, doi: 10.1109/TASE.2024.3524472.
- [39] X. Huo, H. Zhang, Z. Wang, and C. Huang, "A Self-Learning Approach to Heterogeneous Multi-Robot Coalition Formation Under Uncertainty," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 3445–3457, 2025, doi: 10.1109/TASE.2024.3395283.
- [40] A. Grataloup, S. Jonas, and A. Meyer, "A review of federated learning in renewable energy applications : Potential , challenges , and future directions," *Energy and AI*, vol. 17, no. February, 2024.
- [41] M. A. Mohammed et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE J Biomed Health Inform*, vol. 27, no. 2, pp. 664–672, 2023, doi: 10.1109/JBHI.2022.3165945.
- [42] G. Cicceri, G. Tricoli, L. D. Agati, F. Longo, G. Merlino, and A. Puliafito, "A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities," *Sensors*, vol. 4549, pp. 1–25, 2023, doi: <https://doi.org/10.3390/s23094549>.
- [43] J. Jithish, B. Alangot, N. Mahalingam, and S. Member, "Distributed Anomaly Detection in Smart Grids : A Federated Learning-Based Approach," *IEEE Access*, vol. 11, no. December 2022, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.
- [44] S. I. Taheri, M. Davoodi, and M. H. Ali, "A modified modeling approach of virtual power plant via improved federated learning," *International Journal of Electrical Power and Energy Systems*, vol. 158, no. March, p. 109905, 2024, doi: 10.1016/j.ijepes.2024.109905.
- [45] H. Ying and F. Lin, "Self-Learning Fuzzy Automaton With Input and Output Fuzzy Sets for System Modelling," *IEEE Trans Emerg Top Comput Intell*, vol. 7, no. 2, pp. 500–512, 2023, doi: 10.1109/TETCI.2022.3192890.
- [46] H. Wu, Z. Xu, and S. Member, "Multi-Energy Load Forecasting in Integrated Energy Systems : A Spatial-Temporal Adaptive Personalized Federated Learning Approach," *IEEE Trans Industr Inform*, vol. 20, no. 10, pp. 12262–12274, 2024, doi: 10.1109/TII.2024.3417297.
- [47] X. Li et al., "Self-Learning Based Dependable Offloading Optimization in Semi-Trusted Vehicular Edge Computing and Networks," *IEEE Trans Veh Technol*, vol. 74, no. 5, pp. 8141–8157, 2025, doi: 10.1109/TVT.2025.3526696.
- [48] V. Michalakopoulos, L. Spyropoulos, L. Ilias, E. Sarma, V. Marinakis, and D. Askounis, "A comparative analysis of federated learning strategies for short-term photovoltaic power forecasting," *Energy Reports*, vol. 13, no. February, pp. 4223–4235, 2025, doi: 10.1016/j.egy.2025.03.043.
- [49] W. Liu, Q. He, Z. Li, and Y. Li, "Self-Learning Modeling in Possibilistic Model Checking," *IEEE Trans Emerg Top Comput Intell*, vol. 8, no. 1, pp. 264–278, 2024, doi: 10.1109/TETCI.2023.3300189.
- [50] H. Gupta, P. Agarwal, K. Gupta, S. Baliarsingh, and O. P. Vyas, "FedGrid : A Secure Framework with Federated Learning for Energy Optimization in the Smart Grid," *Energies (Basel)*, pp. 1–21, 2023.