Privacy-Aware Edge Intelligence in Smart Meters for Personal Energy Management

Namachivayam[1], Dr. Ramesh Kumar[2], *
[1]Mainefhi College of Engineering and Technology, Department of Computer Science and Engineering, Eritrea
[2]Government Women's Polytechnic, Coimbatore, India
Email: ramesh@gpcwcbe.edu.in

Abstract—Smart meters are becoming increasingly capable, transforming from passive meters into local decision nodes that can include demand forecasting, appliance-level inference, privacy-preserving learning, and demand-response support. This survey presents edge-intelligent smart meters for personal energy management, covering on-device inference, non-intrusive load monitoring (NILM), federated learning, privacy, local control, and meter–gateway–cloud coordination. The review is oriented toward meter-side deployment, and methods are evaluated based not only on prediction accuracy but also on memory footprint, inference latency, communication overhead, explainability, cybersecurity, adaptation, and user trust. The synthesis suggests that a layered architecture will be easiest to deploy in the near term, with trusted sensing and lightweight inference at the meter, heavier learning and user-friendly control at the gateway, and privacy-preserving aggregation and benchmarking in the cloud. Key open problems are continuous personalization under embedded constraints, secure federated NILM, and realistic meter-class benchmarking.

Keywords: Edge intelligence; Smart meters; NILM; Federated learning; Load forecasting; Privacy; HEMS.

I. Introduction

Smart meters are important digital assets in modern power systems. They were originally deployed for automated billing purposes but are currently used for electrical-variable measurement, outage and power-quality event recording, as well as demand response and grid operation. Meanwhile, customers' premises are becoming flexible small-scale grids with the addition of rooftop photovoltaic (PV) systems, batteries, heat pumps, electric vehicles (EVs), and controllable appliances in the home. Effective personal energy management thus starts with local and up-to-date information about energy use, appliance use, tariffs, comfort requirements, and privacy preferences. With conventional architectures, data from the meters are sent back to a utility or cloud-based platform, where they can be analyzed at a central location. While this is appropriate for billing and longer-term planning, it is not appropriate for faster, more privacy-sensitive, user-specific decisions.

Centralized processing increases communication traffic, reveals detailed load traces, and may result in delays in reacting to local changes. Forecasting, anomaly detection, NILM, and demand-side management applications benefit from smart-meter analytics, and edge computing places inference near data sources. These areas converge to create a motivation for edge-intelligent smart metering. This is relevant in the context of the increased need for flexibility in the home to facilitate the incorporation of renewables and decarbonization. Household load traces can show household occupancy, appliances used, daily activities, and lifestyle, all of which could pose privacy concerns if known. At the same time, embedded processors, small-scale neural networks, and federated learning make it increasingly possible

Journal of Intelligent Engineering and Informatics, Volume 1, Issue 1, Pages 83-93
Corresponding author. E-mail address: ramesh@gpcwcbe.edu.in
Received 16 July 2026; **revised** 25 August 2026; **accepted** 31 August 2026; **published** 11 September 2026.

to perform analytics on meters, gateways, or local home energy management system (HEMS) controllers.

The reviewed literature mostly considers smart-meter analytics [1] and HEMS [2] as separate topics; the same applies to edge intelligence [3]–[6] and NILM [7]–[9]. Other NILM approaches rely on cloud training or high-frequency data, which cannot be guaranteed in a typical advanced metering infrastructure (AMI) deployment. Hence, a meter-centric synthesis is required to determine how local intelligence can be hosted, coordinated, and secured for use in home energy management. This review provides a comprehensive overview of low-voltage smart meters, including local gateways and meter-attached controllers for energy-data processing inside customer premises in residential and small-commercial applications. It considers load forecasting, disaggregation of background appliances, anomaly detection, privacy-preserving learning, local demand response, and user recommendations. It does not cover wide-area transmission protection, substation automation, wholesale-market optimization, or cloud-only smart-grid analytics.

The primary issue is not which algorithm is the most accurate, but which methods can be effectively implemented in applications with memory, latency, communication, privacy, cybersecurity, and user-acceptance constraints. The literature is therefore structured by technical function, deployment layer, learning mode, and evidence maturity rather than chronologically. The taxonomy includes meter hardware, communication evolution, cloud-edge analytics, NILM and appliance inference, personal load forecasting, federated learning, local HEMS and demand response, as well as cybersecurity. The proposed architecture is illustrated in Fig. 1, technical classes are summarized in Table 1, and the practical evaluation criteria are listed in Table 2. This architecture is a step toward the shift from metering and data collection to embedded learning, privacy, and local control.

One of the major challenges is privacy-aware continual personalization under embedded constraints. Homes constantly change through the introduction of new and replacement appliances, new residents, new EVs, and updated tariff regulations. Static cloud models may become outdated, and drift may occur with local adaptation, along with risks of cyberattacks, fairness problems, and a lack of local control. Smart meters of the future will thus need explainable, secure, and personalized intelligence, reducing the need to export raw sensitive traces. The review provides a new meter-centric system boundary, a taxonomy from the deployment perspective, a practical readiness comparison, and research directions for edge-intelligent smart meters.

II. Survey Boundary and Novel Challenge

Edge-intelligent smart metering is located at the customer-premise edge between household resources and the utility platform. This boundary includes smart meters, AMI, local energy gateways, HEMS controllers, rooftop PV inverters, batteries, EV chargers, and interfaces with utility services. The functional scope involves personal load forecasting, appliance forecasting and inference, billing-related feedback, local demand response, and user-specific scheduling. These data sources include active energy, reactive energy, voltage, current, time/date stamps, event logs, tariff signals, and, if locally available, proxy weather or occupancy data.

Topics that are not included are transmission-grid state estimation, phasor measurement unit analytics, wide-area protection, wholesale-market clearing, and general cloud-only deployments of smart-grid artificial intelligence that are not directly applicable to meter- or home-side deployments. The boundary highlights that decisions must be made under constraints involving privacy, low latency, local adaptation, and limited embedded resources, without further centralized data aggregation. This topic brings together smart-meter analytics, edge computing, NILM, federated learning, and household energy optimization, for which evidence is found in various research areas. The major challenge is how to ensure that smart meters continuously learn from new households without sacrificing privacy while dealing with embedded-computing constraints or risking unsafe operation. This challenge is called privacy-aware continual personalization under embedded constraints.

III. Meter-Side Intelligence Architecture and Mathematical View

A practical architecture places computation according to latency, privacy, and resource needs. Heavyweight model aggregation and fleet-level benchmarking can continue using the utility's cloud resources, with fast, privacy-sensitive inference taking place on the meter or gateway. Functionality, comfort aspects, and user-facing appliance settings should not be obscured and should not be irreversible. As depicted in Fig. 1, the architecture has four key layers: household flexible resources, the AMI smart meter, the edge gateway, and the utility cloud/distribution system operator (DSO). Supporting functions are on-device intelligence, federated/privacy-preserving learning, and local system services. For household i at time t, the meter observation vector is defined in (1).

$$x_i(t) = [P_i(t), Q_i(t), V_i(t), I_i(t), \tau(t), \pi(t)] \quad (1)$$

In (1), i denotes the household index and t denotes the time index; P_i and Q_i are the active and reactive power, V_i is the voltage, I_i is the current, $\tau(t)$ is the time context, and $\pi(t)$ is the local tariff or control signal. As summarized in (2), a local edge model maps recent observations to next-step demand, appliance states, or the anomaly score.

$$\hat{y}_i(t+h) = f\theta_i(x_i(t-L{:}t), z_i) \quad (2)$$

In (2), $\hat{y}_i(t+h)$ is the predicted output at forecast horizon h, $f\theta_i$ is the local model parameterized by θ_i, L is the look-back window, and z_i is the local context vector. When available, the local context includes contracted power, appliance metadata, and user preferences. The local controller can manage energy cost, comfort, peak demand, and privacy risk through the objective in (3) for personal energy management.

$$\min_{u_i} \; \Sigma_{t=1}^{T} [\pi(t)P_i(t) + \lambda_c C_i(t) + \lambda_p \max(0, P_i(t) - P_i^{lim}) + \lambda_r R_i(t)] \quad (3)$$

In (3), u_i denotes the control action, $C_i(t)$ is a comfort deviation, P_i^{lim} is the local peak limit, and $R_i(t)$ is a privacy or risk penalty. T is the optimization horizon, and λc, λp, and λr are weighting coefficients for the comfort, peak-limit, and privacy/risk terms, respectively. If several households upload a copy of the same model without access to raw traces, federated averaging of the model updates gives the global model specified in (4).

$$\theta^{k+1} = \Sigma_{i=1}^{N} [n_i / \Sigma_{j=1}^{N} n_j] \, \theta_i^k \quad (4)$$

In (4), θ^{k+1} is the updated global model at aggregation round k+1, θ_i^k is the local model from household i at round k, n_i is the number of local samples at household i, and N is the number of participating households. Equations (1)–(4) connect the survey architecture mathematically: meter measurements are used to create local features from which edge models are estimated to provide useful states; a controller is used to make household decisions; and federated aggregation of the edge models can be used to enhance shared models without centralizing raw meter data.

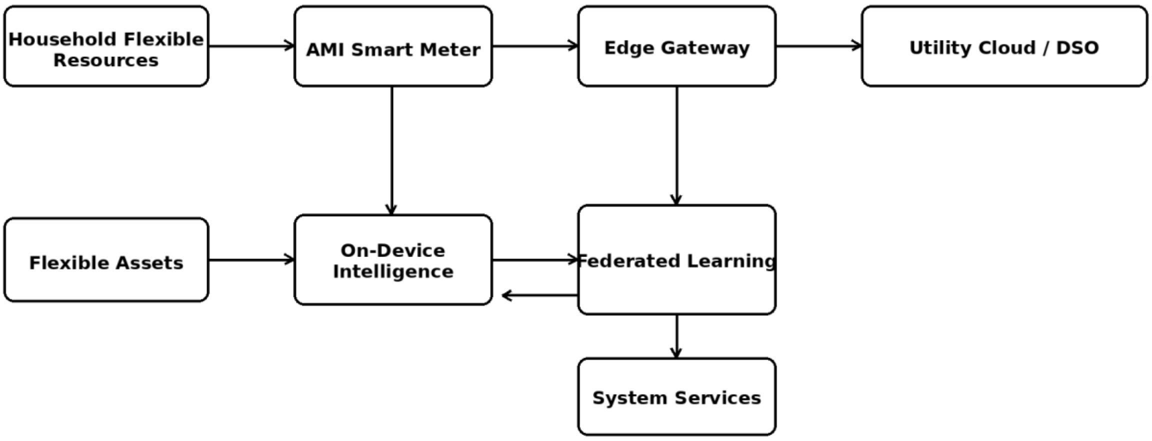

Figure 1. Architecture of privacy-aware edge intelligence for smart-meter energy management.

IV. Classification of Existing Approaches

The literature is organized into seven connected classes that trace the progression from metering hardware and communication to embedded learning, privacy, and user control. Table 1 summarizes each class, its main purpose, representative references, and deployment readiness.

Table 1. Taxonomy of edge-intelligent smart meter research

A. Meter Hardware and Communication Evolution

Class	Main idea	Representative references	Implementation readiness
Meter hardware and AMI evolution	Low-cost meters, sensing channels, billing accuracy, event logs, and communication interfaces.	[1], [10]	High, because utilities already deploy AMI, but firmware openness varies.
Cloud-edge smart-meter analytics	Partitioning inference between meter, gateway, and cloud; latency-aware processing.	[3]–[5]	Medium to high; gateway deployment is easier than replacing meters.
NILM and appliance inference	Appliance disaggregation, event detection, EV charging recognition, and usage feedback.	[7]–[9], [11]–[13]	Medium; accuracy is promising, but low-rate meter data limits appliance separation.
Personal load forecasting	Short-term household forecasting, personalized models, heterogeneity-aware learning.	[14]–[18]	Medium; model drift and household diversity remain major issues.
Federated and privacy-preserving learning	Local training, secure aggregation, split learning, and privacy-preserving forecasting.	[16], [19]–[23]	Medium; attractive for privacy, but communication and robustness need testing.
Local HEMS and demand response	Appliance scheduling, storage control, tariff response, comfort-aware optimization.	[2], [24]–[25]	High for rule-based control; medium for autonomous learning-based control.
Cybersecurity and trust	Meter data integrity, intrusion detection, firmware protection, and user consent.	[26]–[28]	Medium; security is widely recognized but rarely integrated with energy objectives.

Early work on smart meters focused on measurement accuracy, communication reliability, and AMI deployment. Today's meter is capable of measuring electrical state variables and events across a wide range of sampling rates, depending on deployment. Practical limitations still include measurement quality, communication limitations, interoperability, and firmware accessibility. Latency, bandwidth, reliability, and update frequency are affected by power-line communication (PLC), cellular communication, radio-frequency (RF) mesh, Wi-Fi, and low-power wide-area networks (LPWANs) [26]–[27]. Edge algorithms therefore need to be designed for the actual meter population and its installed data rates and communication capabilities.

B. Cloud-Edge Architectures

Edge computing places inference closer to the data source, which decreases dependence on central processing [3]. Cloud-edge partitioning for latency- and privacy-sensitive applications is identified by smart-grid studies [4]–[6]. In smart-meter systems, basic filtering, event detection, and feature extraction can be performed on the meter, whereas more complex NILM or forecasting models can be performed on a home gateway. The cloud may also handle model updates, access performance data across the fleet, and perform fleet-level services. This is a more realistic partitioning method than placing a large neural network (NN) on every meter.

C. Edge-Based Non-Intrusive Load Monitoring

With NILM, the same set of aggregate meter measurements is preserved, and software derives parameters of appliance activity. These have been achieved using spectral clustering [11], comprehensive methods based on neural networks and data [7], data augmentation [8], low-sampling-rate NILM [9], EV-charging detection [12], and implementation of low-cost meters [13]. Many studies, however, are based on high-frequency laboratory data, balanced appliance classes, or online training. In practice, low-rate traces, noise, and non-stationarity need to be addressed at the meter side during deployment. Hence, a practical architecture combines simple event features with a small local model and optional gateway or cloud retraining.

D. Personal Load Forecasting and Heterogeneity

Forecasting household load is more complicated than forecasting feeder load because household loads are highly variable. For smart-meter loads, distributed recurrent forecasting [14] or online adaptive recurrent models [15] can be developed, and personalized federated learning takes advantage of load patterns without centralizing raw data [16]. Moreover, heterogeneity- and metadata-assisted forecasting can further improve personalization [17], [18]. A deployment evaluation should therefore consider not only accuracy but also stability under appliance changes, occupancy, weather, and tariffs.

E. Federated and Privacy-Preserving Learning

Federated learning has the advantage of keeping raw household load traces local and transporting only model parameters or model gradients across locations. The possibility of smart-meter forecasting, privacy-preserving aggregation, personalized federated learning, and secure learning frameworks has been explored [16], [19]–[23]. However, federated learning does not eliminate all exposure risks: gradients might accidentally reveal information, malicious clients might submit poisoned updates, and unreliable communications might disrupt training. Secure aggregation, anomaly screening, robust client selection, configurable differential privacy, and rollback capabilities are therefore necessary for practical deployments.

F. Household Energy Management and Local Decision Making

HEMS translates data and analytics into energy choices for the user. Tariff response, renewable integration, battery control, appliance scheduling, voltage support, peak shaving, and demand response are examples of existing work. User acceptance is one of the main constraints on operation in personal energy management. Recommendations and automated actions need to be understandable, reversible, and comfort-aware, with clear rules for switching automated actions on and off and greater emphasis on comfort rather than only grid goals.

G. Security, Reliability, and Trust in Intelligent Systems

Edge intelligence expands the attack surface by adding local models, firmware, communication links, and user interfaces. Common interoperability, privacy, and security issues are identified as important deployment problems in AMI and Internet of Things (IoT) smart-grid studies [26]–[28]. Forecast errors primarily affect efficiency, while billing, comfort, or safety may be affected by malicious control commands. Therefore, trust requires secure boot, signed model and firmware updates, and tamper detection, together with encrypted communication, access control, and transparent user consent.

V. Evaluation Criteria

Predictive accuracy alone is insufficient for meter-side intelligence. If a slightly less accurate model uses less memory and communication, is faster, and makes more stable and/or explainable decisions, then that model may be preferable. Thus, practical studies should report the multidimensional criteria summarized in Table 2.

Table 2. Evaluation criteria for practical edge-intelligent smart meters

Criterion	Typical measures	Why it matters
Forecasting or NILM accuracy	MAE, RMSE, F1-score, event recall, appliance-level precision.	Required but not sufficient for deployment.
Embedded feasibility	Processor type, random-access memory (RAM), flash, inference latency, quantization, energy use.	Essential for meter- and gateway-class deployment.
Communication cost	Bytes per round, reporting interval, failed packets, network dependency.	Important for AMI bandwidth and federated learning.
Privacy and security	Raw data exposure, secure aggregation, attack testing, differential privacy budget.	Often claimed, but not always measured.
Adaptation and drift	Performance before and after appliance change, occupancy shift, or tariff change.	Central to continual personalization.
User and control quality	Cost savings, peak reduction, comfort violations, override rate, explainability.	Needed for individual energy management.

There must be at least three tiers of reporting: algorithm performance, embedded resource use, and household impact. Forecasting studies should report root mean square error (RMSE) and mean absolute error (MAE), along with inference latency, memory consumed by the meter-class or gateway processor, and tariff benefit. The success of NILM should be expressed in terms of F1-score, precision, and recall and validated at realistic 5- or 15-minute AMI intervals, if applicable. Measurements of accuracy, communication rounds and payload, privacy assumptions, client heterogeneity, and robustness to abnormal or malicious clients should be reported in federated-learning studies.

VI. Detailed Synthesis of Deployment Pathways

The review of the literature indicates the following three main deployment pathways. The first, “meter-plus-gateway intelligence,” leaves certified sensing, billing, and basic feedback functions on the meter, with a separate gateway handling forecasting, NILM, model updates, and user-facing analytics. This pathway is ideal for near-term deployment because it avoids replacing meter processors and allows flexible software upgrades for meter systems comprising routers, energy hubs, or inverter gateways in homes. Its biggest challenges are gateway ownership, interoperability, patch management, and responsibility for cybersecurity. The second is embedded-meter inference, in which small models are used to detect anomalies, extract events, or coarsely classify load. This enables low latency, low communication cost, and high local data retention, with deployment challenges due to processor, memory, firmware-safety, and certification constraints. Embedded learning functions must be deterministic, secure, auditable, and fail-safe because billing meters are regulated infrastructure.

Thus, during early deployment, low-risk advisory activities will be more important than hands-on control of appliances. The third pathway is federated community learning, in which local models are trained or fine-tuned and their protected updates are sent to a utility or aggregator. This can support personalization in heterogeneous households without centralized collection of raw traces, but it requires secure aggregation, client selection, poisoning detection, update compression, privacy accounting, and communication management. Without these safeguards, however, federated learning can leak information about raw-data components, such as through gradients or model behavior. The three pathways can coexist and become integrated in a practical system. The meter handles measurements and lightweight features, while heavier model-learning and user-facing control functions are on the gateway, and the cloud handles model versioning, privacy-preserving aggregation, fleet-level benchmarking, and rollback. This multilevel separation also enhances fault tolerance so that local recommendations can continue during cloud outages and certified metering and basic monitoring can continue without gateway availability.

The maturity level of evidence is uneven. Numerous forecasting studies exhibit high accuracy but do not measure meter latency or memory. Many investigations use sampling rates higher than those of a typical AMI deployment. Federated-learning research tends to neglect communication payload, adversarial clients, and gradient leakage, and HEMS research usually considers controllable appliances and ideal user behavior. Future research should include the complete deployment chain: the dataset and sampling rate, handling of missing data, model size, processor and memory utilization, inference latency, communication overhead, privacy threat model, robustness, and household-level benefit. Both implementation readiness and criteria such as accuracy or cost savings are scientifically important. The practical deployment pathways are summarized in Table 3.

Table 3. Practical deployment pathways for edge-intelligent smart meters

Pathway	**Architecture**	**Best use**	**Main barrier**
Meter-plus-gateway	Gateway hosts learning; meter keeps certified measurement.	Near-term deployment, flexible updates, user dashboard.	Gateway ownership, security patching, interoperability.
Embedded meter inference	Compact model runs inside the meter firmware.	Low latency, low bandwidth, strong privacy.	Certification, memory limits, firmware safety.
Federated community learning	Many homes train locally and share protected updates.	Personalization without raw-data pooling.	Gradient leakage, poisoning, communication rounds.
Cloud-assisted benchmarking	Cloud manages model registry and aggregate evaluation.	Fleet-wide quality control and model rollback.	Must avoid raw-trace centralization.

VII. Critical Analysis

Implementation realism is compared for the major method families in Table 4. Currently, rule-based HEMS and lightweight local forecasting are among the most deployable approaches because they can operate on existing gateways with limited training data and are relatively easy to explain and certify. These approaches can be applied to main load types such as heating, cooling, cooking, and EV charging; detecting events and distinguishing them from one another is also possible but is challenging for other load categories, such as small appliances, when using low-rate meter data. Federated forecasting has potential for privacy and personalization and applies more generally at the gateway than in the meter because privacy-preserving training requires additional memory, communication, and update management.

Secure federated NILM is relatively undeveloped because of the lack of appliance labels, the strong non-IID nature of household data (where IID denotes independent and identically distributed), and the risk of privacy leakage or poisoning. Many of these studies are simulation-based and fail to accurately include aspects of comfort constraints, cyber risk, and failure handling, making deep reinforcement learning for autonomous household control the least deployment-ready family. Learning-based control components should be limited in real deployments through rules, safety filters, or user approval as necessary. A hybrid architecture, with lightweight feature extraction at the meter, adaptive learning at the gateway, privacy-preserving aggregation across households, and transparent user control, is therefore the strongest design concept for the near term.

Table 4. Implementation realism of major edge-intelligent smart-meter methods

Method family	Typical use	Realism level	Main assessment
Rule-based HEMS	Scheduling, tariff response, peak limits.	Realistic now	Simple, explainable, but less adaptive.
Lightweight forecasting	Long short-term memory (LSTM)/gated recurrent unit (GRU), temporal convolutional neural network (CNN), online learning	Realistic at gateway; possible in meters after compression	Useful for tariffs and peak control; drift handling needed.
NILM at edge	Event detection, compact CNN/recurrent neural network (RNN), clustering	Partly realistic	Good for major loads; weak for low-rate small-appliance separation.
Federated forecasting	Federated Averaging (FedAvg), clustered federated learning (FL), personalized FL	Near-term realistic at gateway	Privacy-friendly, but communication and poisoning risks remain.
Secure federated NILM	FL with secure aggregation or privacy noise	Mostly experimental	Label scarcity and gradient leakage must be solved.
Deep reinforcement learning control	Autonomous appliance or battery scheduling	Mostly simulation-based	Needs safety constraints, comfort guarantees, and user override.

VIII. Open Challenges and Future Directions

Personalization is an ongoing challenge, particularly without sacrificing privacy. Household models need to be flexible enough to accommodate appliance replacement, occupancy changes, new EVs, and tariff changes without exporting raw traces. This involves the ability to detect drift, selectively update the local part of the system, secure the federation, and provide compact adaptation mechanisms. Benchmark realism is also important: many publicly released datasets are labeled, appliance-dense, and high-frequency, whereas AMI data are low-rate, noisy, unlabeled, and incomplete. Meter-class processor constraints, limited memory, packet loss, cyberattacks, and user-override behavior should all be considered in future evaluations.

Security and control should be considered together, as a failure of learning-based control or logic can affect billing, comfort, and safety. Explainability must also be considered in the context of the user: recommendations such as rescheduling EV charging must convey expected costs, comfort impacts, and emissions in terms comprehensible to the household. Table 5 provides an overview of the main research gaps, research directions, and evaluation metrics. Future work should move from offline accuracy comparisons to meter-gateway prototypes that demonstrate reproducible household benefits under real AMI constraints.

Table 5. Open research gaps and actionable future directions

Gap	Why it remains open	Recommended direction	Suggested metric
Continual personalization	Models become stale when appliances or occupancy change.	Local drift detection and selective federated update.	Accuracy before/after change; update cost; privacy leakage.

Gap	Why it remains open	Recommended direction	Suggested metric
Low-rate NILM	Many smart meters provide minute-level or longer intervals.	Coarse appliance classes and event-enhanced compact models.	Class-level F1-score under real AMI intervals.
Secure learning	Federated gradients and firmware updates can be attacked.	Secure aggregation, signed updates, anomaly screening.	Attack success rate; recovery time; billing integrity.
User-centered control	Automated control may reduce comfort or trust.	Explainable recommendations and easy override.	Cost savings; comfort violations; override rate.
Embedded benchmarking	Many papers omit processor, memory, and communication limits.	Open meter-gateway testbeds and model compression reports.	Latency, RAM, flash, bytes per learning round.

IX. Conclusion

Edge-intelligent smart meters can be seen as nodes for local sensing, inference, and coordination for personal energy management. The reviewed evidence suggests a three-tiered meter-gateway-cloud design in which meters are responsible for trusted sensing and deployed low-level inference, gateways are used for adaptive forecasting, NILM, and user interactions with the system, and privacy-preserving aggregation and fleet management are performed by cloud- or utility-side platforms. The most plausible near-term deployment includes rule-guided HEMS, lightweight forecasting models, coarse NILM, and federated learning on the gateway. Secure NILM and fully autonomous learning-based control are less developed under real AMI constraints. The main research focus is continual personalization, evaluated in terms of privacy, accuracy, embedded resource use, communication cost, cybersecurity, adaptability, explainability, and user impact.

References

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3125-3148, May 2019, doi: 10.1109/TSG.2018.2818167.

[2] B. Zhou, W. Li, K. W. Chan, Y. Cao, Y. Kuang, X. Liu, and X. Wang, "Smart Home Energy Management Systems: Concept, Configurations, and Scheduling Strategies," Renewable and Sustainable Energy Reviews, vol. 61, pp. 30-40, Aug. 2016, doi: 10.1016/j.rser.2016.03.047.

[3] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[4] H. B. Gooi, J. Zheng, S. Chen, B. Lu, and T. Zhang, "Edge Intelligence for Smart Grid: A Survey on Concepts, Architectures and Applications," CSEE Journal of Power and Energy Systems, 2022.

[5] Q. T. Minh, N. Nguyen, T. H. Nguyen, and E. N. Huh, "Edge Computing for Smart Grid: A Comprehensive Survey," Energies, vol. 15, no. 17, 6140, 2022.

[6] A. N. Akpolat, E. Dursun, and S. Kuzlu, "Edge Intelligence in Smart Grids: A Review of Architectures, Applications, and Challenges," Journal of Sensor and Actuator Networks, vol. 11, no. 3, 47, 2022.

[7] M. Rafiq, H. Zhang, H. Li, and M. K. Ochani, "A Comprehensive Review of Non-Intrusive Load Monitoring: Methods, Datasets, and Challenges," Energy and Buildings, vol. 305, 113890, 2024.

[8] M. Rafiq, G. Hafeez, I. Khan, F. A. Khan, and A. Shafiq, "Data Augmentation for Non-Intrusive Load Monitoring," IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5142-5154, Nov. 2021.

[9] A. Manca, G. Graditi, M. G. Ippolito, and E. R. Sanseverino, "Non-Intrusive Load Monitoring at Low Sampling Rate: A Review," Computer Applications in Engineering Education, 2022.
[10] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy Meters Evolution in Smart Grids: A Review," Journal of Cleaner Production, vol. 217, pp. 702-715, Apr. 2019, doi: 10.1016/j.jclepro.2019.01.229.
[11] Z. Ghaffar, M. K. Hanif, and S. H. Ahmed, "Non-Intrusive Load Monitoring Using Spectral Clustering and Smart Meter Data," Sensors, vol. 22, no. 11, 4036, 2022.
[12] J. Yang, Y. Li, and H. Zhang, "Non-Intrusive Electric Vehicle Charging Detection Using Smart Meter Measurements," IEEE Transactions on Consumer Electronics, 2024.
[13] L. Nardello, M. Rossi, and D. Brunelli, "A Low-Cost Non-Intrusive Load Monitoring System for Smart Meters," in Proc. IEEE PES Innovative Smart Grid Technologies Europe, Torino, Italy, 2017.
[14] M. N. Fekri, K. Grolinger, and S. Mir, "Distributed Load Forecasting Using Smart Meter Data: Federated Learning with Recurrent Neural Networks," International Journal of Electrical Power & Energy Systems, vol. 137, 107669, May 2022, doi: 10.1016/j.ijepes.2021.107669.
[15] M. N. Fekri, K. Grolinger, and S. Mir, "An Online Adaptive Recurrent Neural Network for Load Forecasting of Individual Smart Meters," International Journal of Electrical Power & Energy Systems, vol. 152, 109285, Nov. 2023.
[16] Z. Cui, R. Ke, Z. Pu, and Y. Wang, "Personalized Federated Learning for Smart Meter Data-Based Load Forecasting," CSEE Journal of Power and Energy Systems, 2022.
[17] Y. Wang, N. Zhang, Q. Chen, D. S. Kirschen, P. Li, and Q. Xia, "Data-Driven Probabilistic Net Load Forecasting With High Penetration of Behind-the-Meter PV," IEEE Transactions on Power Systems, vol. 33, no. 3, pp. 3255-3264, May 2018, doi: 10.1109/TPWRS.2017.2762599.
[18] H. Qu, K. Li, and T. Zhang, "Heterogeneous Residential Load Forecasting Based on Clustering and Deep Learning," Big Data Mining and Analytics, vol. 5, no. 2, pp. 135-146, 2022.
[19] A. Taïk and S. Cherkaoui, "Electrical Load Forecasting Using Edge Computing and Federated Learning," in Proc. IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148937.
[20] N. Hudson, J. S. Liu, and A. R. Hota, "Federated Learning for Privacy-Preserving Short-Term Residential Load Forecasting," in Proc. International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 2021, pp. 1-9.
[21] Y. Su, T. T. Kim, and H. V. Poor, "Privacy-Preserving Federated Learning for Residential Short-Term Load Forecasting," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7629-7639, Nov. 2022.
[22] X. Wang, Y. Wang, and D. Shi, "A Privacy-Preserving Distributed Learning Scheme for Smart Meter Data Analytics," IEEE Transactions on Smart Grid, 2021.
[23] M. Husnoo, A. Anwar, Z. Tari, and A. Mahmood, "A Secure Federated Learning Framework for Smart Grid Load Forecasting," IEEE Transactions on Smart Grid, 2023.
[24] M. Raza, N. Javaid, A. Gumaei, and M. Al-Rakhami, "Business Intelligence for Smart Energy Management: A Review," IEEE Access, vol. 11, pp. 119316-119338, 2023.
[25] Z. Chen, A. M. Amani, X. Yu, and M. Jalili, "Control and Optimisation of Power Grids Using Smart Meter Data: A Review," Sensors, vol. 23, no. 4, 2118, 2023, doi: 10.3390/s23042118.

[26] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy Preservation in Smart Grid: A Survey," Computer Science Review, vol. 43, 100424, Feb. 2022.
[27] S. M. Abu Adnan Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-Enabled Smart Energy Grid: Applications and Challenges," IEEE Access, vol. 9, pp. 50961-50981, 2021, doi: 10.1109/ACCESS.2021.3067331.
[28] S. Kirmani, M. Jamil, I. Akhtar, and M. Rizwan, "IoT Applications in Smart Grid: A Survey," Sustainability, vol. 15, no. 1, 717, 2023.
[29] Y. Mehmood, N. Ahmad, and A. Alrajeh, "Edge Computing for Internet of Things Based Smart Grid: A Comprehensive Survey," Wireless Communications and Mobile Computing, vol. 2021, 5524025, 2021.
[30] M. Kolosov, P. Zancanaro, and T. Ahmed, "High-Frequency Smart Meter Data for Edge-Aware Energy Analytics," Sensors, vol. 25, no. 17, 5280, 2025.