

Fostering Energy Sustainability Through Trust

Privacy-Aware Smart Metering Mechanism for Demand-Side Resources in Power Systems

By Jiabao Li^{1b}, Hongxun Hui^{1b}, and Yonghua Song^{1b}



Jiabao Li (li.jiabao@connect.um.edu.mo), Hongxun Hui (hongxunhui@um.edu.mo), and Yonghua Song (yhsong@um.edu.mo) are with the State Key Laboratory of Internet of Things for Smart City and the Department of Electrical and Computer Engineering, University of Macau, Macao 999078, China. Hongxun Hui is the corresponding author.

Digital Object Identifier 10.1109/ESM.2026.3717894
Date of current version: 28 October 2026

THE RAPID ADVANCEMENT OF INFORMATION and communication technologies has accelerated the intelligent transition of power systems. A key enabling component of this transition is advanced metering infrastructure (AMI), which integrates smart meters (SMs), communication networks, and data management platforms to support bidirectional information exchange between utilities and electricity consumers. SMs are capable of measuring electricity consumption at high temporal resolution and transmitting the collected data to utilities in near real time. The availability of such high-frequency smart metering data significantly enhances the observability of demand-side behaviors, enabling utilities and distribution system operators (DSOs) to perform more accurate load monitoring, demand forecasting, and operational planning. Moreover, high-frequency smart metering data support the implementation of demand response (DR) programs. By enabling more efficient utilization of demand-side resources and facilitating the integration of distributed and renewable energy resources, AMI has become critical digital infrastructure for achieving reliable and sustainable operation of modern power systems.

Despite these operational benefits, the large-scale collection of high-frequency smart metering data raises significant concerns regarding consumer privacy. Previous studies have shown that techniques such as nonintrusive load monitoring (NILM) can analyze SM measurements to infer appliance-level electricity usage and household activities. Consequently, sensitive information, such as occupancy patterns, daily routines, and appliance operating schedules, can be inferred from smart metering data. These privacy risks are further amplified by the widespread deployment of SMs and the centralized collection, transmission, and storage of smart metering data within AMI systems. Unauthorized access, data leakage, or improper use of such data may expose highly sensitive details about the private lives of consumers.

Beyond individual privacy risks, insufficient protection of smart metering data may also undermine the long-term development of smart grids. If consumers perceive that their smart metering data may be collected, analyzed, or shared without adequate protection, they may resist the installation or operation of SMs. In several countries, such concerns have already triggered public opposition, regulatory debates, and the introduction of customer opt-out policies that allow consumers to restrict the collection or

transmission of smart metering data. However, large-scale opt-out decisions or strict limitations on high-frequency smart metering data collection can significantly reduce the availability of high-frequency smart metering data required for DR, dynamic pricing, and advanced grid operation. The resulting reduction in data availability may weaken the ability of utilities and DSOs to perform accurate load forecasting, maintain grid stability, and effectively integrate renewable energy resources. Consequently, unresolved privacy concerns not only erode consumer trust but also hinder the establishment of a secure and trustworthy energy data infrastructure. Such an infrastructure is essential for leveraging demand-side resources to support energy sustainability in smart grids.

Addressing the inherent tension between strong privacy protection and data availability remains a critical challenge. This article proposes a privacy-aware smart metering mechanism to enable secure and controlled acquisition of demand-side resources. Guided by the principle of data minimization, the proposed mechanism limits smart metering data collection to the minimum level necessary to support essential smart grid services. Specifically, a privacy-preserving sampling boundary model is developed to determine the maximum admissible sampling interval that preserves the effectiveness of demand-side management. By appropriately adjusting the sampling interval, the proposed model reduces the risk of privacy leakage while maintaining the operational value of smart metering data. To enforce these sampling boundaries in a secure and verifiable manner, a cryptographic downsampling method based on timed-release encryption (TRE) is further introduced to regulate the data sampling frequency of SMs. In addition, the proposed mechanism explicitly incorporates heterogeneous consumer privacy preferences, enabling consumers to actively participate in the protection of their smart metering data. Through this integrated design, the proposed mechanism enables privacy-aware collection of smart metering data while ensuring the data availability required for DR, renewable energy integration, and advanced grid operation. Consequently, the proposed privacy-aware smart metering mechanism provides a systematic framework for balancing privacy protection and data utility, contributing to the development of secure energy data infrastructures that support energy sustainability in smart grids.

Related Work

Extensive research has investigated privacy protection approaches for high-frequency smart metering data in AMI systems. From a measurement perspective, privacy protection in AMI systems can be characterized by three key dimensions: sampling frequency, attribution, and exactness. Sampling frequency determines the temporal resolution of smart metering data, attribution concerns whether metering data can be linked to specific consumers, and exactness refers to the precision of the reported measurements. Existing studies have proposed different privacy protection approaches along these three dimensions.

Sampling Frequency Protection

Reducing the sampling frequency of SMs is one of the most direct and effective approaches for mitigating privacy risks in AMI systems. Lower temporal resolution reduces the amount of behavioral information that can be inferred from smart metering data. Cardenas et al. formulated privacy-preserving DR as a discrete-time control problem and derived the maximum allowable sampling interval that minimizes consumer data exposure while preserving the effectiveness of direct load control programs. Zhang et al. proposed a two-channel smart metering framework that employs data downsampling to mask sensitive behavioral patterns. By introducing an artificial intelligence-based adversary equipped with deep learning models, their study quantified the privacy boundaries associated with different sampling resolutions and identified the downsampling rates required to prevent appliance detectability through NILM.

Although reducing the sampling frequency can effectively limit behavioral information leakage, excessively coarse sampling intervals may reduce the availability of high-frequency smart metering data required for advanced smart grid operations.

Attribution Protection

Another line of research focuses on preventing the association between smart metering data and specific consumers. These approaches typically rely on anonymization, pseudonymization, or spatial aggregation mechanisms. Afrin and Mishra proposed an anonymized authentication framework that assigns separate pseudonyms to low-frequency billing data and high-frequency operational data, thereby preventing service providers from linking fine-grained electricity consumption patterns to specific consumers. In

the context of distributed energy resource management systems, Alsaid et al. applied a k -anonymity approach combined with a dynamically generated generalization hierarchy to conceal personally identifiable information during grid communications. Adewole and Torra further proposed DFTMicroagg, which integrates the discrete Fourier transform with microaggregation to anonymize high-dimensional time-series smart metering data while preserving data utility for tasks such as load forecasting.

Despite these theoretical guarantees, attribution protection approaches face several practical limitations. Anonymized datasets may still be vulnerable to reidentification attacks using external background knowledge or appliance load signatures extracted via NILM. Moreover, these approaches primarily focus on anonymizing data after collection, rather than limiting the amount of sensitive information generated during the data acquisition process.

Data Exactness Protection

A third category of research protects consumer privacy by reducing the exactness of smart metering data. Representative approaches include load shaping and differential privacy mechanisms. Load shaping modifies observable load profiles by using local energy storage. Kalogridis et al. proposed a load signature moderator that combines grid power with battery storage to obscure appliance load signatures. McLaughlin et al. introduced nonintrusive load leveling to maintain a constant load profile observed by the SM, thereby masking appliance switching events. Li et al. later developed a deep reinforcement learning-based approach to optimize battery operation against NILM attacks. Algorithmic approaches based on differential privacy protect smart metering data by injecting noise into meter readings. Barbosa et al. proposed a lightweight Laplacian noise mechanism to achieve ϵ -differential privacy at the SM level. Wang et al. further analyzed the relationship between the differential privacy budget and NILM inference accuracy within a compressive sensing framework.

However, both load shaping and differential privacy approaches inevitably degrade the exactness of smart metering data. Battery-based methods are inherently constrained by storage capacity and cannot completely hide appliance signatures, particularly during battery recharge periods. Differential privacy approaches, while providing rigorous mathematical privacy guarantees, may significantly reduce measurement

fidelity when applied to high-resolution time-series data. This degradation may conflict with applications requiring accurate and auditable measurements, such as electricity billing.

Research Gaps

The above studies provide important technical foundations for protecting consumer privacy in AMI systems. Nevertheless, several fundamental challenges remain.

First, many existing privacy protection approaches treat privacy protection and data utility as a zero-sum tradeoff, where stronger privacy guarantees are achieved at the cost of reduced availability or accuracy of smart metering data. However, AMI systems serve two fundamental functions: 1) metering for billing, which requires accurate and auditable measurements for individual consumers, and 2) metering for grid operations, which requires high-frequency metering data to support load monitoring, DR, and renewable energy integration. Overly aggressive privacy protection mechanisms may significantly degrade data quality, thereby undermining grid operational functions or compromising billing accountability. Designing privacy-aware smart metering mechanisms that preserve both data utility for grid operations and measurement integrity for billing therefore remains a critical challenge.

Second, most existing approaches implicitly assume homogeneous consumer privacy preferences. In practice, electricity consumers exhibit diverse attitudes toward privacy protection and data sharing. While some consumers prefer strong privacy protection with minimal data disclosure, others may be willing to share more detailed data to support grid operations or obtain potential incentives. Ignoring such heterogeneity may lead to rigid privacy protection mechanisms that fail to accommodate the diverse expectations of real-world smart grid participants. Effective privacy protection should therefore adopt a user-centric design, enabling consumers to participate in privacy decisions and control the collection and use of their smart metering data.

These limitations highlight the need for privacy-aware smart metering mechanisms for demand-side resources that can balance privacy protection, data utility, and heterogeneous consumer privacy preferences.

Contributions

To address the limitations of existing privacy protection approaches for smart metering data, this article proposes a privacy-aware smart meter-

ing mechanism for demand-side resources. The main contributions of this article are summarized as follows:

- A privacy-preserving sampling boundary model is proposed to determine the maximum admissible sampling interval that preserves the effectiveness of demand-side management while reducing the risk of privacy leakage.
- A cryptographic downsampling method based on TRE is developed to enforce the sampling boundaries in a secure and verifiable manner. It cryptographically limits real-time behavioral exposure against inference attacks while fully preserving the lossless exactness of high-frequency metering data.
- The privacy-aware smart metering mechanism is designed to enable controlled acquisition of demand-side resources while explicitly incorporating heterogeneous consumer privacy preferences. The proposed mechanism allows consumers to participate in privacy protection and provides a practical framework for balancing privacy protection and data utility in AMI systems.

Architecture of the Privacy-Aware Smart Metering Mechanism

Entities

The architecture of the proposed mechanism consists of five primary entities, each with clearly defined responsibilities and trust assumptions.

- 1) *Private key generator*: The private key generator (PKG) is a trusted authority responsible for initialization and identity-based private key extraction. It generates the master secret keys and provisions identity-based private keys to authorized receivers. After initialization, the PKG remains offline except during scheduled secure provisioning events.
- 2) *Time server*: The time server (TS) is an independent authority responsible for generating time-dependent trapdoors associated with predefined release time slots. It maintains a time master secret and publishes a global time public key. Time trapdoors are periodically broadcast by the TS, and they enable the decryption of ciphertexts that are cryptographically time locked to their corresponding future time slots.
- 3) *DSO*: The DSO is the authorized data receiver that collects smart metering data to execute smart grid operations, such as DR and load monitoring. Successful decryption of

the received ciphertexts requires both the identity-based private key issued by the PKG and the corresponding time trapdoor released by the TS.

- 4) *Electricity consumer*: The electricity consumer is the end user whose electricity consumption is measured by the AMI system for various purposes, including routine billing and participation in demand-side management programs. Consumers may exhibit heterogeneous privacy preferences regarding their smart metering data. They interact with the proposed mechanism by selecting a personalized privacy parameter that determines the temporal resolution of the disclosed data.
- 5) *SM*: The SM is a resource-constrained device deployed at the consumer premises. It measures electricity consumption at the native sampling frequency. Based on the selected privacy parameter, the SM encrypts smart metering data under the identity of the DSO and a designated release time slot, thereby performing the cryptographic downsampling process.

Workflow

The proposed privacy-aware smart metering mechanism operates through five sequential phases, as illustrated in Figure 1.

Initialization

During the initialization phase, the cryptographic parameters are established by the trusted au-

thorities. The PKG generates the master secret keys and provisions the identity-based private key to the DSO. Concurrently, the TS generates the time master secret and publishes the global time public key.

Privacy-Preserving Sampling Boundary Calculation

The DSO calculates the maximum admissible sampling interval $N_{\max}$ based on the security and operational stability requirements of the smart grid. This boundary provides a principled guideline for data minimization by determining the maximum sampling sparsity that the smart grid can tolerate without compromising operational functions, such as DR.

Privacy Parameter Negotiation

To reduce the management complexity associated with arbitrary heterogeneous sampling intervals, the continuous safe region $[1, N_{\max}]$ is mapped to a discrete menu of privacy levels. The DSO publishes a set of available sampling intervals, for example, $N \in \{1, a, N_{\max}, N_{\text{billing}}\}$, where a represents an intermediate privacy level ($1 < a < N_{\max}$) and N_{billing} represents a sparse interval dedicated to billing purposes (e.g., daily or monthly). The N_{billing} interval is not involved in DR or real-time grid operations and is therefore not subject to the sampling boundary constraint. Consumers select a personalized sampling interval N_i from this menu according to their individual privacy preferences. Since higher privacy levels consume the limited uncertainty budget

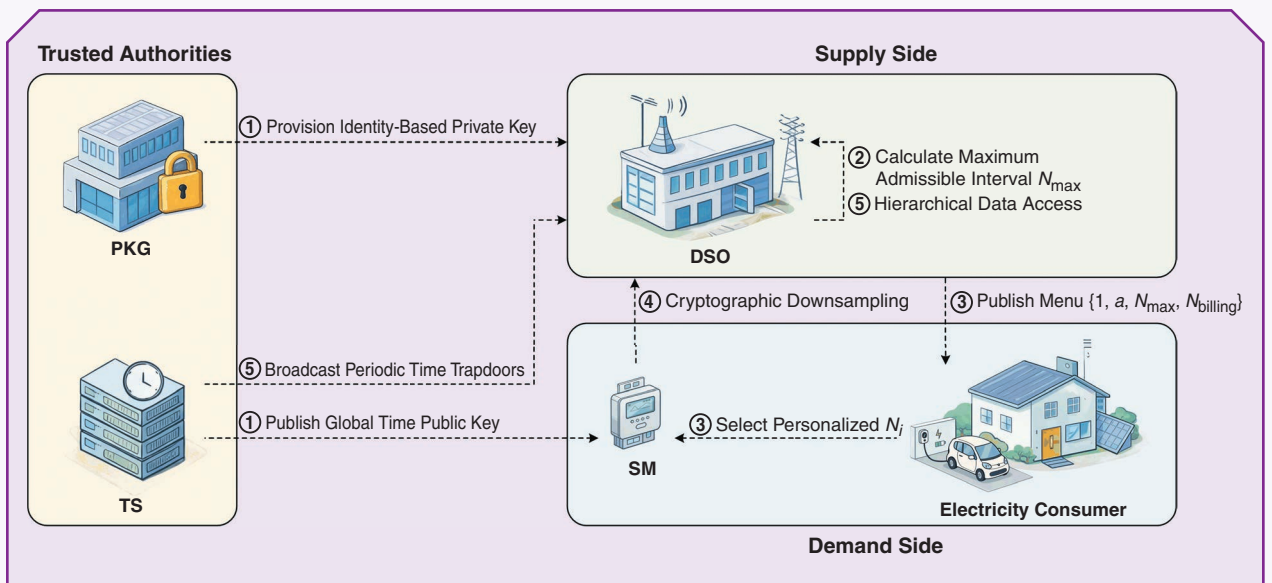


figure 1. The architecture and operational workflow of the proposed privacy-aware smart metering mechanism.

of the smart grid, future implementations may incorporate incentive or pricing mechanisms into this phase. Such mechanisms could guide consumer selections through ex ante price signals or ex post cost allocations.

Cryptographic Downsampling

Once the personalized sampling interval N_i is determined, the SM continues to measure electricity consumption at the native sampling frequency. Unlike conventional physical downsampling that permanently discards high-resolution data and degrades measurement exactness, the proposed mechanism decouples physical data acquisition from data disclosure by enforcing access control at the cryptographic layer. Within each time window of length N_i , only one selected meter reading is cryptographically time locked to the current time slot, enabling immediate decryption. The remaining $N_i - 1$ intermediate readings are cryptographically time locked to future release time slots using the time public key published by the TS. All encrypted readings are subsequently transmitted to the DSO.

Hierarchical Data Access and Grid Operation

After receiving the ciphertexts, the DSO performs hierarchical data access. For real-time smart grid operations, the DSO uses its identity-based private key together with the currently available time trapdoor released by the TS to immediately decrypt the single authorized reading within each N_i window. The intermediate readings remain encrypted and inaccessible. Only when the designated future time slots arrive and the TS broadcasts the corresponding time trapdoors can the DSO decrypt these high-resolution historical data. This delayed access paradigm ensures that detailed behavioral patterns are protected from real-time privacy inference attacks, such as NILM. Meanwhile, the mechanism preserves the exactness of smart metering data for offline analytics, auditing, and billing verification.

Privacy-Preserving Sampling Boundary Calculation

This section derives an upper bound on the SM sampling interval that preserves the operational reliability of the smart grid. Following the probabilistic modeling framework established in existing studies, the uncertainty introduced by reduced data sampling is quantified. A constraint is then formulated to characterize the maximum level of aggregate uncertainty that the smart grid can tolerate while maintaining stable operation.

Based on this constraint, the maximum admissible homogeneous sampling interval, denoted by $N_{\max}$, is derived. The resulting sampling boundary provides a principled guideline for privacy-aware smart metering. It defines the safe region within which the sampling interval can be increased to enhance consumer privacy while ensuring that the quality of the metering data remains sufficient for DR control and other grid operational functions.

Uncertainty Propagation of Electricity Consumption

To quantify how reduced data sampling affects grid observability, the evolution of electricity consumption uncertainty is first modeled at the individual consumer level.

The electricity consumption of consumer i is described by the following discrete-time state equation:

$$y_{i,k+1} = \alpha_i y_{i,k} + \beta_i u_{i,k} + d_{i,k} \quad (1)$$

where $y_{i,k}$ denotes the electricity consumption at time step k and $u_{i,k}$ is the control signal issued by the smart grid for DR. The parameter α_i characterizes the inertia of the consumption dynamics, while β_i captures the responsiveness of the load to the control signal. To ensure the stability of the consumption dynamics, it is assumed that $|\alpha_i| < 1$. The disturbance term $d_{i,k}$ represents stochastic fluctuations in electricity consumption caused by unmodeled behavioral and environmental factors. It is modeled as an independent Gaussian random variable with zero mean and variance $\sigma_{d,i}^2$. Disturbances are assumed to be independent across both time and consumers.

Let $\mathcal{F}_k$ denote the information set available to the grid at time step k . Conditional on $\mathcal{F}_k$, future uncertainty arises solely from the disturbance sequence. Suppose consumer i selects a personalized sampling interval $N_i \in \mathbb{Z}_+$, meaning that the grid receives a meter reading from this consumer only once every N_i steps.

Let m denote the number of forward prediction steps since the last measurement at time k , where $0 < m \leq N_i$. By iterating (1), the electricity consumption at time $k+m$ can be expressed as

$$y_{i,k+m} = \alpha_i^m y_{i,k} + \sum_{\ell=0}^{m-1} \alpha_i^{m-1-\ell} (\beta_i u_{i,k+\ell} + d_{i,k+\ell}) \quad (2)$$

where ℓ serves as the step index within the unobserved prediction window.

Since the control inputs are deterministic given $\mathcal{F}_k$, the uncertainty of $y_{i,k+m}$ originates solely

from the disturbance terms. Applying the index substitution $r = m - 1 - \ell$, the conditional variance of the predicted consumption becomes

$$\text{Var}(y_{i,k+m}|\mathcal{F}_k) = \sigma_{d,i}^2 \sum_{r=0}^{m-1} \alpha_i^{2r}. \quad (3)$$

For $|\alpha_i| < 1$, the geometric series in (3) admits the closed-form expression

$$\text{Var}(y_{i,k+m}|\mathcal{F}_k) = \sigma_{d,i}^2 \frac{1 - \alpha_i^{2m}}{1 - \alpha_i^2}. \quad (4)$$

Consider a distribution system with n consumers. The aggregate electricity demand at time $k + m$ is defined as

$$Y_{k+m} = \sum_{i=1}^n y_{i,k+m}. \quad (5)$$

Under the independence assumption of individual disturbances, the uncertainty of the aggregate demand equals the sum of individual variances.

$$V_{\text{total}}(k+m) = \text{Var}(Y_{k+m}|\mathcal{F}_k) = \sum_{i=1}^n \text{Var}(y_{i,k+m}|\mathcal{F}_k). \quad (6)$$

Equation (6) shows that increasing the sampling interval increases the uncertainty of the aggregate demand estimation, thereby reducing the accuracy of DR control.

Grid Security Budget Constraint

DR control aims to maintain the aggregate electricity demand close to a desired operating target. Let Y_{k+m}^* denote the target aggregate demand at the future time step $k + m$, and let Y_b denote the maximum allowable deviation from this target. The grid operational reliability requirement can therefore be expressed through the following probabilistic constraint:

$$\Pr(|Y_{k+m} - Y_{k+m}^*| \leq Y_b) \geq 1 - \epsilon \quad (7)$$

where ϵ denotes the acceptable probability of constraint violation.

The DR controller is assumed to achieve unbiased tracking in expectation such that

$$\mathbb{E}[Y_{k+m}|\mathcal{F}_k] = Y_{k+m}^*. \quad (8)$$

Under the Gaussian disturbance assumption introduced in the previous section, the aggregate demand follows the conditional distribution

$$Y_{k+m}|\mathcal{F}_k \sim N(Y_{k+m}^*, V_{\text{total}}(k+m)) \quad (9)$$

where $V_{\text{total}}(k+m)$ is the aggregate demand uncertainty derived in (6).

Based on the properties of the normal distribution, the probability in (7) can be expressed as

$$\Pr(|Y_{k+m} - Y_{k+m}^*| \leq Y_b) = 2\Phi\left(\frac{Y_b}{\sqrt{V_{\text{total}}(k+m)}}\right) - 1 \quad (10)$$

where $\Phi(\cdot)$ denotes the cumulative distribution function of the standard normal distribution.

Enforcing the probabilistic reliability requirement in (7) yields the following bound on the aggregate demand uncertainty:

$$V_{\text{total}}(k+m) \leq \left(\frac{Y_b}{\Phi^{-1}\left(1 - \frac{\epsilon}{2}\right)}\right)^2 \triangleq \Sigma_{\text{budget}}. \quad (11)$$

The quantity Σ_{budget} represents the maximum aggregate uncertainty that the grid can tolerate while maintaining the required operational reliability.

Derivation of the Maximum Sampling Boundary

Consider first a homogeneous sampling configuration in which all consumers adopt the same sampling interval N . Within each sampling period, the grid performs state prediction without receiving new measurements. As shown in the previous section, the prediction variance of consumer i increases with the prediction horizon and reaches its maximum at the end of the sampling interval ($m = N$). The corresponding peak variance is therefore

$$v_i(N) = \sigma_{d,i}^2 \frac{1 - \alpha_i^{2N}}{1 - \alpha_i^2}. \quad (12)$$

Aggregating over all consumers yields the worst-case aggregate demand uncertainty within the sampling interval.

$$V_{\text{worst}}(N) = \sum_{i=1}^n \sigma_{d,i}^2 \frac{1 - \alpha_i^{2N}}{1 - \alpha_i^2}. \quad (13)$$

Since $0 \leq \alpha_i^2 < 1$, the term $1 - \alpha_i^{2N}$ increases monotonically with N . Consequently, the function $V_{\text{worst}}(N)$ monotonically increases in N and converges to the steady-state aggregate variance limit.

$$V_{\infty} = \sum_{i=1}^n \frac{\sigma_{d,i}^2}{1 - \alpha_i^2}. \quad (14)$$

Combining the worst-case uncertainty in (13) with the grid security budget constraint derived in (11), the maximum admissible homogeneous sampling interval is defined as

$$N_{\max} = \max\{N \in \mathbb{Z}_+ : V_{\text{worst}}(N) \leq \Sigma_{\text{budget}}\} \quad (15)$$

where $\mathbb{Z}_+$ denotes the set of positive integers. The value $N_{\max}$ therefore characterizes the largest sampling interval that preserves the required grid reliability level.

In practice, consumers may adopt heterogeneous sampling intervals reflecting different privacy preferences. Let each consumer select an individual interval $N_i \leq N_{\max}$. For any prediction horizon $m \leq N_i$, the individual variance satisfies

$$\text{Var}(y_{i,k+m} | \mathcal{F}_k) \leq v_i(N_i) \leq v_i(N_{\max}). \quad (16)$$

Summing over all consumers yields

$$V_{\text{total}}(k+m) \leq V_{\text{worst}}(N_{\max}) \leq \Sigma_{\text{budget}}. \quad (17)$$

Therefore, any heterogeneous sampling configuration satisfying $N_i \leq N_{\max}$ remains within the prescribed grid security budget. The derived boundary thus provides a principled upper limit on privacy-preserving sampling intervals, ensuring the reliability requirements of DR operation.

Cryptographic Downsampling Method

This section presents the cryptographic downsampling method that operationalizes the privacy-preserving sampling boundary derived in the previous section. The objective is to enforce the personalized sampling interval N_i without compromising the native high-frequency sensing capabilities of SMs.

The design is motivated by the observation that the privacy sensitivity of smart metering data is highest when the data are immediately available in plaintext and gradually decreases as disclosure is delayed. Instead of physically reducing the sampling frequency, the proposed method controls the temporal availability and preserves the temporal confidentiality of the collected smart metering data. Within each sampling interval N_i , only one reading is immediately decryptable to support real-time grid monitoring and control, while the remaining intermediate readings are encrypted and released at designated future time slots.

Preliminaries

Let p be a large prime. Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be cyclic groups of order p , where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive groups and $\mathbb{G}_T$ is a multiplicative group. Let $P_1 \in \mathbb{G}_1$ and $P_2 \in \mathbb{G}_2$ denote generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

A bilinear pairing is defined as

$$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T \quad (18)$$

which satisfies the following properties:

- *Bilinearity*: For all $X \in \mathbb{G}_1$, $Y \in \mathbb{G}_2$, and $a, b \in \mathbb{Z}_p$, it holds that $e(aX, bY) = e(X, Y)^{ab}$.
- *Nondegeneracy*: $e(P_1, P_2) \neq 1_{\mathbb{G}_T}$.
- *Efficient computability*: There exists a polynomial-time algorithm for evaluating $e(\cdot, \cdot)$.

The proposed construction employs asymmetric (type 3) bilinear groups, where the pairing is defined between distinct source groups $\mathbb{G}_1$ and $\mathbb{G}_2$, and no efficiently computable isomorphism exists between them. Such groups can be instantiated using pairing-friendly elliptic curves (e.g., BLS12-381), which offer roughly 128-b security under standard parameter settings while maintaining compact system parameters.

Cryptographic Construction

The proposed cryptographic downsampling method combines identity-based encryption (IBE) with a TRE mechanism. The construction consists of five polynomial-time algorithms.

- 1) *Setup*: Given the security parameter λ , the PKG and TS jointly initialize the system. The PKG generates a master secret key $s \leftarrow \mathbb{Z}_p$ and computes the master public key.

$$P_{\text{pub}} = sP_2 \in \mathbb{G}_2. \quad (19)$$

Concurrently, the TS generates a time master secret $\theta \leftarrow \mathbb{Z}_p$ and publishes the time public key.

$$T_{\text{pub}} = \theta P_2 \in \mathbb{G}_2. \quad (20)$$

Three hash functions are modeled as random oracles.

$$\begin{aligned} H_1 &: \{0, 1\}^* \rightarrow \mathbb{G}_1 \\ H_2 &: \mathbb{G}_T \rightarrow \{0, 1\}^{L_m + L_r} \\ H_3 &: \{0, 1\}^* \rightarrow \{0, 1\}^{L_{\text{tag}}} \end{aligned} \quad (21)$$

where L_m denotes the bit length of a binary-encoded meter reading, L_r is the length of an auxiliary random string, and L_{tag} denotes

the integrity tag length. The operators $\parallel$ and $\oplus$ denote string concatenation and bitwise XOR, respectively.

The public parameters are defined as

$$\text{Params} = \{p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2, P_{\text{pub}}, T_{\text{pub}}, H_1, H_2, H_3\}. \quad (22)$$

- 2) *Key generation*: For each operational epoch j , let $\text{epoch}_j \in \{0, 1\}^*$ be its unique string identifier and $\text{ID}_{\text{DSO}} \in \{0, 1\}^*$ be the identity of the DSO. The PKG generates the identity-based private key of the DSO.

$$d_{\text{DSO},j} = sH_1(\text{ID}_{\text{DSO}} \parallel \text{epoch}_j) \in \mathbb{G}_1. \quad (23)$$

- 3) *TS release*: For a designated release time slot $T_\tau \in \{0, 1\}^*$ within epoch j , the TS generates and broadcasts the corresponding time trapdoor.

$$\text{st}_{T_\tau} = \theta H_1(T_\tau) \in \mathbb{G}_1. \quad (24)$$

This trapdoor enables the decryption of ciphertexts cryptographically time locked to that time slot.

- 4) *Encrypt*: Let $M \in \{0, 1\}^{L_m}$ denote the binary representation of a meter reading collected within the sampling interval. The SM first computes or retrieves from offline precomputation the pairing-derived element

$$\Omega_{j,\tau} = e(H_1(\text{ID}_{\text{DSO}} \parallel \text{epoch}_j), P_{\text{pub}}) \cdot e(H_1(T_\tau), T_{\text{pub}}) \in \mathbb{G}_T. \quad (25)$$

During the online encryption phase, the SM generates a random scalar $\rho \leftarrow \mathbb{Z}_p$ and an auxiliary random string $\xi \leftarrow \{0, 1\}^{L_\tau}$, and it computes

$$C_1 = \rho P_2 \in \mathbb{G}_2 \quad (26)$$

where C_1 serves as the ephemeral public value associated with the encryption randomness.

Next, the SM derives a session key by exponentiating the pairing-derived element $\Omega_{j,\tau}$ with the same randomness ρ .

$$K = \Omega_{j,\tau}^\rho \in \mathbb{G}_T. \quad (27)$$

The SM then encrypts the meter reading by applying a hash-based mask to the randomized message $(M \parallel \xi)$.

$$C_2 = (M \parallel \xi) \oplus H_2(K). \quad (28)$$

Finally, a verification tag η is generated to ensure the structural integrity of the ciphertext during decryption.

$$\eta = H_3(C_1 \parallel M \parallel \xi). \quad (29)$$

The resulting ciphertext is defined as

$$CT = \langle C_1, C_2, \eta, T_\tau, \text{epoch}_j \rangle. \quad (30)$$

- 5) *Decrypt*: Upon receiving the ciphertext CT , the DSO first derives the encapsulated shared secret associated with the ciphertext.

$$K' = e(d_{\text{DSO},j} + \text{st}_{T_\tau}, C_1). \quad (31)$$

This pairing operation reconstructs the same session key used during encryption.

Next, the DSO removes the hash-based mask from the ciphertext payload to recover a candidate plaintext.

$$M' \parallel \xi' = C_2 \oplus H_2(K'). \quad (32)$$

Finally, the integrity is verified by checking

$$\eta = H_3(C_1 \parallel M' \parallel \xi'). \quad (33)$$

If the verification succeeds, the algorithm outputs the recovered original reading M .

Case Studies

This section provides a comprehensive evaluation of the proposed privacy-aware smart metering mechanism from three complementary perspectives: system-level effectiveness, security, and computational feasibility.

First, the effectiveness of the proposed privacy-preserving sampling boundary model is validated through numerical simulations using real-world smart metering data. This evaluation specifically examines whether the derived maximum admissible sampling interval N_{max} can effectively bound aggregate demand uncertainty while preserving the operational reliability of DR programs. Second, the security properties of the cryptographic downsampling method are analyzed, demonstrating its capability to securely regulate data disclosure in strict accordance with the defined privacy-preserving sampling boundary. Finally, the computational feasibility of the proposed mechanism is assessed, verifying that

the underlying cryptographic operations are highly optimized and fully viable for deployment on resource-constrained SMs.

System-Level Effectiveness

To evaluate the effectiveness of the proposed privacy-preserving sampling boundary model, numerical simulations are conducted using real-world smart metering data from the Pecan Street Dataport, which provides a native sampling resolution of 15 min. A cluster of 25 residential consumers in Austin, TX, USA, is selected to represent a typical community microgrid or local aggregation node. The evaluation focuses on August 2018, a summer period characterized by pronounced electricity demand and frequent operation of flexible demand-side resources, such as air-conditioners and electric vehicles.

The simulation configuration follows the analytical framework developed in the preceding sections. In particular, the parameters of the discrete-time state equation describing electricity consumption dynamics are identified from historical load profiles of the selected consumers. The grid operational reliability parameters are set to $Y_b = 14$ kW and $\epsilon = 0.05$, which require the aggregate electricity demand to remain within the operational boundaries with a probability of at least 95%.

Figure 2 gives the baseline aggregate electricity demand of the selected residential consumers over a representative summer day. The red dashed lines denote the operational boundaries defined by the target aggregate demand Y_{k+m}^* and the maximum allowable deviation Y_b . The frequent proximity to or violation of these boundaries indicates the necessity of DR actions

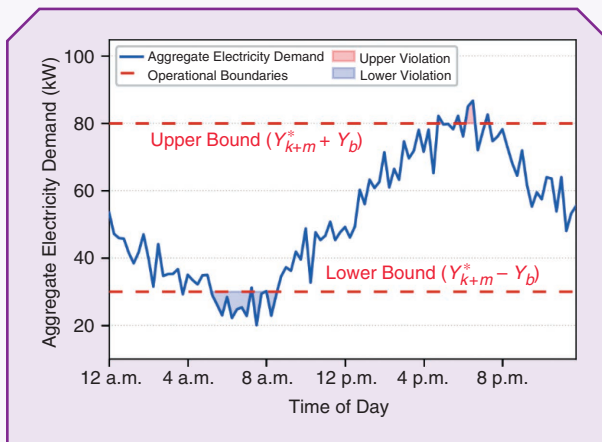


figure 2. The aggregate electricity demand relative to the operational boundaries.

to maintain grid stability, which in turn requires sufficiently accurate and timely observations of aggregate electricity demand.

According to the uncertainty propagation model, reducing the SM sampling frequency increases the number of unobserved time steps and leads to the accumulation of estimation uncertainty. Using historical load data, the consumption dynamics are identified through autoregressive modeling, yielding an average load inertia coefficient of **0.51** and an average disturbance standard deviation of **1.06** kW. The steady-state aggregate variance limit is calculated as **53.59** kW². This result indicates that excessively large sampling intervals would lead to unacceptable degradation of operational reliability, highlighting the necessity of imposing a finite upper bound on the sampling interval.

Figure 3 graphs the relationship between the sampling interval and operational reliability, measured by the probability $\Pr(|Y_{k+m} - Y_{k+m}^*| \leq Y_b)$. The results show that the maximum admissible sampling interval is $N_{\max} = 5$, which corresponds to a temporal resolution of 75 min. At this boundary, the operational reliability remains above the required threshold of **0.95**, satisfying the reliability requirement defined by $\epsilon = 0.05$.

As the sampling interval increases, the prediction horizon between successive observations expands, leading to the accumulation of aggregate demand uncertainty. Consequently, the probability that the aggregate demand remains within the operational boundaries decreases monotonically with N . When the sampling interval is small, frequent observations effectively constrain uncertainty and enable reliable DR operation. However, as N increases, the aggregate

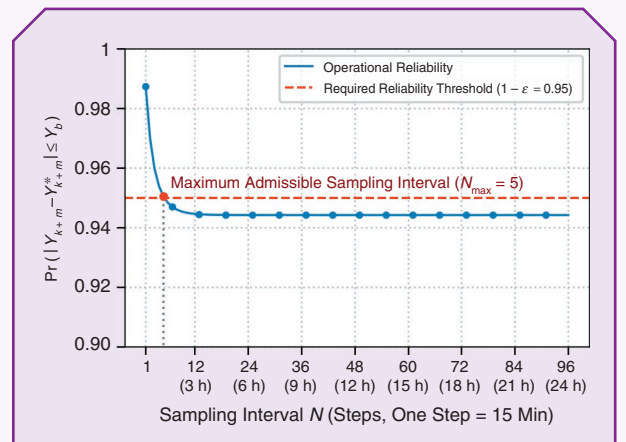


figure 3. The operational reliability as a function of the sampling interval.

uncertainty approaches the steady-state limit derived in the previous section, resulting in a progressive decline in reliability.

For $N \leq N_{\max}$, the worst-case aggregate demand and uncertainty remains within the maximum allowable deviation $Y_b = 14$ kW, ensuring that DR control can maintain the aggregate demand within operational constraints with the required confidence level. In contrast, sampling intervals exceeding $N_{\max}$ cause the uncertainty to surpass the grid security budget and thus cannot guarantee stable system operation.

These results provide empirical validation of the proposed privacy-preserving sampling boundary model. The identified bound $N_{\max}$ establishes the maximum admissible level of sampling reduction that preserves operational reliability while limiting the temporal resolution of observable consumption patterns. The derived boundary also enables flexible privacy configurations. Individual consumers may select personalized sampling intervals $N_i \in [1, N_{\max}]$ according to their privacy preferences, while the aggregate demand uncertainty remains within the prescribed security budget.

In summary, the simulation results confirm that the proposed sampling boundary provides a principled mechanism for balancing privacy protection and data utility.

Security Analysis

Threat Model

The security analysis considers the following threat assumptions:

- *External adversaries*: These adversaries are capable of eavesdropping on communication channels, intercepting ciphertexts, and attempting data manipulation.
- *DSO*: The DSO is assumed to be honest but curious, following the protocol while potentially trying to infer fine-grained consumption patterns from accessible data. The DSO stores identity-based private keys in a hardware security module and securely erases expired keys after the corresponding epoch ends.
- *PKG and TS*: The PKG and TS are trusted entities operating in independent domains without collusion.
- *Communication infrastructure*: The communication infrastructure provides origin authentication, antireplay protection, and device authorization via standard smart grid protocols.

Security Claims

The following claims provide a structured analysis of the security properties of the proposed cryptographic downsampling method. The arguments are based on standard cryptographic assumptions and are intended to provide security intuition suitable for smart grid engineering applications.

- *Security claim 1 (data confidentiality)*: The proposed method preserves the confidentiality of smart metering data against polynomial-time adversaries under an identity-based timed-release chosen-plaintext attack model.
 - *Justification*: The ciphertext payload is constructed as $C_2 = (M \parallel \xi) \oplus H_2(K)$, where K is a pairing-derived session key dependent on the system parameters, the DSO identity, the epoch identifier, the release time slot, and the encryption randomness. An adversary observing the ciphertext can obtain C_1 , C_2 , and the public parameters but cannot derive the session key K without access to both the identity-based private key $d_{\text{DSO},i}$ and the corresponding time trapdoor st_r . Under the hardness assumption of the underlying bilinear pairing problem and modeling $H_2(\cdot)$ as a random oracle, the keystream $H_2(K)$ is computationally indistinguishable from a random string. Therefore, the ciphertext does not reveal any meaningful information about the meter reading M .
 - *Implication for smart grids*: This property ensures that high-frequency smart metering data cannot be inferred by external adversaries or prematurely accessed by internal system entities. It effectively protects consumer privacy against data leakage and behavioral inference attacks, such as NILM.
- *Security claim 2 (integrity and tamper detection)*: The proposed method enables the probabilistic detection of ciphertext tampering and transmission errors.
 - *Justification*: Each ciphertext includes a verification tag $\eta = H_3(C_1 \parallel M \parallel \xi)$. During decryption, the DSO recomputes the tag using $M' \parallel \xi'$. Any modification of the ciphertext propagates to these recovered values. Due to the second-preimage resistance of H_3 , forging a valid tag without knowledge of the original plaintext is computationally infeasible.

Consequently, tampered ciphertexts will fail the verification process with overwhelming probability. This ensures that random transmission errors or malicious bit flipping attacks on the ciphertext are effectively detected. Note that η provides postdecryption integrity verification rather than full authenticated encryption; the origin authenticity of the SM is instead assured by the aforementioned underlying authenticated communication channel.

- *Implication for smart grids:* This property prevents corrupted or manipulated metering data from being accepted by the DSO, thereby avoiding incorrect load estimation or erroneous DR actions.
- *Security claim 3 (temporal privacy protection):* The proposed method enforces delayed access to smart metering data and prevents premature disclosure before the designated release time.
 - *Justification:* Within each sampling interval, meter readings are encrypted and cryptographically time locked to specific future time slots. Before the TS releases the corresponding time trapdoor, the ciphertexts remain computationally indistinguishable from random values under the confidentiality guarantee. Therefore, neither the honest-but-curious DSO nor external adversaries can access the plaintext data during the protected time window.
 - *Implication for smart grids:* This delayed disclosure limits the real-time exposure of detailed consumption patterns. It effectively mitigates privacy risks from behavioral inference attacks like NILM while still allowing lossless data access for offline analysis and auditing.
- *Security claim 4 (identity binding and replay resilience):* The proposed method supports resistance to message injection and replay attacks when combined with standard authenticated communication protocols.
 - *Justification:* Ciphertexts are generated using IBE tied to the identity of the DSO, ensuring that only the intended recipient can decrypt them. In addition, each ciphertext includes the epoch identifier and the release time slot, explicitly binding it to a specific temporal context. When combined with replay protection

mechanisms at the communication layer, replayed or injected messages outside their valid temporal context can be efficiently detected and discarded.

- *Implication for smart grids:* This property ensures that outdated or maliciously injected metering data cannot disrupt grid monitoring or operational control processes.
- *Property 1 (data exactness):* The proposed method preserves the exactness of smart metering data.
 - *Justification:* Unlike privacy-preserving approaches that modify or perturb data, the proposed method encrypts the original meter readings directly. After the designated release time, the DSO recovers the exact plaintext through the decryption process, ensuring lossless data recovery.
 - *Implication for smart grids:* This guarantees that applications requiring accurate and auditable data, such as billing, settlement, and historical load forecasting, are not compromised by the privacy protection mechanism.

Computational Feasibility for SMs

Although bilinear pairings are inherently resource intensive, the proposed cryptographic downsampling method is meticulously optimized for the hardware constraints of the SM. The computationally heavy pairing operations necessary to derive $\Omega_{j,\tau}$ remain entirely independent of both the real-time meter reading and the random scalar ρ . As a result, the SM can precompute and store these elements offline during idle periods. During the time-critical online encryption phase, the SM executes zero pairings, requiring only a single lightweight scalar multiplication in $\mathbb{G}_2$ to calculate $C_1 = \rho P_2$, alongside one exponentiation to compute the session key $K = \Omega_{j,\tau}^\rho$. This decoupling strategy minimizes the online computational overhead, thereby ensuring that high-frequency data sampling is not bottlenecked by cryptographic processing on the SM.

Conclusions

This article presented a privacy-aware smart metering mechanism for demand-side resources in power systems, addressing the fundamental tension between consumer privacy protection and the data availability required for smart grid operations. A privacy-preserving sampling boundary model was developed to determine

the maximum admissible sampling interval that preserves the operational reliability of DR, and a cryptographic downsampling method based on TRE was introduced to securely enforce the designated sampling interval. By integrating sampling boundary analysis, cryptographic enforcement, and heterogeneous consumer privacy preferences, the proposed mechanism establishes a systematic framework for privacy-aware acquisition while maintaining the operational value of demand-side resources, thereby promoting energy sustainability in smart grids.

Several directions remain for future research. First, the current method assumes that the PKG and TS operate independently without collusion. More robust designs that remain secure under partial trust or collusion scenarios warrant further investigation. Promising mitigation directions include employing threshold cryptography to distribute the functionalities of the PKG and TS across multiple independent nodes or adopting decentralized multiauthority architectures to eliminate single points of trust and reduce the impact of potential collusion. Second, the sampling boundary model may be extended to incorporate additional environmental and operational factors, such as temperature variations, weather conditions, and renewable generation uncertainties. In addition, the current case study involves only a relatively small population of residential consumers. Future work should therefore validate the model in larger-scale aggregation scenarios to assess its computational efficiency, boundary estimation accuracy, and scalability under more complex operating conditions. Third, the response delay and dynamic characteristics of DR programs can be explicitly modeled to further improve the realism of operational analysis. Fourth, future work should quantitatively evaluate the proposed mechanism against mainstream privacy protection approaches, such as differential privacy, under representative NILM inference attacks. Such studies would provide a more comprehensive assessment of the

proposed mechanism privacy protection effectiveness and the associated privacy–utility tradeoffs. Finally, incentive mechanisms that guide consumer participation under heterogeneous privacy preferences represent an important direction for enabling the practical deployment of privacy-aware smart metering mechanisms.

Acknowledgment

This work is funded in part by the National Natural Science Foundation of China (Grant 52407075); in part by the Science and Technology Development Fund, Macao SAR (Grants 0089/2026/RIB1, 0050/2025/AIJ, 001/2024/SKL, and 0002/2025/EQP); and in part by the Chair Professor Research Grant of University of Macau (Grant CPG2026-00026-IOTSC).

For Further Reading

X.-Y. Zhang, P. Guo, S. Kuenzel, and C. Yin, “Ethical considerations in advanced metering infrastructure integration: A systematic review,” *Energy Strategy Rev.*, vol. 56, Nov. 2024, Art. no. 101571, doi: [10.1016/j.esr.2024.101571](https://doi.org/10.1016/j.esr.2024.101571).

S. Finster and I. Baumgart, “Privacy-aware smart metering: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1088–1101, 2nd Quart. 2015, doi: [10.1109/COMST.2015.2425958](https://doi.org/10.1109/COMST.2015.2425958).

J. Zhang, C. Lu, H. Yi, and C. Wu, “User-perceptual privacy protection in NILM: A differential privacy approach,” *Appl. Energy*, vol. 382, Mar. 2025, Art. no. 125233, doi: [10.1016/j.apenergy.2024.125233](https://doi.org/10.1016/j.apenergy.2024.125233).

M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro, and J. P. S. Catalao, “Preserving privacy of smart meter data in a smart grid environment,” *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 707–718, Jan. 2022, doi: [10.1109/TII.2021.3074915](https://doi.org/10.1109/TII.2021.3074915).

J. Li, H. Hui, Y. Song, Y. Chen, T. Chen, and P. Siano, “Value-based data governance and security protection for virtual power plants aggregated by demand-side flexible loads,” *J. Mod. Power Syst. Clean Energy*, early access, Dec. 9, 2025, doi: [10.35833/MPCE.2025.000787](https://doi.org/10.35833/MPCE.2025.000787).

es

National Natural Science Foundation of China, 52407075 Science and Technology Development Fund, Macao SAR 0089/2026/RIB1, 0050/2025/AIJ, 001/2024/SKL, 0002/2025/EQP University of Macau, CPG2026-00026-IOTSC