Article

Not peer-reviewed version

The Privacy Risks of PV Inverter Telemetry: A Systematic Analysis of Leakage Vectors in Modern DER Ecosystems

V. Salas *

Posted Date: 16 March 2026

doi: 10.20944/preprints202603.1181.v1

Keywords: PV inverters; telemetry privacy; behavioural inference; metadata exposure; privacy leakage vectors; distributed energy resources (DER); SunSpec Modbus; Modbus TCP; IEEE 2030.5; cloud retention; privacy-by-design; data minimization

 doi:10.20944/preprints202603.1181.v1

Article

The Privacy Risks of PV Inverter Telemetry: A Systematic Analysis of Leakage Vectors in Modern DER Ecosystems

V. Salas

Department of Computer Science – IES Vista Alegre, Cybersecurity & PV Systems, Madrid, Spain; vsm425@educa.madrid.org

Abstract

The large-scale deployment of photovoltaic (PV) inverters in distributed energy resource (DER) ecosystems has created a highly connected environment where telemetry, remote access, and cloud platforms play a central operational role. Unlike smart meters, however, PV inverters have not been systematically examined from a privacy perspective, despite continuously generating fine-grained data that can reveal sensitive information about users and installations. This preprint presents the first comprehensive analysis of privacy leakage vectors in modern PV inverter ecosystems, covering device-level measurements, local interfaces, fieldbus protocols, cloud platforms, and external actors such as installers, aggregators, and utilities. Through a technical examination of inverter telemetry and widely adopted DER communication protocols (SunSpec Modbus, Modbus TCP, IEEE 2030.5), we identify structural risks including telemetry oversharing, metadata exposure, behavioural inference, cloud retention leakage, and installer-side overprivilege. Our findings show that inverter telemetry can reveal occupancy patterns, behavioural routines, consumption habits, and installation characteristics with high fidelity. We conclude by outlining initial recommendations for telemetry minimization, metadata reduction, and cloud governance, establishing the foundation for a dedicated privacy-by-design framework for PV inverters and DER systems. This work establishes that PV inverters represent a first-order privacy threat in the modern home, demanding immediate attention from manufacturers, standard-setting bodies, and policymakers.

Keywords: PV inverters; telemetry privacy; behavioural inference; metadata exposure; privacy leakage vectors; distributed energy resources (DER); SunSpec Modbus; Modbus TCP; IEEE 2030.5; cloud retention; privacy-by-design; data minimization

1. Introduction

The rapid growth of distributed photovoltaic (PV) generation has transformed residential and commercial energy systems into highly connected cyber-physical environments. Modern PV inverters are no longer isolated power-electronic devices; they continuously exchange telemetry with vendor cloud platforms, installer portals, aggregators, and utilities. This connectivity enables advanced monitoring, remote configuration, predictive maintenance, and participation in grid-support functions. As a result, PV inverters have become critical nodes in distributed energy resource (DER) ecosystems, with a communication footprint that increasingly resembles that of smart meters, IoT devices, and industrial controllers.

Despite this evolution, the privacy implications of inverter telemetry remain largely unexplored. While smart meters have been extensively studied for their potential to reveal occupancy patterns, behavioral routines, appliance usage, and sensitive household information, PV inverters have not received comparable scrutiny. This gap is striking, given that inverters generate high-resolution electrical measurements, operational metadata, device identifiers, commissioning information, and cloud-side logs that can be linked to user behaviour and installation characteristics. Moreover, the

 doi:10.20944/preprints202603.1181.v1

involvement of multiple external actors—installers, maintenance providers, utilities, and cloud vendors—creates complex data flows that amplify the risk of unintended exposure.

Existing research on DER cybersecurity has focused primarily on integrity and availability threats, such as false data injection attacks (FDIA), manipulation of grid-support functions, and protocol-level vulnerabilities in SunSpec Modbus or IEEE 2030.5. However, privacy has remained a secondary concern, often reduced to encryption or access control. No prior work has systematically examined how inverter telemetry, metadata, and cloud retention practices can lead to privacy leakage across the entire lifecycle of the device.

This preprint addresses this gap by presenting the first comprehensive analysis of privacy risks in PV inverter ecosystems. We examine leakage vectors at the device level, across local interfaces, within fieldbus protocols, in cloud platforms, and through interactions with external actors. Through a technical analysis of telemetry structures and communication protocols, we demonstrate how inverter data can reveal behavioural patterns, occupancy information, consumption habits, and installation details. We also highlight structural issues such as telemetry oversharing, metadata exposure, cloud retention leakage, and installer-side overprivilege.

By mapping these risks across the full telemetry pipeline, this work establishes the foundation for a dedicated privacy-by-design framework for PV inverters and DER systems. The findings presented here motivate the need for minimization strategies, metadata reduction, cloud governance, and lifecycle-aware privacy controls, which will be developed in subsequent preprints of this research series.

2. Background

The increasing digitalization of photovoltaic (PV) systems has transformed inverters from isolated power-electronic devices into fully networked components of distributed energy resource (DER) ecosystems. Modern inverters integrate sensors, embedded processors, communication modules, and cloud-connected services that enable continuous monitoring, remote configuration, and participation in grid-support functions. Understanding the privacy risks associated with these devices requires a clear view of their operational characteristics, telemetry flows, communication protocols, and the broader ecosystem in which they operate.

2.1. PV Inverters as Cyber-Physical DER Components

PV inverters convert DC power from solar modules into AC power for local consumption or grid injection. Beyond this core function, contemporary inverters incorporate:

- Embedded operating systems
- Local data logging and storage
- Wireless and wired communication interfaces
- Remote monitoring and control capabilities
- Cloud-based analytics and firmware updates

These capabilities position the inverter as a cyber-physical device with a continuous bidirectional data exchange between the physical installation and digital services. As a result, the inverter becomes a persistent source of fine-grained telemetry that can reveal operational, behavioural, and contextual information.

2.2. Telemetry Characteristics of Modern Inverters

Inverters typically generate multiple categories of telemetry, including:

- **Electrical measurements**: voltage, current, power, frequency, harmonics
- **Operational states**: MPPT behaviour, grid-support modes, alarms
- **Environmental data**: temperature, irradiance (in some models)
- **Metadata**: serial numbers, firmware versions, commissioning data
- **Event logs**: faults, restarts, configuration changes

 doi:10.20944/preprints202603.1181.v1

- **Cloud-side logs**: authentication events, installer access, API calls

Telemetry frequency ranges from **1–10 seconds** for real-time monitoring to **1–5 minutes** for aggregated reporting. This granularity is sufficient to infer behavioural patterns, occupancy, and consumption habits, similar to smart meter data but often with richer contextual metadata.

2.3. Communication Protocols in DER Ecosystems

PV inverters rely on a variety of communication protocols, each with different implications for privacy and security:

SunSpec Modbus (RTU/TCP)

Widely used for local monitoring and control.
- Exposes structured registers containing electrical measurements and metadata.
- Lacks built-in encryption or authentication in its basic form.
- Often used over RS485 or TCP/IP networks.

Modbus TCP

Common in commercial and industrial installations.
- Simple, lightweight, but inherently insecure.
- Susceptible to eavesdropping and manipulation.

IEEE 2030.5 (Smart Energy Profile 2.0)

Used for utility-inverter communication.
- Supports secure transport (TLS).
- Includes rich metadata and device models.
- Can expose detailed operational information.

Vendor-specific APIs and cloud protocols

- MQTT, HTTPS, WebSockets, proprietary telemetry channels.
- Often undocumented, with varying levels of minimization and retention.

These protocols define not only how data is transmitted but also what data is exposed, how frequently, and to whom.

2.4. Cloud Platforms and Installer Portals

Most inverter manufacturers operate cloud platforms that aggregate telemetry from millions of devices. These platforms typically provide:
- **User dashboards** for system owners
- **Installer portals** with privileged access
- Utility or aggregator interfaces for grid-support programs
- **APIs** for third-party integrations
- **Firmware update services (OTA)**
- **Long-term data retention and analytics**

Cloud platforms introduce additional privacy considerations:
- **Retention policies** that may exceed operational needs
- **Overprivileged installer accounts**
- **Cross-tenant data exposure risks**
- **Opaque data-sharing practices**
- **Metadata accumulation over years of operation**

Because cloud platforms sit at the center of the DER ecosystem, they become a major locus of privacy risk.

 doi:10.20944/preprints202603.1181.v1

2.5. External Actors and Data Flows

PV inverter data is accessed by multiple stakeholders:

- System owners
- Installers and maintenance providers
- Manufacturers
- Utilities and aggregators
- Third-party service providers

Each actor has different motivations, privileges, and access patterns. This multi-actor environment increases the risk of:

- Overprivileged access
- Unintended data sharing
- Cross-domain inference
- Long-term exposure through cloud retention

Understanding these relationships is essential for mapping privacy leakage vectors.

Figure 1 summarizes the end-to-end telemetry pathway and the associated privacy leakage surfaces across the inverter ecosystem.

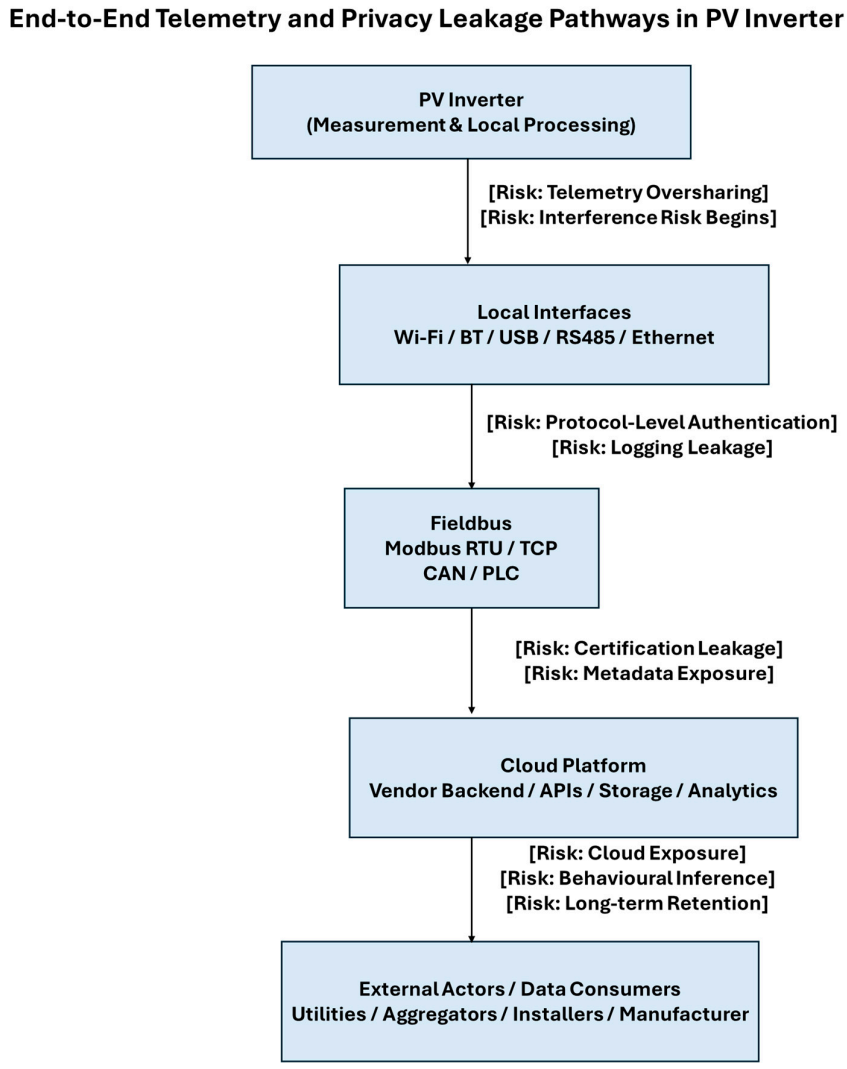

Figure 1. End-to-End Telemetry and Privacy Leakage Pathways in PV Inverter Ecosystems.

 doi:10.20944/preprints202603.1181.v1

3. Methodology

This work adopts a multi-layered analytical methodology designed to identify, classify, and evaluate privacy leakage vectors across the full telemetry pipeline of modern PV inverter ecosystems. The methodology combines technical inspection of telemetry structures, protocol analysis, actor modelling, and risk classification. The goal is not to assess a single device or vendor, but to derive generalizable insights applicable across the inverter industry.

3.1. Scope and Analytical Framework

The analysis focuses on five domains where privacy leakage may occur:

1. Device-level telemetry and local logging
2. Local communication interfaces (wired and wireless)
3. Fieldbus and DER communication protocols
4. Cloud platforms and vendor ecosystems
5. External actors with legitimate or delegated access

These domains correspond to the typical operational layers of PV inverter systems and reflect the multi-actor, multi-protocol nature of DER environments.

To structure the analysis, we adopt a privacy-centric adaptation of threat modelling approaches commonly used in cybersecurity (e.g., LINDDUN, STRIDE) but tailored to the specific characteristics of inverter telemetry and DER communication.

3.2. Telemetry Inspection and Data Characterization

We conducted a technical examination of telemetry formats and data structures used by commercial PV inverters. This included:

- Register maps from SunSpec Modbus models
- Sample telemetry payloads from Modbus TCP
- IEEE 2030.5 device models and resource structures
- Vendor-specific API payloads (where publicly documented)
- Metadata fields exposed during commissioning and operation

The analysis focused on identifying:

- **Measurement granularity**
- **Metadata richness**
- **Temporal resolution**
- **Contextual information**
- **Identifiers and cross-linkable fields**
- **Event and fault logs**

This step allowed us to determine which data elements could contribute to behavioural inference, occupancy detection, or installation profiling.

3.3. Protocol Analysis

We examined the communication protocols most commonly used in PV inverter ecosystems:

- SunSpec Modbus (RTU and TCP)
- Modbus TCP
- IEEE 2030.5 (Smart Energy Profile 2.0)
- Vendor-specific cloud protocols (MQTT, HTTPS, WebSockets)

For each protocol, we evaluated:

- **Data exposure** (fields, registers, metadata)
- **Security properties** (encryption, authentication, integrity)
- **Default configurations**
- **Potential for passive or active interception**

 doi:10.20944/preprints202603.1181.v1

- **Cross-layer interactions** (e.g., metadata leakage through TLS certificates or API endpoints)

This analysis enabled the identification of protocol-level leakage vectors independent of specific device implementations.

3.4. Actor and Adversary Modelling

We modelled the ecosystem of stakeholders interacting with inverter telemetry, including:

- System owners
- Installers and maintenance providers
- Manufacturers
- Utilities and aggregators
- Cloud vendors
- Potential adversaries (network-level, cloud-side, inference-based)

For each actor, we assessed:

- **Access privileges**
- **Data visibility**
- **Potential misuse scenarios**
- **Cross-domain inference capabilities**

This modelling step is essential because privacy leakage often arises not from a single actor, but from the combination of multiple legitimate access paths.

3.5. Risk Classification and Leakage Taxonomy

Based on the telemetry and protocol analysis, we developed a taxonomy of privacy leakage vectors grouped into five categories:

1. Device-level leakage
2. Interface-level leakage
3. Fieldbus-level leakage
4. Cloud-level leakage
5. External-actor leakage

Each leakage vector was evaluated according to:

- **Data sensitivity**
- **Inference potential**
- **Exposure likelihood**
- **Persistence and retention**
- **Cross-actor propagation**

This classification provides the foundation for the structured analysis presented in Section 4.

3.6. Limitations

This methodology focuses on:

- publicly available documentation,
- protocol specifications,
- telemetry structures,
- and generalizable architectural patterns.

It does not rely on reverse engineering of proprietary firmware or undisclosed vendor APIs, ensuring that the findings are broadly applicable and ethically grounded. By basing our analysis exclusively on publicly available documentation and industry-standard protocol specifications, our findings are inherently generalizable and verifiable, and they reveal systemic vulnerabilities that exist independently of any vendor-specific closed-source implementation.

 doi:10.20944/preprints202603.1181.v1

4. Privacy Leakage Vectors in PV Inverters

PV inverter ecosystems expose multiple categories of privacy leakage that arise from device-level telemetry, local interfaces, fieldbus protocols, cloud platforms, and interactions with external actors. Unlike traditional smart meters, inverters generate richer contextual metadata, more frequent measurements, and multi-actor access patterns, creating a broader and more complex privacy surface. This section presents a structured taxonomy of leakage vectors across the full telemetry pipeline.

The privacy risks identified in this work span multiple layers of the inverter ecosystem, from device-level telemetry to cloud retention and external-actor access. Figure 2 provides a high-level threat model that organizes these leakage surfaces across the main operational layers of PV inverter systems.

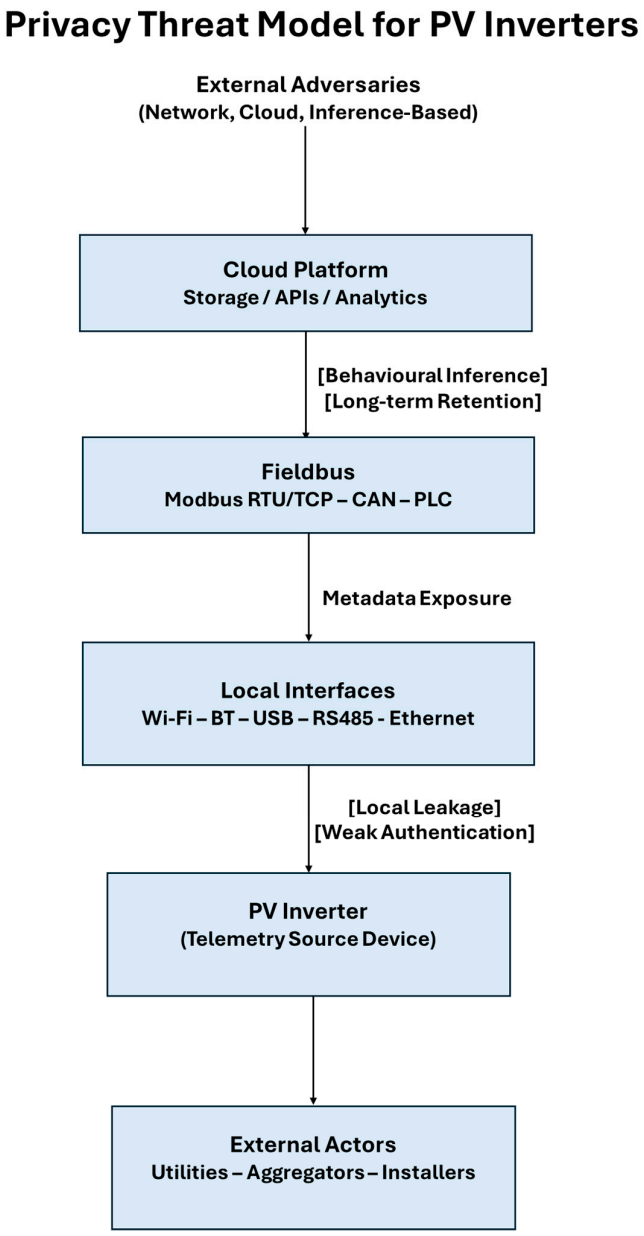

Figure 2. Privacy Threat Model for PV Inverters.

 doi:10.20944/preprints202603.1181.v1

4.1. Device-Level Leakage

Device-level leakage originates from the inverter's internal sensing, logging, and operational behaviour.

4.1.1. Fine-Grained Electrical Measurements

Inverters continuously report voltage, current, power, frequency, and MPPT behaviour at intervals of 1–10 seconds. These measurements can reveal:

- occupancy patterns
- appliance usage
- behavioural routines
- load signatures

Even without consumption data, PV production combined with inverter state transitions can infer when users are home, asleep, or away.

4.1.2. Local logging and event histories

Inverters maintain logs of:

- faults
- restarts
- configuration changes
- grid events
- installer interventions

These logs often include timestamps and contextual metadata that can expose long-term behavioural patterns or installation characteristics.

4.1.3. Persistent identifiers and metadata

Serial numbers, firmware versions, commissioning timestamps, and installer IDs can be used to:

- uniquely identify installations
- correlate data across platforms
- infer device age, maintenance history, or vulnerabilities

These identifiers often persist for the lifetime of the device.

4.2. Interface-Level Leakage

Local interfaces expose additional privacy risks, especially when default configurations are insecure.

4.2.1. Wi-Fi and Bluetooth interfaces

Many inverters broadcast:

- SSIDs containing device model or serial number
- Bluetooth identifiers
- Setup or commissioning beacons

These broadcasts can reveal:

- device presence
- installation type
- manufacturer
- commissioning status

In some cases, pairing or configuration interfaces expose telemetry without authentication.

4.2.2. USB, RS485, and service ports

Local service interfaces often provide:

 doi:10.20944/preprints202603.1181.v1

- raw telemetry
- configuration access
- commissioning data
- installer logs

If not protected, these ports enable:

- passive data extraction
- cloning of device metadata
- unauthorized access to historical logs

4.2.3. Installer commissioning apps

Mobile apps used during installation may leak:

- GPS coordinates
- installation photos
- user identifiers
- Wi-Fi credentials

These data flows are rarely documented.

4.3. Fieldbus-Level Leakage

Fieldbus protocols used for inverter monitoring and control expose structured telemetry and metadata.

4.3.1. SunSpec Modbus (RTU/TCP)

SunSpec models include:

- electrical measurements
- device metadata
- configuration parameters
- operational states

Because Modbus lacks encryption and authentication by default, attackers or unauthorized actors can:

- eavesdrop on telemetry
- infer behavioural patterns
- extract device identifiers
- correlate installations across networks

4.3.2. Modbus TCP

Used in commercial systems, it exposes:

- real-time telemetry
- fault logs
- configuration registers

Its simplicity makes it widely deployed but inherently privacy-weak.

4.3.3. IEEE 2030.5 (SEP2)

Although secured with TLS, IEEE 2030.5 exposes rich metadata:

- DER capabilities
- operational modes
- event histories
- device models

Metadata alone can reveal installation characteristics and user behaviour.

 doi:10.20944/preprints202603.1181.v1

4.4. Cloud-Level Leakage

Cloud platforms are a major source of privacy exposure due to long-term retention, multi-actor access, and opaque data practices.

4.4.1. Telemetry oversharing

Cloud platforms often collect:

- high-frequency telemetry
- detailed event logs
- commissioning metadata
- installer identifiers
- geolocation data

Much of this exceeds operational needs.

4.4.2. Long-term retention

Telemetry is frequently stored for:

- years
- indefinitely
- or without clear retention policies

This enables long-term behavioural profiling.

4.4.3. Overprivileged installer accounts

Installers often retain:

- full access to user systems
- historical data
- configuration capabilities

This creates privacy and security risks long after installation.

4.4.4. Cross-tenant exposure

Cloud dashboards sometimes aggregate:

- multiple customers
- multiple sites
- multiple devices

This increases the risk of accidental or unauthorized data visibility.

4.4.5. Vendor analytics and third-party integrations

Cloud vendors may use telemetry for:

- performance analytics
- fleet management
- predictive maintenance
- third-party services

These practices are rarely transparent to users.

4.5. External-Actor Leakage

PV inverter ecosystems involve multiple stakeholders, each with different access rights and motivations.

 doi:10.20944/preprints202603.1181.v1

4.5.1. Installers and maintenance providers

They often have:

- privileged access
- long-term visibility
- ability to extract logs
- access to commissioning metadata

This creates risks of:

- unauthorized monitoring
- data misuse
- cross-customer inference

4.5.2. Utilities and aggregators

Through IEEE 2030.5 or vendor APIs, utilities may access:

- operational states
- grid-support modes
- event histories

This can reveal:

- consumption patterns
- occupancy
- system behaviour

4.5.3. Third-Party Service Providers

Energy management platforms may access:

- telemetry
- metadata
- user identifiers

These actors introduce additional privacy surfaces.

4.6. Summary of Leakage Categories

PV inverter ecosystems expose privacy risks across five layers. Table 1 summarizes the main leakage categories identified in this work.

Table 1. Summary of Privacy Leakage Categories in PV Inverter Ecosystems.

Device	Measurement & metadata	Power, MPPT, logs, serials
Interfaces	Local access	Wi-Fi, BT, USB, RS485
Fieldbus	Protocol exposure	SunSpec, Modbus TCP, IEEE 2030.5
Cloud	Retention & overprivilege	Installer access, analytics
External actors	Multi-stakeholder access	Utilities, aggregators

This taxonomy provides the foundation for the discussion and recommendations in subsequent sections.

5. Behavioural and Occupancy Inference

Telemetry generated by PV inverters can reveal far more than electrical performance. Because measurements are continuous, fine-grained, and tightly coupled to household activity, they enable behavioural and occupancy inference similar to, and in some cases more detailed than, smart meter data.

 doi:10.20944/preprints202603.1181.v1

5.1. Occupancy Detection

Inverter telemetry exhibits characteristic patterns that correlate with user presence:

- rapid changes in self-consumption
- transitions between grid import and export
- inverter wake-up and sleep cycles
- load-driven fluctuations in PV utilisation

These patterns allow an observer to infer when occupants are home, away, or asleep. Even in systems with high PV export, inverter state transitions (e.g., MPPT behaviour, ramp-up curves) can reveal daily routines.

5.2. Behavioural Routines and Daily Patterns

High-frequency telemetry exposes:

- morning and evening activity peaks
- appliance-driven consumption signatures
- weekend vs weekday routines
- seasonal behavioural changes

Because inverters often report data every 1–10 seconds, the temporal resolution is sufficient to reconstruct detailed behavioural timelines.

5.3. Appliance and Load Inference

Although inverters do not directly measure consumption, they indirectly reveal:

- EV charging events
- heat pump operation
- HVAC cycles
- water heater usage
- battery charging/discharging patterns

These events create distinctive power signatures visible in inverter telemetry, especially in hybrid systems.

5.4. Installation Profiling

Metadata and operational parameters can reveal:

- system size and configuration
- presence of batteries
- type of inverter (hybrid, string, microinverter)
- commissioning date
- maintenance history

This information can be used to infer socioeconomic status, building characteristics, and user preferences.

5.5. Long-Term Behavioural Profiling

Cloud retention amplifies inference risks. Years of telemetry enable:

- lifestyle profiling
- occupancy probability models
- prediction of future behaviour
- correlation with external datasets (weather, tariffs, events)

Such long-term behavioural visibility is rarely disclosed to users.

 doi:10.20944/preprints202603.1181.v1

6. Discussion

The analysis presented in this preprint demonstrates that PV inverter telemetry exposes a broad and largely unaddressed privacy surface. Unlike smart meters—whose privacy implications have been extensively studied and regulated—PV inverters operate in a fragmented ecosystem with inconsistent data governance, heterogeneous protocols, and multi-actor access patterns.

6.1. Comparison with Smart Meter Privacy

Smart meters typically operate under strict regulatory frameworks that mandate:

- data minimization
- retention limits
- access control
- transparency requirements

In contrast, PV inverters:

- collect richer metadata
- transmit data more frequently
- involve more external actors
- rely heavily on cloud platforms
- lack standardized privacy requirements

This creates a privacy gap that is not reflected in current DER standards.

6.2. Implications for CRA, NIS2, and GDPR

The findings highlight several regulatory tensions:

- **CRA**: inverter vendors must address data protection as part of cybersecurity requirements.
- **NIS2**: operators of DER fleets must manage telemetry as sensitive operational data.
- **GDPR**: inverter telemetry qualifies as personal data when linked to identifiable users or behavioural patterns.

Current industry practices—particularly long-term retention and installer overprivilege—are difficult to reconcile with GDPR principles of minimization and purpose limitation.

6.3. Need for a Privacy-by-Design Framework

The leakage vectors identified across device, interface, fieldbus, cloud, and external-actor layers reveal the absence of a unified privacy strategy. A privacy-by-design baseline is needed to:

- reduce telemetry granularity
- minimize metadata exposure
- enforce lifecycle-aware access control
- govern cloud retention
- limit installer privileges
- ensure transparency for end users

This preprint establishes the analytical foundation for such a framework.

6.4. Limitations and Generalizability

This study focuses on:

- publicly documented telemetry structures
- protocol specifications
- common architectural patterns

While specific implementations vary across vendors, the leakage categories identified here are generalizable across the inverter industry.

 doi:10.20944/preprints202603.1181.v1

7. Recommendations

Based on the leakage vectors and inference risks identified, this section proposes a set of privacy-by-design principles to guide manufacturers, operators, and policymakers toward privacy-preserving inverter ecosystems. These principles are organized into layered controls spanning the device, interface, communication, cloud, and lifecycle domains. Figure 3 summarizes this baseline architecture.

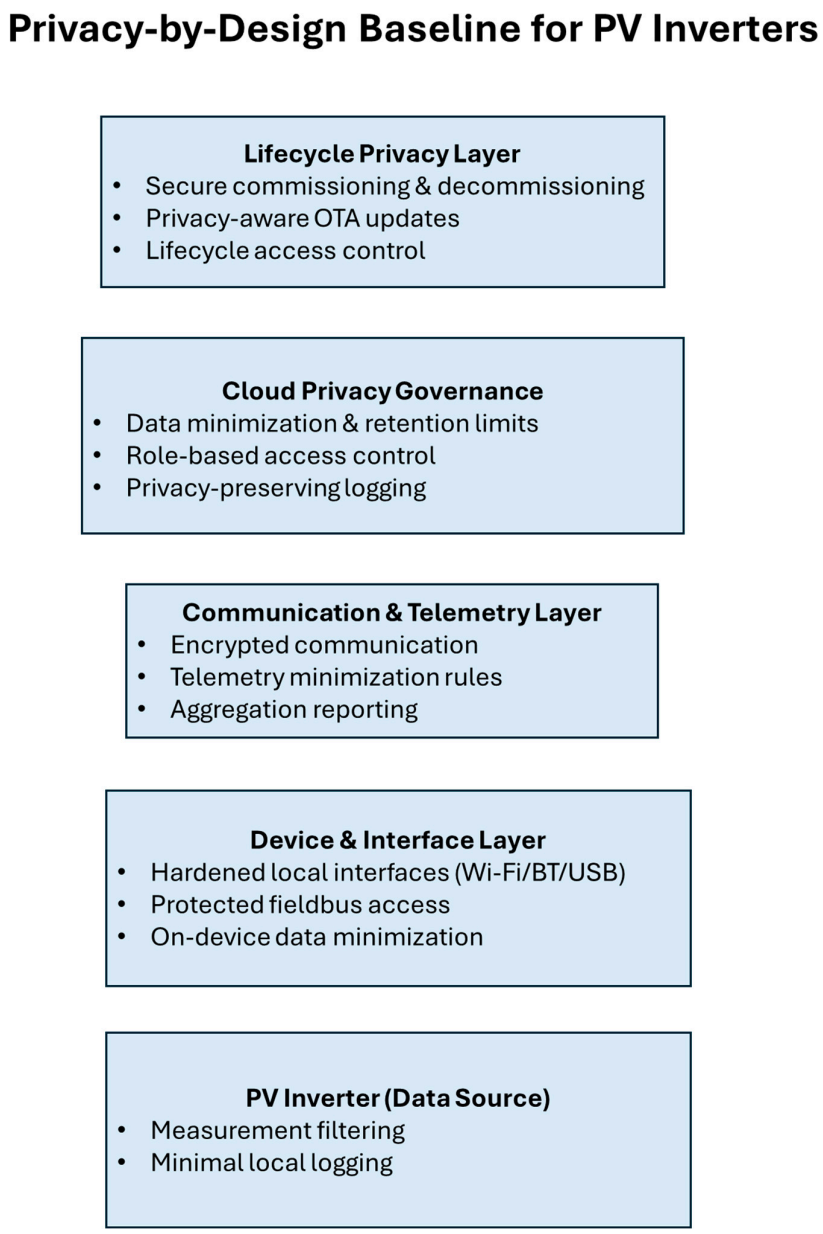

Figure 3. Privacy-by-Design Baseline for PV Inverters.

Building on the baseline principles summarized in Figure 3, Figure 4 provides a high-level reference architecture for privacy-aware PV inverter ecosystems. This architecture organizes privacy controls across device, interface, communication, cloud, and lifecycle layers, illustrating how the proposed measures can be applied in practice.

 doi:10.20944/preprints202603.1181.v1

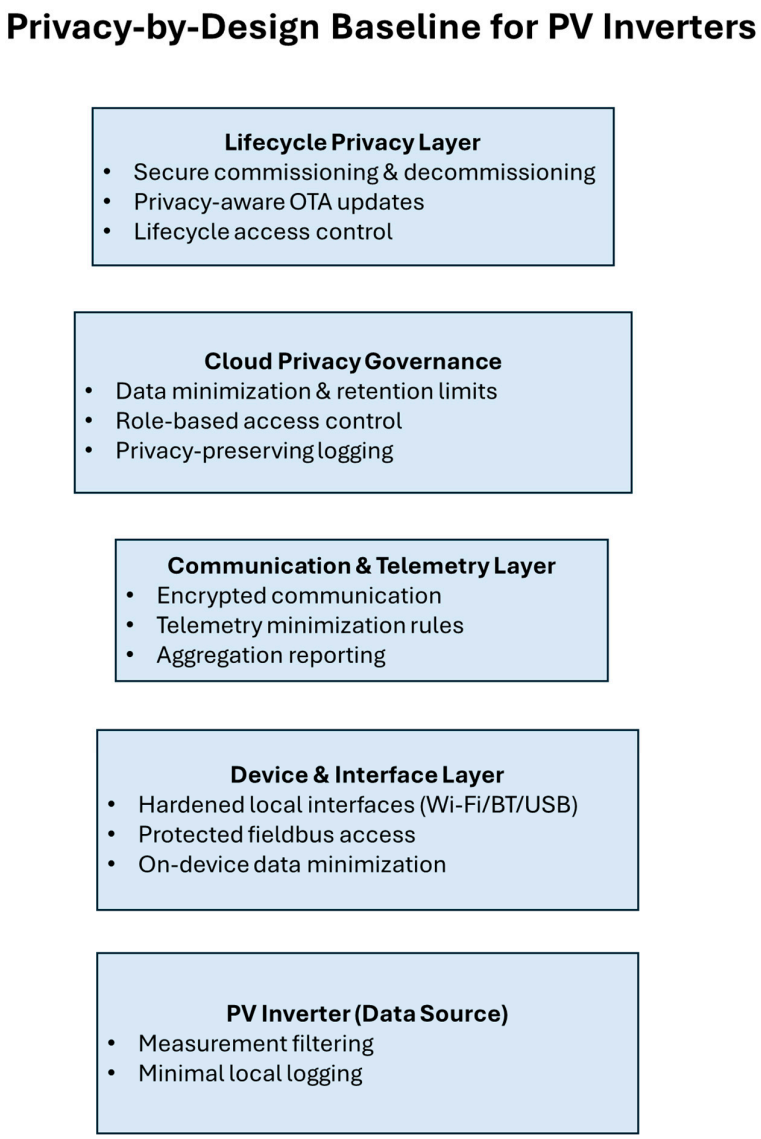

Figure 4. High-Level Privacy-Aware Architecture for PV Inverter Ecosystems.

7.1. Telemetry Minimization

- Reduce measurement frequency where possible.
- Limit reporting of high-resolution power data.
- Avoid transmitting redundant or non-essential fields.

7.2. Metadata Reduction

- Remove or hash persistent identifiers.
- Avoid exposing commissioning timestamps or installer IDs.
- Minimize device-specific metadata in cloud payloads.

7.3. Secure and Minimal Interfaces

- Disable Wi-Fi/Bluetooth after commissioning.
- Protect USB/RS485 ports with authentication.
- Restrict local access to essential functions only.

 doi:10.20944/preprints202603.1181.v1

7.4. Protocol Hardening

- Use encrypted and authenticated transport for Modbus TCP.
- Apply privacy-aware profiles for IEEE 2030.5.
- Limit exposure of SunSpec metadata.

7.5. Cloud Governance

- Enforce strict retention limits.
- Implement role-based access control (RBAC/ABAC).
- Remove installer access after commissioning.
- Provide transparency dashboards for users.

7.6. Lifecycle Privacy Controls

- Secure commissioning workflows.
- Privacy-aware OTA updates.
- Secure decommissioning and certificate revocation.

7.7. Multi-Actor Access Management

- Define clear privilege boundaries.
- Audit access by installers, utilities, and third parties.
- Provide user-controlled access revocation.

8. Conclusion

- This preprint has presented the first comprehensive analysis of privacy leakage vectors in modern PV inverter ecosystems. Through a structured examination of device-level telemetry, local interfaces, fieldbus protocols, cloud platforms, and multi-actor access patterns, we have shown that PV inverters expose a significantly broader privacy surface than previously recognized. Unlike smart meters—whose privacy implications have been extensively studied and regulated—PV inverters operate in a fragmented and largely unregulated environment where telemetry oversharing, metadata exposure, long-term retention, and installer overprivilege are common.
- Our findings demonstrate that inverter telemetry can reveal sensitive behavioural information, including occupancy patterns, daily routines, appliance usage, and long-term lifestyle profiles. These risks are amplified by cloud-centric architectures, persistent identifiers, and the involvement of multiple external actors with varying levels of access and visibility. The analysis highlights a clear gap between current industry practices and the privacy expectations established by frameworks such as GDPR, as well as the emerging cybersecurity obligations introduced by CRA and NIS2.
- By mapping privacy leakage across the full telemetry pipeline, this work establishes the analytical foundation for a dedicated privacy-by-design framework for PV inverters and DER systems. The recommendations provided—covering telemetry minimization, metadata reduction, interface hardening, protocol governance, cloud retention policies, and lifecycle-aware access control—outline initial steps toward more privacy-preserving inverter architectures.

 doi:10.20944/preprints202603.1181.v1

- Future work will build on this foundation by proposing a structured Privacy-by-Design Baseline, a reference architecture, and a case study demonstrating practical implementation. Together, these contributions aim to support manufacturers, operators, and policymakers in developing inverter ecosystems that are not only secure and interoperable, but also aligned with modern privacy principles.