privitty

# Privitty Edge Use-Case

Control Layer for Industrial Data Sharing in IIoT

info@privittytech.com
www.privittytech.com

# The Importance of Control layer

Industrial IoT systems have successfully adopted encryption, secure transport protocols, and cloud-native architectures. However, they continue to suffer from a **post-access control gap** -- once data is shared with a trusted entity, **control is effectively lost**.

This is not a cybersecurity failure. It is a **control architecture failure**.

In modern IIoT ecosystems:

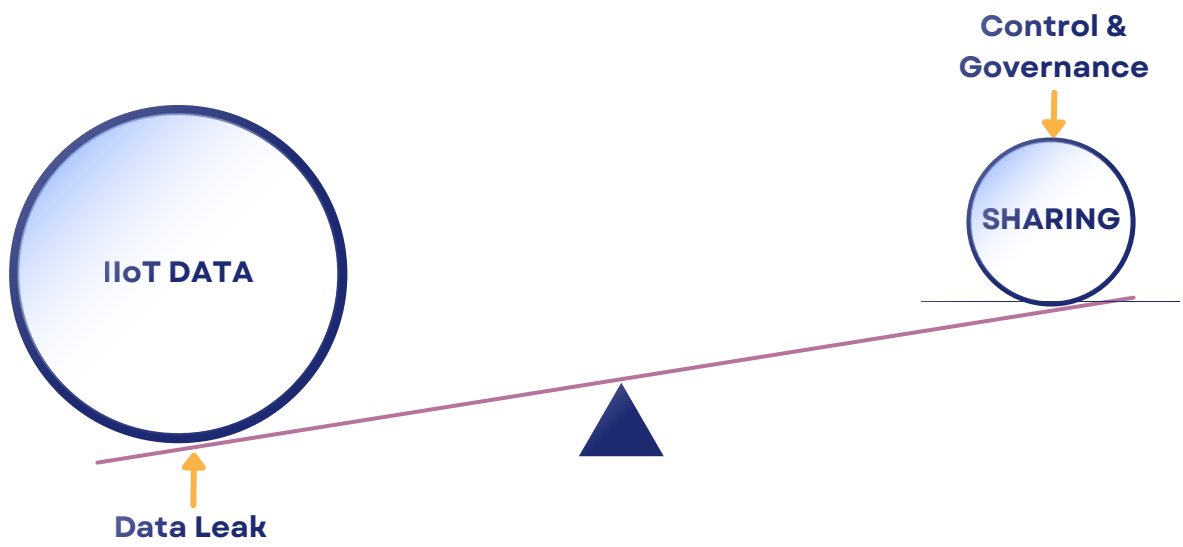
- Data flows across OEMs, suppliers, analytics vendors, and regulators
- Access is granted legitimately
- Risk emerges **after authorization**, not before

This creates a class of vulnerabilities where:

- Data is copied and stored indefinitely
- Usage exceeds contractual or operational intent
- Sensitive industrial insights are extracted without detection

No exploit is required.
No perimeter is breached.

*| The threat originates from legitimate access paths.*



# The IIoT Control Gap

## Current Security Stack

| Layer | Technology | Status |
|---|---|---|
| Trasnport | TLS, VPN | Mature |
| Identity | PKI, IAM | Mature |
| Storage | Encryption at rest | Mature |
| Processing | Cloud/Edge compute | Mature |
| Post-access Control | None | Missing |

## Current Security Stack

Once data leaves the originating system:

- It can be duplicated infinitely
- It can be retained beyond policy
- It can be reprocessed in unauthorized contexts

This aligns with findings in International Data Spaces Association (IDSA) architecture and recent IIoT data-sharing research, which highlight the lack of **usage control enforcement after data exchange.**

# Threat Model: Legitimate Access Misuse

## Scenario 1: Predictive Maintenance Data Leakage

Context:
An OEM shares vibration and thermal data with a third-party analytics provider.

Attack vector:

- Data is copied into internal data lakes
- Models are trained beyond agreed scope
- Insights are reused across competing clients

Impact:

- Loss of proprietary machine behavior patterns
- Competitive advantage erosion

| Metric | Value |
|---|---|
| Data volume shared | 50–200 GB/day |
| Model training reuse | 3–5 downstream applications |
| Estimated IP leakage cost | $2M–$10M/year |

## Scenario 2: Supply Chain Data Overexposure

Context:
Tier-1 supplier receives production data for optimization.

Failure:

- Data retained beyond contract duration
- Shared with subcontractors

Impact:

- Exposure of production rates
- Demand forecasting leakage

| Metric | Value |
|---|---|
| Retention violation window | 6–18 months |
| Downstream exposure | 2–4 subcontractors |
| Revenue impact | 1–3% margin erosion |

### Scenario 3: Edge Analytics Drift

Context:
Edge gateway shares filtered data with multiple services.

Failure:

- Data aggregation enables reconstruction of sensitive patterns
- Cross-correlation across datasets

Impact:

- Reconstruction of full operational state
- Reverse engineering of process logic

# Root Cause Analysis

The core issue is absence of **data-centric control primitives**:

| Capability | Status in Current Systems |
|---|---|
| Time-bound access | Limited |
| Revocation after sharing | Not enforceable |
| Usage restriction | Not enforceable |
| Auditability (post-access) | Weak |

# Privitty Edge: A Control Layer for IIoT

Privity introduces a **data-level control plane** enforced at the edge.

## Core Capabilities

| Capability | Description |
|---|---|
| Persistent Encryption | Data remains encrypted beyond transport |
| Policy-bound Access | Access tied to explicit constraints |
| Revocation | Access can be withdrawn after sharing |
| Usage Control | Data usable only in permitted contexts |
| Audit Trails | Every access is logged and verifiable |

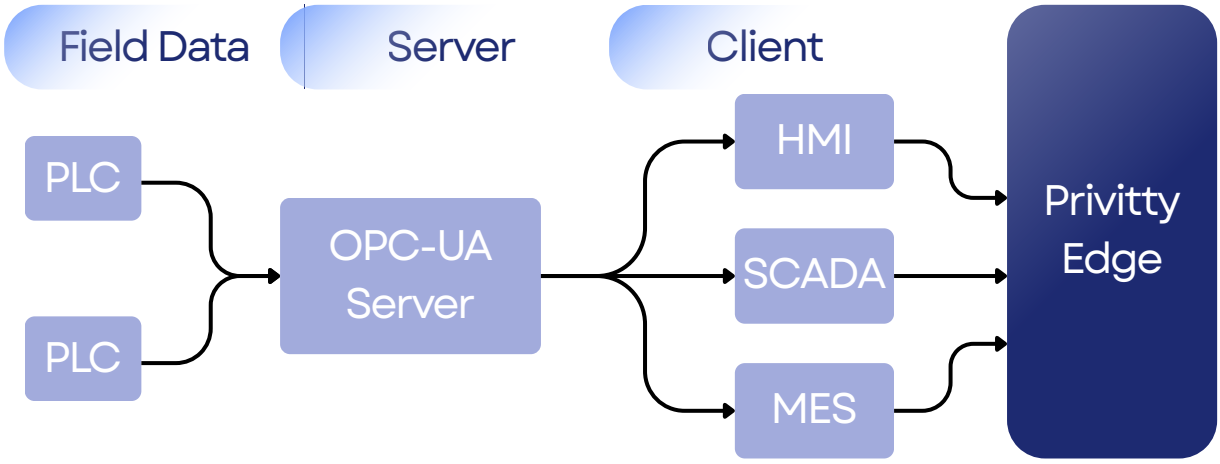
# Architecture Overview

Deployed on:

- IIoT gateways
- Edge compute nodes
- Data aggregation layers

Integrates with:

- Existing data pipelines
- PLC/Sensor → OPC-UA Server → OPC Clients (HMI, SCADA, Edge Server, UA Expert, MES systems, SCB)




# Quantified Impact

## Without Control Layer

| Risk Category | Probability | Impact |
|---|---|---|
| Data reuse beyond scope | High | High |
| IP leakage | Medium | High |
| Regulatory non-compliance | Medium | Medium |
| Insider misuse | High | Medium |

## With Privitty Edge

| Metric | Improvement |
|---|---|
| Unauthorized reuse | Nearly Impossible |
| Data retention violations | Almost Gone |
| Audit visibility | ↑ 100% |
| Revocation capability | Enabled |

# The Privitty Approach

Privity aligns with emerging architectures such as:

- International Data Spaces Association (IDSA)
- Data sovereignty frameworks in EU and industrial ecosystems

However, it differs by:

| *Enforcing control at the data level, not just at the connector or policy layer*

## How It Works

### 1. At the Edge (Industrial Gateway)

- Data is:
  - Encrypted
  - Tagged with ownership & policies

Example policy:

- "Only OEM can read fault logs"
- "Access valid for 7 days"
- "No forwarding allowed"

### 2. During Transmission

- Data flows via Privitty messaging stack
- Policies travel with the data

"Not just secure transport
Policy-bound data movement"

### 3. At the Consumer (OEM / Partner)

Access is enforced based on policy:

- Fine-grained visibility (no over-sharing)
- Time-bound access
- Purpose-limited usage

## 4. After Sharing (Key Differentiator)

Revocation

- Data owner can revoke access anytime
- Previously shared data becomes unusable

Auditability

- Full trace of:
  - who accessed data
  - when and how

“Share industrial data freely – without ever losing control”

privitty

info@privittytech.com
www.privittytech.com