TrustIoT.AI Security Whitepaper

Zero Trust AIoT Decision Platform

Version: v1.0

Date: 20 November 2025

Laysi Co., Ltd.

Website: https://trustiot.ai

Contact: trustiot.ai@laysi.io

TrustIoT.AI Security Whitepaper

Zero Trust AIoT Decision Platform Security Whitepaper

Version: v1.0

1. Introduction

TrustIoT.AI is a Zero Trust-based AIoT decision platform designed to help enterprises derive actionable operational insights from equipment and energy data.

This whitepaper describes the security principles and controls implemented across edge devices, data transmission, cloud storage, AI processing, and operational processes.

The platform is built on the following foundations:

- Edge: Official gateway equipped with TPM 2.0
- Cloud: Deployed on AWS infrastructure
- AI: Models and gateway services provided via Cloudflare
- Security: End-to-end Zero Trust security model

2. Security Architecture Overview

The TrustIoT.AI security architecture follows these principles:

- No implicit trust in any user, device, or network
- Every access must be authenticated and authorized
- Privileges are granted on a least-privilege basis
- All critical operations are auditable and traceable

The system is logically divided into four layers:

1. 1. Edge layer: Official gateway responsible for data collection, preprocessing, and device identity verification
2. 2. Transport layer: Encrypted communication and mutual authentication
3. 3. Cloud layer (AWS): Data storage, service execution, and access control
4. 4. AI layer (Cloudflare): Model inference, content filtering, and traffic governance

3. Data Security and Privacy

3.1 Data Categories

TrustIoT.AI primarily processes the following types of data:

- Equipment and energy-related data (e.g., meters, equipment operating status)
- System-generated analytics, insights, and reports
- System operations and audit logs

3.2 Data Collection and Processing

- Raw data is stored as-is (raw values), without overwriting or fabrication
- Derived data (e.g., aggregation, cleaning, features) is managed separately from raw data
- Data schemas and data sources are clearly labeled to support traceability and audit

3.3 Data Storage

- Data is stored in AWS and protected using encryption mechanisms
- Different data purposes (raw, cleaned, analytical results) are isolated in separate logical spaces
- Audit and operational logs are stored separately from business data

3.4 Data Retention and Deletion

- Data retention periods are defined according to customer requirements and contractual agreements
- Cleaned or temporary analytical data can be configured for automatic deletion
- Customers may request data export or deletion; the platform provides corresponding mechanisms

4. Identity and Access Management

4.1 Users and Roles

- Role-Based Access Control (RBAC) is used to manage permissions
- Roles such as administrators, operators, and viewers are clearly separated
- Shared accounts are not allowed; all operations are recorded under named identities

4.2 Authentication

- Backend access requires account credentials and, where applicable, multi-factor authentication
- Management interfaces and APIs are accessed exclusively over encrypted channels
- Administrative accounts are reviewed regularly and unused permissions are revoked

4.3 Access Principles

- Permissions are assigned according to separation-of-duties principles
- Only the minimum privileges necessary to perform a task are granted
- Direct human access to production databases for querying or modification is not permitted

5. Edge Devices and Hardware Security

5.1 Official Gateway

- TrustIoT.AI-designated official gateways are used as edge nodes
- Industrial-grade hardware design suitable for industrial and operational environments
- Integrated hardware and software management reduces configuration errors

5.2 TPM 2.0 and Device Identity

- Official gateways are equipped with TPM 2.0
- Boot process and firmware integrity are measured during startup
- Only devices that pass verification are allowed to connect to the cloud

5.3 Edge Operating Mode

- Supports offline buffering when network connectivity is unstable
- Automatically retransmits unsent data once connectivity is restored
- Includes mechanisms to detect abnormal states and self-isolate when required

6. Network and Communication Security

6.1 Encrypted Communication

- All communication between edge gateways and the cloud uses encrypted channels
- Modern standard protocols and secure configurations are preferred
- Risks such as replay attacks and man-in-the-middle attacks are assessed and mitigated

6.2 Mutual Authentication

- Gateways and cloud services mutually authenticate using certificates
- Certificates have defined lifetimes and revocation mechanisms
- Connections that fail authentication are rejected

6.3 Network Segmentation and Isolation

- Cloud services are segmented into security zones according to function
- Only necessary communication paths between services are permitted
- Lateral movement by unauthorized services is prevented

7. AI and Cloudflare Security Controls

7.1 AI Processing Flow

- Customer data is processed before being used as AI model input
- Only de-identified or minimum necessary content is sent to models

7.2 Cloudflare AI Gateway

- All model requests are routed and governed through Cloudflare
- Provides traffic control, error protection, and unified monitoring
- Reduces the risks associated with directly calling multiple external model providers

7.3 Model Safety and Abuse Prevention

- Model outputs are prevented from exceeding authorized scope
- Basic checks are applied to prompts and outputs to reduce injection and misuse risks
- Usage boundaries and responsibilities for AI functionality are defined in agreement with customers

8. Multi-Tenant Architecture and Isolation

8.1 Tenant Data Isolation

- Each customer's data is logically isolated
- Queries and reports are restricted to data belonging to the corresponding tenant
- System design prevents cross-tenant data access

8.2 Configuration Isolation

- Tenant-specific configurations (e.g., dashboards, alert rules) are managed independently
- System updates and maintenance procedures are designed to avoid misapplying settings across tenants

9. Incident Management and Business Continuity

9.1 Monitoring and Detection

- Cloud resources, API access, and critical operations are continuously monitored
- Anomalous patterns (e.g., suspicious logins, sudden traffic spikes) trigger alerts

9.2 Incident Handling

- Defined processes exist for security incident reporting, investigation, and response
- Major incidents are reported in accordance with customer contracts
- Appropriate evidence and records are preserved during investigations

9.3 Resilience and Recovery

- Cloud environments are deployed on highly available infrastructure
- Backup strategies and recovery procedures are reviewed regularly
- Fault tolerance and recovery capabilities of critical components are tested

10. Compliance and Governance

10.1 Alignment with Standards

The security design principles of TrustIoT.AI are aligned with the spirit of the following frameworks and standards:

- ISO/IEC 27001: Information Security Management
- ISO/IEC 27017: Security Controls for Cloud Services
- ISO/IEC 27018: Protection of Personal Data in the Cloud
- ISO 50001: Energy Management and Data Traceability
- International frameworks related to Zero Trust architectures

10.2 Internal Governance

- Platform changes are controlled through versioning and formal review
- Permission changes and critical configuration updates are recorded for audit
- Security policies and technical implementations are reviewed on a regular basis

11. Customer Data Rights

- Customers retain full ownership of their data
- Customer data is not used to train public or shared models
- Customer data is not provided to third parties without authorization
- The platform supports data export, deletion, or anonymization in line with contractual agreements

12. Conclusion

TrustIoT.AI is built around a Zero Trust security philosophy, combining official TPM 2.0-enabled gateways, AWS-based cloud infrastructure, and AI capabilities provided through Cloudflare to form a secure chain from edge to cloud.

This whitepaper is intended to give enterprises, system integrators, and other stakeholders a clear view of TrustIoT.AI's security design and commitments, and to serve as a reference for internal procurement, risk assessment, and information security review.