

ITU-T Technical Report

(06/2026)

XSTR.sec-iepi-AI

Security guidelines for artificial intelligence applications of an Internet of things (IoT)-based electric power infrastructure monitoring system

Technical Report ITU-T XSTR.sec-iepi-AI

Security guidelines for artificial intelligence applications of an Internet of things (IoT)-based electric power infrastructure monitoring system

Summary

This Technical Report ITU-T XSTR.sec-iepi-AI analyses security risks and threats affecting artificial intelligence (AI) applications of an Internet of things (IoT)-based electric power infrastructure monitoring system and specifies security guidelines to mitigate those risks and threats.

Artificial intelligence (AI) applications of an IoT-based electric power infrastructure (IoT-EPI) monitoring system encompass the cloud side, management side, edge side and device side of the electric power grid. It is critical for such AI applications to ensure the security of AI infrastructure, data, AI models and AI applications to support safe and efficient electric power production and operation.

Keywords

Artificial intelligence, electric power infrastructure.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

Editor:	Fangfang DANG SGCC China	Tel: +86 15838135919 Email: 1621597980@qq.com
Editor:	Boyu LIU SGCC China	Tel: +86 13939010853 Email: 13939010853@163.com
Editor:	Shaoyong GUO BUPT China	Tel: +86-18510088000 E-mail: syguo@bupt.edu.cn
Editor:	Zhaotai MENG SGCC China	Tel: +86 17621687881 Email: mengzhaotai@pku.edu.cn

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Technical Report	1
4	Abbreviations and acronyms	1
5	Overview of AI applications of IoT-EPI	2
6	Security risks and threats of AI applications of IoT-EPI monitoring system.....	4
7	Security guidelines of AI applications of IoT-EPI monitoring system	5
	7.1 Security guidelines of ED AI applications	5
	7.2 Security guidelines of MED AI applications.....	6
	7.3 Security guidelines of CMED AI applications	7
	Appendix I – Use cases for security guidelines of AI applications of IoT-EPI monitoring system	9
	I.1 Security guidelines for AI application in intelligent operation diagnosis of electric power metering devices	9
	I.2 Security guideline for AI application in intelligent inspection of power dispatching automation.....	9
	I.3 Security guideline for AI application in intelligent analysis of power-economy relationships	11
	Bibliography.....	12

Security guidelines for artificial intelligence applications of an Internet of things (IoT)-based electric power infrastructure monitoring system

1 Scope

This Technical Report provides security guidelines for artificial intelligence (AI) applications of the Internet of things (IoT)-based electric power infrastructure (IoT-EPI) monitoring system defined in [ITU-T Y.4221]. The scope of this Technical Report includes:

- Overview of AI applications of IoT-EPI monitoring system;
- Security risks and threats of AI applications of IoT-EPI monitoring system; and
- Security guidelines of AI applications of IoT-EPI monitoring system.

2 References

[[ITU-T Y.4221](#)] Recommendation ITU-T Y.4221 (2024), *Requirements of IoT-based electric power infrastructure monitoring systems*.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 artificial intelligence (AI) [b-ISO/IEC 22989]: Research and development of mechanisms and applications of AI systems.

NOTE – Research and development can take place across any number of fields such as computer science, data science, humanities, mathematics and natural sciences.

3.1.2 deep learning [b-ISO/IEC 22989]: Approach to creating rich hierarchical representations through the training of neural networks with many hidden layers.

3.1.3 machine learning (ML) [b-ISO/IEC 22989]: Process of optimizing model parameters through computational techniques, such that the model's behaviour reflects the data or experience.

3.1.4 risk [b-ITU-T Y.3539]: Effect of uncertainty on objectives.

3.1.5 security [b-ISO/IEC/IEEE 24641]: Ability of the system to withstand an attack, whether it is an intrusion, interference, or theft.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AI	Artificial Intelligence
CMED	Cloud-Management-Edge and Device
ED	Edge and Device
EPI	Electric Power Infrastructure
IoT-EPI	IoT-based Electric Power Infrastructure

MED	Management-Edge and Device
ML	Machine Learning

5 Overview of AI applications of IoT-EPI

[ITU-T Y.4221] introduces an IoT-based electric power infrastructure (IoT-EPI) monitoring system, as shown in Figure 1, to support long-term monitoring of electric power systems. IoT-EPI data is closely related to the operational status of the electric power system and may include sensitive information about sensing devices, electricity equipment and grid operation.

Artificial intelligence (AI) applications of IoT-EPI monitoring system can be divided into three parts, based on respective characteristics:

Edge and device (ED): The edge and device side mainly consist of electric power infrastructures (EPs), sensing devices and IoT area networks, responsible for IoT-EPI data collection, local processing, and preliminary analysis. Deploying edge and device AI applications of IoT-EPI on the ED side enables real-time processing of massive sensing data of IoT-EPI.

Management: The management side mainly comprises gateway devices and wide area networks, responsible for connecting the edge and device side with the cloud. It is used for device management, monitoring and scheduling of AI applications. Deploying management-edge and device (MED) AI applications of IoT-EPI on the MED side allows for recording and analysing the behaviour of terminal devices.

Cloud: The cloud side consists of data platform, responsible for large-scale data storage, in-depth analysis, and model training. Deploying cloud-management-edge-device (CMED) AI applications on the CMED side enables the cloud to store massive data, train high-performance models, and push optimized models or rules to the MED sides for real-time application.

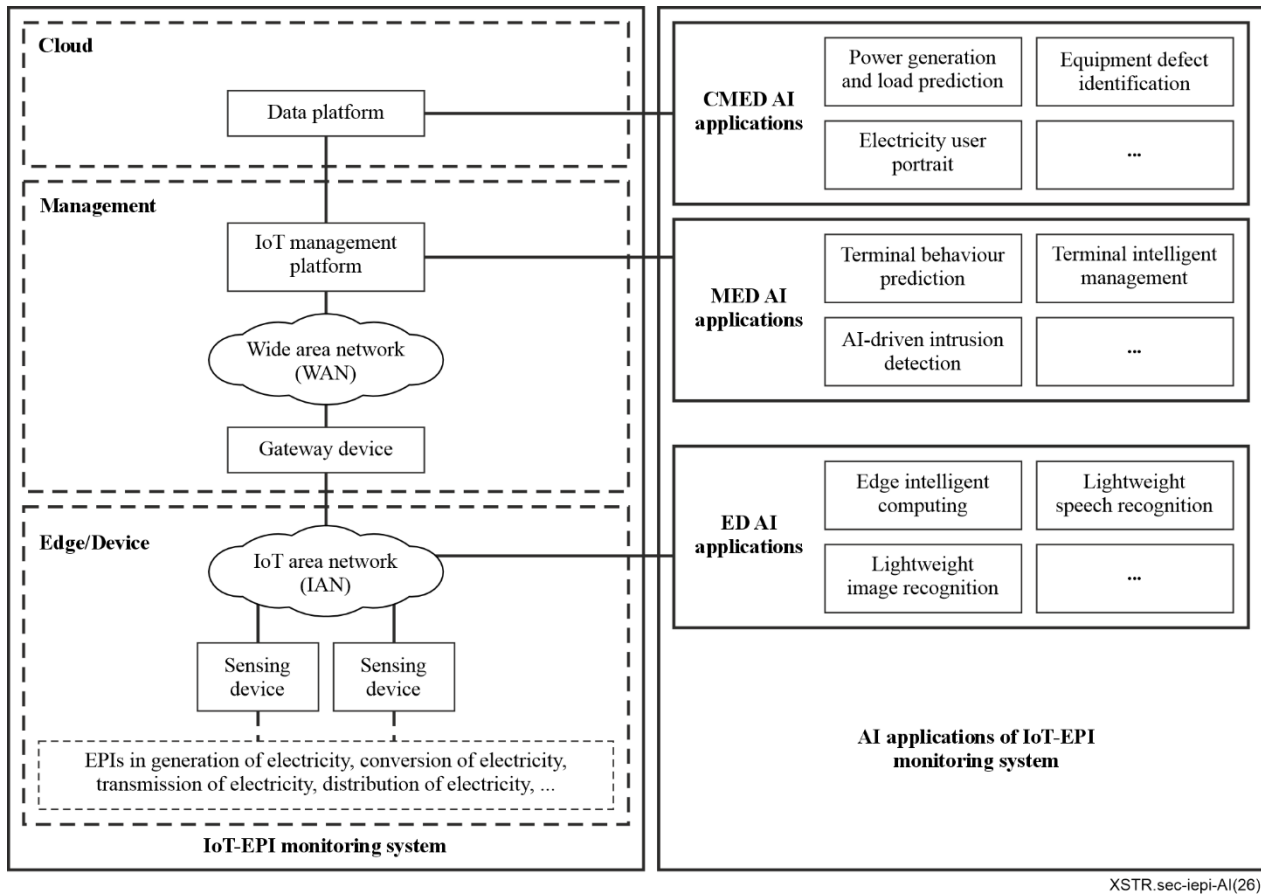


Figure 1 – Overview of AI applications of IoT-EPI monitoring system

(IoT-EPI monitoring system is defined in [ITU-T Y.4221])

A general framework for AI applications of IoT-EPI monitoring system consists of four interconnected layers (see Figure 2):

AI infrastructure layer: It establishes the foundational framework for AI operations of IoT-EPI. It delivers cloud computing services, provides hardware support, and maintains compatible operating systems to enable scalable AI development and deployment.

Data layer: It handles the collection of multi-source data from IoT-EPI. It performs critical preprocessing tasks including data cleaning, standardization, and sample management. Additionally, it enforces data security protocols to ensure integrity and compliance throughout the data lifecycle.

AI model layer: It develops core AI capabilities through model training and optimization. It implements adversarial training to enhance system robustness and supports federated learning for secure multi-party collaboration. Model version control mechanisms are also integrated to track iterations and ensure reproducibility.

AI application layer: It hosts practical implementations across IoT-EPI AI operations. Key applications include power generation and load forecasting, equipment defect identification, electricity user portrait, and power dispatching decision-making.

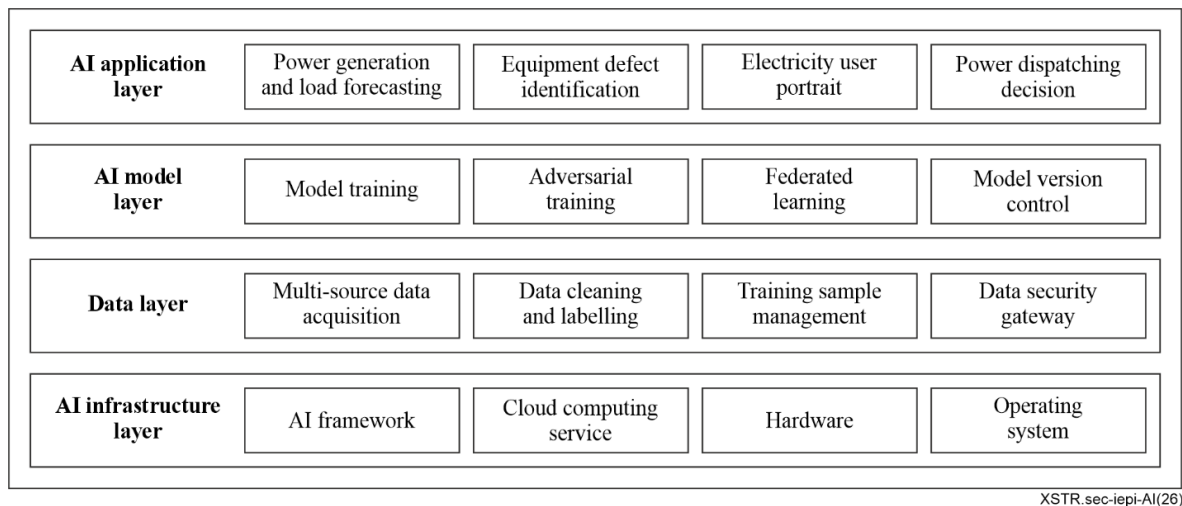


Figure 2 – General framework of AI applications of IoT-EPI monitoring system

6 Security risks and threats of AI applications of IoT-EPI monitoring system

In smart grid environments, AI applications are increasingly used for load balancing, management of distributed energy resources and autonomous fault management. These responsibilities introduce new attack vectors across the cloud, management, edge and device sides. AI applications of IoT-EPI monitoring systems enhance smart grid operation through a cloud-management-edge-device hierarchy and a layered AI framework. However, this complexity introduces risks such as edge node compromise, data tampering, model vulnerabilities and control failures that may affect safety, privacy and system stability. These risks require multilayer security defences tailored to IoT-EPI monitoring systems, as summarized in Table 1.

Table 1 – Security risks and threats of AI applications of IoT-EPI monitoring system

Subjects	Risks and threats	AI application of IoT-EPI monitoring system		
		ED AI applications	MED AI applications	CMED AI applications
AI application layer	Human-AI collaboration breakdown	○	●	●
	Autonomous decision-making failures	○	●	●
AI model layer	Model drift	●	●	○
	Model inversion attacks	●	●	○
	Lack of model interpretability	●	●	○
	Federated learning poisoning	●	●	○
Data layer	Data integrity compromise	○	●	●
	Adversarial example attacks	○	●	●
	Bias and discrimination	○	●	●
AI infrastructure layer	Cyber-physical cross-domain attacks	●	●	●
	Supply chain attacks	●	●	●
	Edge node compromise	●	●	●
NOTE – ● = critical security impact on the smart grid; ● = substantial security impact on the smart grid; ○ = measurable security impact on the smart grid.				

Human-AI collaboration breakdown: Poor interface design or over-reliance on CMED AI application of IoT-EPI may lead to electric power staff misjudgment or delayed responses on potential power events.

Autonomous decision-making failures: CMED AI application of IoT-EPI may make flawed decisions due to algorithmic defects or data biases, like erroneous electric power dispatching decision.

Model drift: Model performance of ED AI application may degrade over time due to changes in environmental conditions or evolving conditions such as transformer aging.

Model inversion attacks: Sensitive training data, like electric power grid topology information and user privacy, may be inferred from AI model outputs.

Lack of model interpretability: Black-box AI applications cannot provide credible decision-making rationales. Electric power staff cannot use the results of these AI applications to make complex orders, such as power dispatching.

Federated learning poisoning: Embed covert trigger conditions, such as specific weather patterns, to make the AI model output preset error results in power generation.

Data integrity compromise: Attackers may tamper with input IoT-EPI data or training datasets for AI applications. This could result in imbalanced power generation plans and failure to detect electricity theft.

Adversarial example attacks: Deliberately perturbed data may be fed into AI detection models, causing erroneous outputs. In power transmission and substation stages, this may lead to undetected line defects or equipment failures, potentially triggering blackouts.

Bias and discrimination: AI applications trained on biased data may perpetuate or amplify discrimination, leading to flawed decisions such as unplanned power outage.

Cyber-physical cross-domain attacks: Exploiting AI vulnerabilities to simultaneously damage physical power assets and IT infrastructure, such as triggering mechanical failures in electric switching devices via algorithmic flaws.

Supply chain attacks: Backdoors may be implanted by compromising AI development toolchains or hardware components, potentially causing widespread AI applications failures across all stages of IoT-EPI.

Edge node compromise: Attackers may hijack edge-deployed AI devices, such as inspection drones and smart meters, causing drones to collide with power lines or leak sensitive geolocation data.

7 Security guidelines of AI applications of IoT-EPI monitoring system

As introduced in clause 6, AI applications in IoT-EPI monitoring systems face security risks across the AI infrastructure, data, AI model, and AI application layers. To reduce these risks, security guidelines need to be implemented on the cloud, management, edge and device sides. These guidelines help ensure that AI applications of IoT-EPI monitoring systems operate securely and efficiently.

7.1 Security guidelines of ED AI applications

7.1.1 AI infrastructure layer

Secure boot and firmware validation: Edge devices and EPIs in IoT-EPI monitoring system are often deployed in high-voltage environments such as unattended fields or transmission towers and need to withstand physical attacks such as equipment disassembly and electromagnetic interference. Edge devices such as smart meters and drones in the ED side need firmware signature verification and resistance to physical tampering to block malicious updates to AI models.

Enhanced physical tamper-resistance and self-destruct mechanisms: The ED devices in IoT-EPI monitoring system could be designed with physical sealing and integrated tamper-detection sensors. Upon detection of unauthorized opening, the system automatically triggers key zeroization or critical AI model parameter erasure. In anti-electricity-theft application scenarios, this effectively prevents attackers from physically tampering with the internal AI model of energy consumption recognition in electricity meters.

7.1.2 Data layer

On-device real-time anonymization: Data from the ED side is directly related to the operating state of the electric grid, such as sudden current changes that may indicate a fault, and may require millisecond-level response. Sensitive data, such as user identifiers, should be dynamically anonymized in real time on ED devices such as smart meters. During visual inspections, drones should automatically blur civilian facilities and human faces in real time. Only essential equipment data, such as the condition of transmission towers and power lines, should be transmitted.

Ensuring edge computing data integrity: Lightweight cryptographic algorithms can be used to generate a hash or a message authentication code for the data processing in the ED side, ensuring that the AI data will not be tampered with during transmission. For example, an online line monitoring device performs local analysis of collected insulator leakage current data and uploads the results together with the hash value to the cloud platform for assessing the contamination level of external insulation.

7.1.3 AI model layer

Edge adversarial training: AI applications deployed on the ED side often face complex natural environments such as high temperature, ice cover, and strong winds. ED AI applications need to inject adversarial samples, such as perturbed transmission line images and current waveform containing harmonics, during model training.

Implementing model quantization and compression security verification: When compressing CMED AI models into smaller models suitable for ED side, it is essential to retain critical features that resist adversarial attacks, such as weather and temperature, and conduct specialized security tests.

7.1.4 AI application layer

Least privilege access: Data instruction in the ED side can directly control EPIs such as the relay protection equipment, and wrong instructions can cause cascading power outages. Restrict API permissions of ED AI applications for device control. API of ED AI applications can only read data such as voltage data from smart meters or pictures from drones, and only the instructions from the MED and CMED AI applications can control EPIs.

Container isolation and secure communication: Lightweight container technology can be used to encapsulate different AI applications and provide mutual isolation. Inter-application communication on the ED side needs to use encrypted channels. For example, on an edge computing gateway, the power equipment monitoring AI application, and the video monitoring AI application run in separate containers. Even if the video monitoring AI application is compromised, it cannot affect other security-critical AI applications.

7.2 Security guidelines of MED AI applications

7.2.1 AI infrastructure layer

Multiple network protocol security conversion: There are many types of electric power devices in an IoT-EPI monitoring system, and communication among these devices involves multiple industrial protocols. Secure protocol conversion and validation are needed to prevent wide-area attacks caused by protocol vulnerabilities or insecure protocol translation.

7.2.2 Data layer

End-to-end encryption: Use forward-secrecy protocols for edge-to-cloud data. Even if the wide area network in IoT-EPI monitoring system is hijacked, the attacker cannot parse the sensitive data such as substation location from the ED side.

Attribute-based access control: Restrict data access by subject attribute (e.g., user role, organization), object attribute (e.g., power plant, grid operator), environmental attribute (e.g., time, location, network status). Electric power grid involves power generation, transmission, power transformation, distribution, electricity consumption and other aspects, the participants include grid operators, power generation enterprises, users, third-party service providers, etc. Their authority requirements change in real time with the fault state, load peak, and other environments.

7.2.3 AI model layer

Model behaviour security auditing and tracing: A comprehensive log recording and security audit can be conducted for the decision-making process and output results of AI applications on the MED side. It is essential to record the AI model's input data, key inference parameters, and final decision results to ensure traceability and analysability in case of erroneous decisions. For example, when a MED-side AI model used for photovoltaic power generation prediction repeatedly exhibits excessive prediction deviations, the audit logs enable retrospective analysis to determine whether the issue lies with the input meteorological data or results from the model drift, thereby facilitating rapid root cause identification.

7.2.4 AI application layer

Dual authorization: Critical actions need approval from both CMED and MED functions before instructions are passed to the ED side to control EPIs. EPIs such as relay protection devices and transformers directly affect the security of the electric power grid, and operation authority needs to be strictly limited to prevent mis-operation or malicious attacks.

Intelligent security monitoring and automated response: An AI-based security monitoring system or intelligent agent can be deployed on the MED side. It can utilize machine learning or deep learning to analyse network traffic, system logs, and AI application behaviours. It can enable real-time detection of anomalies, automated correlation analysis of security events, and the capability to trigger predefined response strategies, such as isolating compromised powers devices or blocking malicious IPs. For example, upon detecting that a feeder automation terminal sends anomalous broadcast messages to multiple adjacent terminals within a short period, the AI-based security monitoring system can automatically generate alerts and temporarily isolate the anomalous terminal to prevent the fault from propagating in the distribution network.

7.3 Security guidelines of CMED AI applications

Security guidelines for CMED AI applications of IoT-EPI monitoring systems include the following:

7.3.1 AI infrastructure layer

Establishing a secure and controllable full-stack AI infrastructure: CMED-side deployments should prioritize AI frameworks, computing hardware and key software components that can be securely managed, verified and maintained throughout their lifecycle in order to reduce supply chain attack risks.

Cloud-edge disaster recovery: The secure operation of CMED AI applications, such as power generation and load prediction, will be related to the security of the city's power supply. In order to ensure the security of electric power grid and defend against natural disasters such as typhoons and earthquakes, it is necessary to optimize the elasticity of cloud resources of AI applications. Synchronize models/data in real time on the CMED side to achieve sub-second failover of the IoT-EPI monitoring system while reducing dependence on the centralized cloud.

7.3.2 Data layer

Multi-party computation: Power user data may reveal production patterns, such as factory scheduling or power-user profiles; therefore, enhanced privacy protection is needed. Secure multi-party computation can enable collaboration among power generation companies, power grid operators and power users while preventing each party's raw data from being disclosed. This supports the principle that data can be used for analysis without being directly visible to other parties.

Secure and compliant use of multimodal large-scale models: Deploy content security filtering and compliance review modules for the inputs and outputs of large-scale models in CMED side. These modules can prevent the generation of harmful content or the leakage of sensitive information (such as substation coordinates, equipment nameplates, and user information).

7.3.3 AI model layer

Robustness-preserving distillation: Retain attack-resistant features when compressing cloud models for ED/MED side deployment.

7.3.4 AI application layer

Ethical compliance checks: Enforce or block ethical policies via predefined rules. Electric power service has a strong attribute for serving public society, and some ethical rules need to be enforced, such as giving priority to the power supply in hospitals. At the same time, discriminatory policies such as multiple power outages and delayed restoration of power supply in specific areas need to be avoided.

Constructing a digital twin sandbox for AI decision testing: A high-fidelity smart grid digital twin environment can be built in the CMED side. It can place critical AI applications in a sandbox for security verification and attack-defence drills. For example, before executing major power dispatch actions for AI applications in the CMED side, all load transfer strategies can be simulated in the digital twin system to verify system behaviour under extreme scenarios such as renewable energy fluctuations or cyberattacks. Execution is permitted only after safety is confirmed.

Conducting cross-security-domain penetration testing: Regularly initiate red team and blue team exercises from the CMED side that simulate advanced persistent threats among CMED. The red teams can simulate attack chains progressing from compromised inspection drones in ED side to the central AI platform in the CMED side, in order to evaluate the overall defence system and remediate identified defence-in-depth vulnerabilities.

Appendix I

Use cases for security guidelines of AI applications of IoT-EPI monitoring system

I.1 Security guidelines for AI application in intelligent operation diagnosis of electric power metering devices

I.1.1 AI application description

Accurate metering devices are the source of power operation data and the fundamental basis for electricity settlement. The intelligent operation diagnosis of metering devices mainly analyses the operating status of smart electricity meters, judges whether the smart electricity meters can operate normally, and transforms the previous electricity meter replacement strategy based on service life into precise management of meter replacement according to the actual operating status of the meters. Its core functions include accurate identification of abnormal meters, intelligent traceability of fault causes, etc. This type of AI application usually needs collaborative judgment and analysis between the edge and device (ED) side and the cloud-management-edge-device (CMED) side.

I.1.2 Security considerations

Data security in ED side: Attribute-based least privilege access control for metering AI application and data: Complying with the access control guidelines in clauses 7.1.4 and 7.2.2, access permissions for metering data, AI model inference results and fault traceability functions are needed to be restricted based on subject attributes (e.g., user role, organization), object attributes (e.g., metering device scope, regional grid operator) and environmental attributes (e.g., operation time, network security status). The ED side AI application is needed to only be granted read permission of local metering data, and modification of meter operation parameters and replacement decision release is needed to only be executed through dual authorization of the CMED side system and professional management personnel, to avoid unauthorized access and malicious operation.

Data security in CMED side: Full lifecycle end-to-end encryption and privacy anonymization of user electricity data. In line with the data layer security guidelines specified in clauses 7.1.2, 7.2.2 and 7.3.2, real-time dynamic anonymization of sensitive data such as user identification, electricity consumption behaviour and time-series electricity usage data is needed to be implemented on ED-side smart metering devices. Forward-secrecy end-to-end encryption protocols are needed for data transmission from the ED side to the CMED side, and encrypted storage and strict access control is needed to be implemented for the full lifecycle of metering data on the ED and CMED sides, to prevent leakage of user privacy data and unauthorized access to core electricity settlement data.

Data security between CMED side and ED side: Data integrity verification for ED-CMED collaborative model: In accordance with the ED side computing data integrity guidelines in clause 7.1.2, lightweight cryptographic algorithms are needed to be used to generate digital digests for the pre-processed metering data and local inference results of the ED side AI model. The CMED side model is needed to complete data integrity verification before launching collaborative analysis, to prevent tampering of metering data during transmission, which may lead to abnormal meter misjudgement, fault traceability deviation, and adverse impacts on the accuracy of electricity settlement.

I.2 Security guideline for AI application in intelligent inspection of power dispatching automation

I.2.1 AI application description

The power dispatching automation system is an important carrier for core businesses of power grid operation such as operation monitoring, automatic control, and online analysis. It usually needs to

monitor dozens of substations and power plants simultaneously, and identify thousands of alarm messages, which consumes a lot of manual work and needs professional knowledge for judgment and analysis. AI-based automatic inspection can effectively improve inspection efficiency, quickly identify risk points and hidden dangers of power equipment, support hidden danger management, and ensure the safe operation of the power grid.

1.2.2 Security considerations

Model security in MED side: Full-process security audit and traceability for AI model inference and operation behaviour: In accordance with the model behaviour security auditing guidelines in clause 7.2.3, a comprehensive log recording and security audit mechanism is needed to be implemented for the whole process of the MED side inspection AI application. The input original alarm data, key inference parameters, model operation version, identification results, manual review records, and final decision execution status of the AI model are needed to be fully recorded and stored in a tamper-proof manner, to ensure complete traceability and analysability in the event of model misjudgement, missed inspection or dispatching operation accidents, and support rapid root cause location.

Model security in CMED side: Model interpretability enhancement and robustness verification: Complying with the AI model layer security guidelines in clause 7.3.3, targeted adversarial training is needed to be carried out for the CMED side intelligent inspection AI model, with adversarial samples such as perturbed alarm messages, superimposed fault signals and extreme operating condition data injected during the training process, to enhance the model's anti-interference ability and robustness. Meanwhile, the interpretability of the model is needed to be improved, and clear decision basis, feature weight and risk confidence level is needed to be provided for each alarm identification result and equipment risk judgment, to avoid the "black box" problem of the model and reduce operational risks caused by over-reliance on model outputs.

Application security in CMED side: Digital twin sandbox security verification for AI model update and strategy release: Complying with the security verification guidelines in clause 7.3.4, a high-fidelity digital twin sandbox of the power grid dispatching system is needed to be established on the CMED side. Before the update of the intelligent inspection AI model, adjustment of inspection strategies or release of new identification rules, full-scenario security verification and attack-defence drills are needed to be carried out in the digital twin sandbox. The model performance under extreme scenarios such as large-scale alarm floods, multi-station concurrent faults and cyberattack interference are needed to be fully simulated and verified, and the model or strategy can only be officially released and put into operation after safety and stability are confirmed, to prevent grid operation risks caused by model update failures.

Application security in CMED side: Human-in-the-loop dual authorization mechanism for AI-assisted dispatching decision-making: In line with the AI application layer security guidelines in clause 7.3.4 and the risk control requirements for human-AI collaboration breakdown specified in clause 7, a complete human-in-the-loop mechanism is needed to be established for the AI application. All AI-generated inspection results, hidden danger disposal suggestions and dispatching auxiliary decisions are needed to only be used as professional references for operators, and cannot be directly issued as formal dispatching instructions. The release of critical operation instructions and major hidden danger disposal strategies must go through dual authorization of CMED side model security verification and manual review by professional dispatching personnel, to prevent decision-making errors caused by over-reliance on AI outputs and missing of potential risks that can be identified by manual inspection.

I.3 Security guideline for AI application in intelligent analysis of power-economy relationships

I.3.1 AI application description

Electricity serves as a key barometer of economic development, providing critical support for decision-making by enterprises and government authorities. Traditional manual analysis involves assessing electricity consumption data from a large volume of users across diverse scopes, which can face challenges in achieving both high efficiency and the required level of accuracy. AI-based intelligent analysis of power-economy relationships facilitates the identification of electricity consumption growth characteristics, anomaly traceability, trend forecasting, and automatic report generation, thereby effectively enhancing the operational efficiency of grassroots business processes. This type of AI application usually needs collaborative judgment and analysis between ED-side data and CMED-side AI models.

I.3.2 Security considerations

Data security between ED side and CMED side: Real-time data anonymization and integrity verification for the ED side: In line with the data layer security guidelines specified in clause 7.1.2, real-time dynamic anonymization is needed to be performed on sensitive data such as user identifiers on the ED-side devices to prevent user privacy disclosure. Lightweight cryptographic algorithms are needed to generate digital digests for pre-processed electricity data and economic-related indicators, ensuring that data transmitted from the ED side to the CMED side is free from tampering and supports reliable AI-based power-economy analysis.

Data security in CMED side: Secure multi-party computation for cross-stakeholder data collaboration: Complying with the data layer security guidelines in clause 7.3.2, secure multi-party computation is needed to be applied to collaborative data analysis scenarios involving grid enterprises, power users, government authorities and other stakeholders. It is needed to be guaranteed that raw sensitive electricity and economic data of all participants remain "available but not visible" during joint analysis, so as to prevent core data and user privacy from being leaked while supporting cross-departmental intelligent decision-making.

Model security in MED side: Full-process security auditing and traceability for AI model inference behaviour: In accordance with the AI model layer security auditing guidelines in clause 7.2.3, a complete log recording and security audit mechanism is needed to be established for the inference process and output results of the CMED side power-economy analysis AI model. The model's input electricity data, economic correlation parameters, key inference logic, analysis conclusions and report generation records are needed to be fully recorded and stored in a tamper-proof manner to ensure full traceability and analysability in the event of abnormal prediction deviations or data drift.

Model security in CMED side: Model robustness verification and digital twin sandbox security validation for strategy release: Complying with the AI model layer and application layer security guidelines in clauses 7.3.3 and 7.3.4, adversarial training and robustness-preserving model distillation is needed to be carried out to retain critical anti-attack features during model compression and deployment. Before the release of model updates and economic analysis strategies, full-scenario security verification, and simulation drills are needed to be conducted in the CMED side digital twin sandbox to ensure stability and accuracy under extreme conditions such as large-scale electricity load fluctuations and abnormal economic data changes.

Bibliography

- [[b-ITU-T Y.3539](#)] Recommendation ITU-T Y.3539 (2023), *Cloud computing – Framework of risk management*.
- [b-ISO/IEC 22989] ISO/IEC 22989:2022, *Information technology – Artificial intelligence – Artificial intelligence concepts and terminology*.
- [b-ISO/IEC/IEEE 24641] ISO/IEC/IEEE 24641:2023, *Systems and Software engineering – Methods and tools for model-based systems and software engineering*.
-