Research on Security Access of Power Internet of Things Terminals Based on Edge Computing Technology

Yong Tang\textsuperscript{1,a}, Linghao Zhang\textsuperscript{1,b}, Juling Zhang\textsuperscript{1,c}, Siyu Xiang\textsuperscript{1,d}, He Cai\textsuperscript{2,e}\textsuperscript{*}

\textsuperscript{1}State Grid Sichuan Electric Power Research Institute, Chengdu High-tech Zone, Sichuan Province, China
\textsuperscript{2}School of Electrical and Electronic Engineering, North China Electric Power University, Changping District, Beijing, China
\textsuperscript{a}email: 18415820@qq.com, \textsuperscript{b}email: 16100178@qq.com, \textsuperscript{c}email: zjl725@qq.com, \textsuperscript{d}email: 280552598@qq.com, \textsuperscript{e}email: 120212201260@ncepu.edu.cn

Abstract—In view of the current lack of unified security authentication and control for the power Internet of Things terminal equipment, at the perception level of the power Internet of Things, the perception layer terminal access control, front-end authentication technology realization and terminal equipment abnormal behavior detection methods are proposed. This method enhances the communication security between power equipment and edge nodes, and ensures the safe and stable operation of the power Internet of Things.

1. Introduction
In recent years, driven by the rapid growth in global energy and power demand\cite{1}, the power grid has gradually evolved from a traditional power grid to a smart grid, from a single regional power grid to a large-scale power grid across provinces and regions. At the same time, with the rapid development of the Internet, the power grid has been transformed into an energy Internet in which energy and information are deeply coupled. In terms of equipment status monitoring, it realizes real-time monitoring of equipment operating status and environmental status on the power generation side, grid side, and customer side, and intelligent analysis is performed\cite{2}. Power generation forecasting, grid dispatching, equipment operation and maintenance, and grid smart operation are all inseparable from the power Internet of Things built by various power smart terminal equipment and transmission networks. The power Internet of Things plays an important role in promoting the realization of all-round real-time perception, fault recovery, and security control at the energy internet level\cite{3}. The traditional power Internet of Things has been developed for many years, but the power Internet of Things, especially the security research at the terminal level, is still in its infancy. Due to the lack of unified security certification and control for terminal equipment at the perception layer, the situation of network security at home and abroad has become increasingly severe in recent years, which has caused many criminals to take advantage of the virtual intrusion and use illegal equipment and viruses to invade the power network, resulting in a blackout in Ukraine, 2019 Latin American countries blackouts, etc. Therefore, how to promote the evolution of the traditional power Internet of Things to a new form of full-service perception and ubiquitous power Internet of Things, and how to fully cope with the new international situation, new risks and new challenges of the new form of the Internet of Things are the questions that the State Grid Corporation of China needs to answer\cite{4}.
2. Basic introduction to edge computing

Edge computing is a new type of computing paradigm that performs computing tasks at the edge of the network. Data computing tasks can be divided into two parts: the uplink Internet of Everything service and the downlink cloud service. The edge in edge computing refers to any computing, storage, and network resources between the path from the source of data to the cloud computing center. According to the specific requirements of different application services and actual scenarios, the edge can be one or more resource nodes on this path. The edge concept of edge computing is relative to the cloud computing center. Edge resources include a variety of devices. In the power Internet of Things, such as smart meters, non-intrusive user power load collection terminals, and line-side data collection terminals, etc.; Edge nodes are scattered nearby users, line protection and measurement equipment, have many different types of resources, and are independent of each other [5]. The purpose of edge computing is to integrate these independently distributed resources. These resources are separated in the spatial dimension, but are close to the power Internet of Things terminal in the network dimension, and can be executed at the appropriate edge nodes.

2.1 Features of edge computing

(1) Low latency
Low latency is a recognized feature in edge computing academia [6]. Because the deployment of edge computing is close to the terminal equipment of the power Internet of Things, massive data is directly processed locally, avoiding the delay and congestion caused by local uploading to the cloud, which is of great significance for businesses that require timely feedback. For example, for the relay protection equipment on the line side, when the sensor detects abnormal data, after receiving the terminal data and judging the fault, the edge node located nearby can issue the protection instruction in time, switch the line quickly, and avoid the power grid cascading failure [7].

(2) Distributed deployment
Compared with traditional centralized servers, decentralized computing nodes are distributed near terminal devices, which can process data more safely, and avoid terminal node failures caused by large-scale data tampering and attacks on cloud servers [8]. In the power Internet of Things, some terminal devices continuously upload monitoring information to the cloud center. Massive terminal devices cause a large amount of data congestion, increase the burden on the network, and affect the upload of other important services of the power grid [9]. Therefore, by deploying edge computing nodes, relying on its distributed technical advantages, the business data can be temporarily stored to the edge nodes, and when the cloud needs to detect data, the required data can be sent to the cloud.

(3) High bandwidth
Due to the distributed deployment characteristics of edge computing, simple and real-time data processing and analysis can be performed locally without uploading all data or information to the cloud, reducing network transmission pressure and avoiding network congestion caused by business uploads. Therefore, the network transmission rate can be greatly increased.

(4) High security
Since the computing node is at the edge of the network, the edge node encrypts the data after receiving the data, and then uploads it to the central node through the transmission network. Compared with traditional terminal equipment, encryption is performed close to the equipment to ensure data security from the source of the data as much as possible [10]. In the power Internet of Things, user load data and power protection service data can be encrypted at edge nodes, which is of great significance for some power services with high real-time requirements.
3. Ubiquitous Power Internet of Things Model

The ubiquitous power Internet of Things system structure is shown in Figure 1, including the perception layer, network layer, platform layer and application layer. The application layer includes the internal business and external business of the grid company, the internal business includes production operation and operation management, and the external business mainly includes integrated energy services. The platform layer mainly includes a unified data center for the entire business of the power grid and an edge management center of the power Internet of Things. The main function of the platform layer is to perform abnormal behavior detection, black and white list management, and log management for power equipment. The network layer mainly includes the access network, the backbone network, the business network and the support network. The network layer guarantees the normal data transmission and data security of each device node to the cloud center, edge node to cloud node. The perception layer includes on-site data collection components, intelligent business terminals, local communication access modules, and edge computing IoT management modules. The main functions of the perception layer include device identity authentication, abnormal behavior detection, access control, access audit, and log playback.

4. Terminal security mechanism for power Internet of Things

4.1 Power terminal equipment identity authentication

Fig. 1 Structure of Ubiquitous Power Internet of Things

Fig. 2 Schematic diagram of identity authentication process
When power terminal equipment is connected to the power Internet of Things, nodes will periodically send identity verification requests. Because the edge computing nodes in the power Internet of Things generally have small data storage space, their computing capabilities can only meet small-scale task processing. Therefore, the authentication method of challenge and response is adopted, and the joint authentication method of HASH encryption and pseudo-random number is used. The schematic diagram of the identity authentication process of the power edge equipment is shown in Figure 2.

The power terminal requests authentication, connects to the edge node by sock connection, the edge terminal checks its user name, the edge terminal responds to the terminal and sends a challenge, the power terminal responds to the challenge sent, and sends the response back to the edge server, and the edge server verifies that the device is successful. The edge terminal sends a random number to update the status information of the device, and the power terminal receives the authentication result, updates the random number, and completes identity authentication.

4.2 Access audit and log playback

![Access audit flow chart](image)

Access review is mainly to review the hardware physical address of the terminal equipment connected to the power Internet of Things, the data content request sent, and whether it contains illegal characters and other content, and save important logs uploaded by the terminal. First, determine whether the access device belongs to the white list. If the device belongs to the white list, record the requested operation and return a response. If the device is not in the whitelist, it is judged whether it is in the blacklist. If it is not in the blacklist, its characteristic value is quantified and its behavior is compared with the library. If it is a normal behavior, its request operation is recorded and the response is returned.

4.3 Abnormal behavior detection

By extracting the characteristics of the attack behavior of the power Internet of Things, the specific threshold is obtained, and a detection result is judged by comparing with the empirical threshold. The rule base matching method is adopted for detection, that is, the rule base inspection is performed within
an interval of the threshold. The flow chart of abnormal behavior detection is shown in Figure 4.

![Flow chart of abnormal behavior detection](image)

Fig. 4 Flow chart of abnormal behavior detection

The specific process of abnormal behavior detection: First, the edge node extracts device information and operation information, and compares it with the rule base in the node. If the behavior belongs to the rule base, the process ends; otherwise, the feature value is extracted and quantified, and calculate its characteristic value; if the characteristic value is less than the threshold, it is judged to be a non-abnormal behavior, and if it is greater than the threshold, the process ends.

5. Conclusion

Based on edge computing, this paper adopts the edge security access process of the power Internet of Things that combines terminal device security authentication, access audit, log playback, and abnormal behavior detection. Compared with the original traditional power Internet of Things device access process, at the edge node, relying on the edge node for device identity authentication and abnormal behavior detection, the method proposed in this paper is suitable for implementation in resource-constrained terminal devices, and can improve the equipment Certification efficiency.

Acknowledgments

We would like to express our heartfelt thanks to all those who have helped this research work. This project is supported by the company's project "Ubiquitous Power Internet of Things User Behavior Intelligent Perception and Prediction Technology Research Based on Big Data and AI Technology" (SGSCDK00XXJS2100178).
References

[1] Lu S.L., Ding J, Zhang H.B., (2021) Research and Thinking on the Standard System of Intelligent IOT Sensing Technology for New Power System. J. Electric Power Information and Communication Technology, 19(08):39-46.

[2] Liu W.Q., Tan Y.H., Deng X., (2021) End-side cloud and fog collaboration model for power cyber-physical system. J. Journal of Electric Power System and Automation, 1-7.

[3] Gong G.J., Luo A.Q., Chen Z.M., (2018) Cyber-physical system of active distribution network based on edge computing. J. Power grid technology, 42(10):3128-3135.

[4] Cai M.Y., Fen S.Y., Du H.W., (2019) Edge node perception adaptive data processing method for ubiquitous power Internet of Things. J. High voltage technology, 45(06):1715-1722.

[5] Chen L., Chen H.Z., Deng S., (2014) Research on Security Access Control Method of Electric Power Intranet Terminal. J. Electric Power Information and Communication Technology, 12(06):1-5.

[6] Hou B., (2021) Research on Surveillance Video Acquisition and Adaptive Playback System Based on Edge Computing. D. Inner Mongolia University.

[7] Lu S.L., Ding J, Zhang H.B. (2021) Research and Thinking on the Standard System of Intelligent IOT Sensing Technology for New Power System. J. Electric Power Information and Communication Technology, 19(08):39-46.

[8] Wu Y.C., Li M.L., Peng W., (2020) Security Protection Design for Edge Computing of Power Internet of Things. J. China Science and Technology Information, Z1:84-85.

[9] Zhao Z.X., Li H.F., Hou W., (2021) Research and Practice of Power Internet of Things in State Grid Jilin Electric Power Infrastructure. J. Journal of Electrical Engineering, 16(02):166-173.

[10] Li F.R., Yi Y.P., Shi W., (2021) Distribution Big Data Technology of Active Distribution Network Based on Edge Computing. J. Software Guide, 20(08):160-165.