Application Research of "Edge-Cloud Collaboration" Architecture in Security Protection of Ubiquitous Power Internet of Things

Hu Song¹, Yuhang Chen², Qingquan Dong²* and Xiaolong Wang²

¹State Grid Jiangsu Electric Power Co., Ltd. Information and Communication Branch, Nanjing City, Jiangsu Province, China
²Information System Integration Company, NARI Group Corporation, Nanjing City, Jiangsu Province, China

*Corresponding author

Abstract. With the planning and construction of the ubiquitous power Internet of Things (UPIOT), how to achieve secure connection and interaction between the platform and the terminal becomes a crucial issue. Based on cloud computing and edge computing, this paper constructs the "edge-cloud collaboration" architecture of UPIOT to meet the functional requirements of grid-side intelligent services and core-side data analysis and low-latency, high-bandwidth, and large-access performance. According to the actual deployment situation of Jiangsu electric power, the firewall and VPN application scenario security protection scheme is proposed to provide a theoretical basis for the UPIOT security protection.

1. Introduction

With the development of artificial intelligence, the world has set off a wave of digital and intelligent transformation [1]. And with the maturity of technologies such as cloud computing, big data, artificial intelligence, and edge computing, some application scenarios such as VR/AR, industrial Internet of Things, and smart terminals are strongly supported, providing a feasible solution for the traditional industry from the physical world to digital development [2]. At the same time, the power industry is also facing development: 1) The overall shape of the power grid has undergone tremendous changes, the number of connected devices and the types of equipment are large and complex; 2) With the changes in the global digital economy, enterprise services are from the pipeline to the close User transformation. The ubiquitous power Internet of Things connects the power users and their equipment, the grid companies and their equipment, the power enterprises and their equipment, suppliers and their equipment, and then connects people and things, and finally realizes the interconnection of electricity and the full use of the platform. The effect and sharing role of providing services to a wide range of users and institutions is the best solution to the challenges facing the current grid. This requires a combination of the smart grid physical world and cloud computing numbers represented by applications, computing, networking, and storage to provide high bandwidth, low latency, large access, and high security performance to meet business needs. The "edge-cloud collaboration" architecture brought about by the combination of edge computing and cloud computing will promote the construction of the UPIOT.

2. Edge-Cloud Collaborative Architecture

2.1. Cloud Computing and Edge Computing

Cloud computing adopts centralized management, with highly configured server, storage, network and management platforms to provide users with continuous and flexible IaaS, PaaS and SaaS services, creating high economic value and user service experience [3]. However, hundreds of millions of terminal accesses require faster and more secure access to resources in the UPIOT. If the physical world is directly connected
to the digital world of cloud computing, high latency and high bandwidth costs will be faced. Risks such as security and privacy, as well as lack of reliability, so relying solely on cloud computing platforms can no longer meet the performance requirements of the business.

Edge computing refers to a new computing model that performs computation at the edge of the network. This edge refers to any computing, storage, and network resources from the data source to the core data center path. It provides edge intelligence services in the vicinity, meeting industry digitization in agile connections, real-time. Key requirements for business, data optimization, application intelligence, and security and privacy protection. Cloud computing focuses on the calculation and storage of massive data, and generally does not use real-time as its core goal. Edge computing enables real-time, autonomy and collaboration of the physical world based on distributed computing.

2.2. Edge-Cloud Collaborative Architecture

The cloud computing platform that provides services such as local computing, storage, and communication to the edge of the network near the source or data source is called the edge cloud [4]. A cloud platform that centralizes computing, storage, and network resource establishment in a central data center is called a core cloud. Since the edge cloud localization handles access by the terminal access device, low latency performance of less than 20 ms can be provided.

This paper aims to build a side cloud collaborative technology architecture for the UPIOT, managing and controlling core clouds, edge clouds, IoT platforms, edge nodes and terminals. The provincial core cloud platform performs tenant management, network management, resource management, and application lifecycle management for the edge cloud. Each edge cloud is used to access and manage the Internet of Things agent device, and the edge cloud provides localized computing, network, storage and safety ability.

![Figure 1. Edge-Cloud Collaborative Architecture schematic diagram.](image_url)

2.3. Edge-Cloud Service Mode

In order to achieve side cloud collaborative work, the core cloud needs to be able to manage tenant management, computing storage management, network security management and data service management for edge clouds [5].

1) Tenant management

The core cloud can assign resource usage rights of corresponding edge clouds to different users. When performing tenant management, you can assign resource usage rights to tenants based on the types of resources provided by the edge cloud, such as virtual machines, containers, security level, geographic location, and service delay.

2) Computing storage management

Computational storage resources are the basis for the operation of the grid business system and are a prerequisite for the continuous development of integrated delivery by devops. Tenants can perform resource scheduling, configuration delivery, application-one-click deployment, service monitoring, and log viewing in the core cloud.
3) Network security management
The core cloud can orchestrate network services, define network policies, establish network service chains, decouple traditional hardware devices, rapidly distribute virtualized network functions (VNFs) to edge clouds, and conduct edge cloud network communication using SDN/NFV technology.

4) Data Service Management
The edge cloud uses its own computing storage network resources for localized data processing and responds quickly to application requests. The delay can be less than 20ms. At the same time, the data can be uploaded to the core cloud in the north direction. The core cloud saves historical global data, and can perform offline data analysis by using centralized high-performance computing performance and combine the data analysis result and the real-time incremental data analysis result to provide the user with Fast data search and other services.

3. Firewall and VPN Application Scenarios
In order to verify the superiority of the edge cloud collaborative architecture in service deployment, configuration and operation and maintenance, and in the role of UPIOT security protection, we use two scenarios of virtual firewall and VPN in multiple edge clouds.

3.1. Test Environment
A core cloud and a set of edge clouds were deployed in Nanjing, and a set of edge clouds was deployed in Suzhou. The resource scale of these cloud instances is shown in the following table. The core cloud is mainly to provide core computing and storage capabilities for important grid systems in the province. Nanjing and Suzhou as edge clouds are mainly used for terminal data collection and localization processing of power grid systems.

This paper uses the open source project OSM based on the ETSI standard framework as the network function virtualization management and orchestration (MANO) platform. The virtualized infrastructure management uses openstack as the underlying infrastructure service, which carries virtual firewalls, VPNs and various grid business system virtual machines.

| Cloud instance | Position | Scale |
|----------------|----------|-------|
| Core cloud     | Nanjing  | 139   |
| Edge cloud     | Nanjing  | 45    |
| Edge cloud     | Suzhou   | 34    |

3.2. Service Process

**Scenario 1: Creating a virtual firewall (vFW) in an edge cloud**
First, deploy the network orchestration platform in the core cloud. Here we use the automated operation and maintenance platform CMDB, which can perform tenant management, resource management and application management for multiple cloud instances. The cloud instance is deployed by the openstack platform to provide virtual machine resources. Package firewall functions into virtual machine image VNF and orchestrate virtual firewall network functions. During the orchestration service, we define the vFW northbound interface vlan103 and the two southbound interfaces vlan101 and vlan102, where vlan101 is provided for service A and vlan102 is provided for service B. First, connect the Nanjing openstack cloud instance through the CMDB platform, and then deliver the vFW network service and VNF to the Nanjing openstack cloud instance.

After the service A is deployed, the CMDB automatically starts the deployment of the virtual machine A in the IP A network. The virtual machine A communicates with the outside through the vFW. Through the policy configuration of the vFW, you can control the north-south traffic of service A. For example, you can control the source IP address of access service A, etc., so that the security protection of the edge cloud Nanjing cloud instance can be satisfied.
Scenario 2: Creating a VPN tunnel in two edge clouds
Similar to scenario 1 deployment vFW method, the CMDB first interfaces with Suzhou openstack and Nanjing openstack cloud instances. Then, the vFW network virtualization function and the VPN network service are arranged, and the two vFWs are respectively deployed to the Suzhou openstack cloud instance and the Nanjing openstack cloud instance through the CMDB. By centrally configuring Suzhou and Nanjing vFW to establish two edge cloud VPN channels, it can meet the communication needs of Service A in the cloud instance and the service A in the Nanjing cloud instance, reject the access requirements of the service B, and reach the core cloud to the edge cloud network.

4. Conclusion
In the context of smart grid and ubiquitous power internet of things, this paper studies the relationship between intelligent computing, edge computing and cloud computing, and analyses the application scenarios and functional requirements of intelligent terminals, artificial intelligence, and network security. Based on cloud computing and edge computing, "edge-cloud collaboration" architecture of UPIOT is built to meet the functional requirements of grid services on the edge side of intelligent services and core side data analysis, and low latency, high bandwidth, and large access. Performance requirements, and scenario applications in the firewall and VPN areas. In the future, the new generation network architecture combining SDN and NFV is the development trend of cloud-side collaborative computing and puts forward higher requirements in the security protection of the UPIOT station.
Acknowledgement
This research was financially supported by the Science and Technology projects of State Grid Jiangsu Electric Power Co., Ltd. (J2019123).

References
[1] Hu Pan. Proposed Development of Power Internet of Things and Key Technology Prospects [J]. Hubei Electric Power, 2019(1): 1-9.
[2] Hong Guangying. Application of Intelligent Wireless Internet of Things Technology in Jinjiang Power Information Collection [J]. Communication World (21): 189-191.
[3] Cui Ajun, Zhang Huafeng, Fan Dilong, et al. Research on Security Protection Technology of Power Internet of Things[J]. Electric Power Information and Communication Technology, 2013, 11(3):10-13.
[4] Zhao Ting, Gao Kunlun, Zheng Xiaokun, et al. Research on Intelligent Grid IoT Technology Architecture and Information Security Protection System[J]. China Electric Power, 2012, 45(5): 87-90.
[5] Liao Huimin, Xuan Jiaxing, Pei Ping. Overview of ubiquitous information security of power internet[J]. Electric Power Information and Communication Technology, 2019, 17(8).
[6] Zhang Limin, Shen Wendong, Meng Jun. Technology Application and Security Protection of Internet of Things in Smart Grid[J]. Shanxi Electric Power, 2012(4): 36-38.
[7] Wang Yi, Chen Qixin, Zhang Ning. Fusion of 5G Communication and Ubiquitous Power Internet of Things: Application Analysis and Research Prospects[J]. Power System Technology, 2019(5): 1575-1585.