Research on Cloud Platform Security Protection System for Power Plant

Xinming Yin\textsuperscript{1,2}, Yi Guo\textsuperscript{*}, Zhiwei Cao\textsuperscript{2}, Han Liu\textsuperscript{2} and Min Xiong\textsuperscript{2}

\textsuperscript{1} School of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China
\textsuperscript{2} The Third Research Institute of Ministry of Public Security, Shanghai 200031, China
Email: guoyi@ecust.edu.cn

Abstract. In the electric power industry, the information construction of IT systems is in an important period evolving to cloud computing technology and implementing digital transformation. The power cloud is a critical infrastructure for the digital construction in electric power companies. Cloud computing technology fundamentally introduces a flexible and dynamically allocated shared resource pool, and provides a way to share cloud resources different from traditional information systems, but it also brings new security risks and challenges. This paper analyses the security risks of the power cloud from the aspects of network security, host security, application security, data security, and management risks. The focus of research is on the construction of a security protection system for private cloud infrastructure in electric power companies. According to the business characteristics and important levels of business modules, the partition and domain protection design recommendations of the power cloud is proposed. An overall security protection architecture including three aspects of cloud platform self-security, cloud platform security services and cloud security operation management is presented. And specific key protection measures in the above three aspects are given, which has important guiding significance to electric power companies.

Keywords. Power cloud; cloud platform security; virtualization security; cloud platform security service.

1. Introduction

At present, cloud computing technology has been widely used in e-government, finance, telecommunications operators, the Internet and all levels of government and information industry infrastructure construction of multiple industries and groups. In the power industry, the IT system information construction is in an important phase towards the evolution of cloud computing technology and the implementation of digital transformation.

For example, a power plant proposed in its digital construction action plan to transform itself from a traditional information system to a new generation of cloud-based digital basic platform and Internet application. First it will complete the interconnection of upstream and downstream energy industry chains, then support smart power grid operation, energy value chain integration and energy ecological service capabilities, and finally make a digital power grid corporation.

Cloud computing takes virtualization technology as its core, and provides high-effective, low-cost continuous computing, storage space, and various software services through aggregation, abstraction, and scheduling of various computing resources to support various information applications [1].
Cloud computing innovates the service model to provide users with on-demand purchase and flexible expansion services. As cloud computing technology fundamentally introduces flexible and dynamically allocated shared resource pools [2], which provides a cloud resource sharing mechanism different from traditional information systems in terms of resource management [3]. While facing traditional security threats, it also brings new security risks and challenges.

This paper studies how to build a power cloud platform security protection system from the aspects of power cloud security risk analysis, partition and domain protection, cloud platform's self-security protection and the security services to be provided.

2. Security Risk Analysis of Power Cloud

2.1. Cyber Security Risks
The power cloud uses network virtualization technology to improve the utilization of network resources. Network virtualization is mainly achieved through virtual switch technology, for example virtual machines on the same physical machine can communicate directly through the virtual switch. The service flows do not pass through the physical switch, so that the traditional network security protection boundary disappear, and traditional security protection such as firewalls and intrusion detection systems measures no longer take effect [4].

2.2. Host Security Risks
The power cloud uses server virtualization technology, and each virtual machine has its own independent operating environment. Server virtualization technology brings a series of new security risks, the virtualization technologies such as virtual machines, containers can be broken through, so that security threats can be passed between virtual machines and host machines. Attackers can directly use the specific hotkeys in the host computer's operating system to kill virtual machine processes, monitor virtual machine resource usage or shut down virtual machines. They also can use network sniffer tools to capture incoming and outgoing data traffic from network cards. Once an attacker gains control of a virtual machine, he can use the virtual machine to attack other virtual machines or its host machine.

2.3. Application Security Risks
The power cloud has a large number of users that provides services for the departments, branch companies, and power end users, etc. so as to bring serious challenges to user ID authentication and access control. Improper resource isolation between business departments may result in unauthorized access to business application systems, information leakage risks and attack risks for cloud tenant business application systems. The customer service website is an important part of the power cloud. There are also various web attacks in the power cloud. Once hackers use bug to tamper with the content of the web page or insert malicious code, the service of power users will be seriously affected.

2.4. Data Security Risks
Cloud tenants and user data are concentrated in the cloud. Improper protection of data transmission, storage and isolation may cause user data to be lost or destroyed. In a cloud environment, the files or data transmitted in a virtual environment may be intercepted; cloud users obtain image files or other users’ private data after escaping from a virtual machine; it is uncontrollable due to drift of sensitive data storage; data security and isolation is not strictly obeyed, resulting in malicious users be able to access other users’ data and other issues.

2.5. Management Responsibility Risk
For the cloud computing model, the three entities of the cloud computing platform as the management entity, the operating entity, and the data security responsibility entity are different, and it is difficult to define their responsibilities. In a cloud computing environment, tenants migrate their data and business
systems to the cloud losing direct control over these data and services. While the cloud service department can access, utilize, or manipulate tenant data. The internal personals of the cloud service department may unauthorized access and use of tenant data, that increases the risk of tenant data and business.

3. The Deployment Model of Power Cloud and Partition Protection

3.1. The Deployment Model of Power Cloud

Service is the essence of cloud computing, which includes two entities: cloud service provider and cloud tenant. The main cloud deployment models include private cloud, public cloud, community cloud, and hybrid cloud [5]. At this stage, private cloud model is populated in the cloud construction of power plants. For example, a power plant proposed in its digital construction action plan to build a private cloud platform realizing the unified management of IT resources across the entire network; making use of public cloud resources actively and steadily on the premise of ensuring data security.

This paper focuses on the analysis and research of a cloud platform security protection system for a private cloud of a power plant.

3.2. Divisional Protection

According to the principle of divisional protection of the power grid security, based on the business feature of the power system and the importance level of the business module, following the requirements of the national network security level protection, the security level should be accurately divided and the security area should be reasonably divided. Therefore, the protection of the power cloud should be divided into different regions [6]. As shown in figure 1, first, the enterprise management cloud is deployed in the information intranet area, the public service cloud is deployed in the information extranet area, and logical isolation facilities are deployed between the two areas. Secondly, domain-based protection is implemented for cloud platforms, protection levels for cloud-based application systems is determined according to the requirements of graded protection, power enterprise network security management and control plans, security domains are divided to ensure cloud-based application systems at different protection levels are classified into logically isolated different security subdomains.

![Figure 1. Power cloud partition protection.](image)

4. Power Cloud Platform Security Protection System

4.1. Cloud Platform Security Architecture Design

As shown in figure 2, Cloud platform security architecture is logically divided into two levels: cloud
platform's self-security and security services. The cloud platform itself should have capabilities such as physical network security, host and virtualization security, cloud platform management security and other security protection etc. while it is necessary to realize the abstraction and pooling of security resources based on the traditional security technology architecture. The cloud platform provides security service capabilities for the upper-layer IaaS, PaaS, and SaaS services, and protects the services of cloud.

4.2. Cloud Platform Security

4.2.1. Physical Network Security: Physical network security is the foundation of the cloud platform's self-security and the premise for ensuring the safe and stable operation of physical servers and virtual machines. For the cloud platform, the internal security domain of the cloud platform should be differentiated according to the service feature, identify the business plane, storage plane, and management plane, solidify the network behavior pattern of each region, and prevent the penetration of network attacks.

Chain The physical network security technical measures of cloud platform include access control, intrusion prevention, security audit, communication security, traffic cleaning, traffic audit, malicious code prevention, etc.

For physical network security, the following security protection measures need to be implemented:

1. Implement network isolation through technical means, strictly check the cloud platform network boundary, and prevent unauthorized access.

2. Check the network traffic of authorized users, detect abnormal behaviors in the cloud platform and cloud platform business access traffic, and prevent attacks and damages to the cloud platform network and host.

3. Abstract modeling for a variety of network traffic to prevent DDOS attacks, such as FLOOD attacks, CC attacks, to prevent the system from being unavailable due to resource exhaustion.

4.2.2. Host and Virtualization Security. The host security of the cloud platform involves the security reinforcement, security protection, access control and trusted computing technologies of the host system. As an important part in the cloud platform, the virtual machine carries different business applications. For the safe and reliable operation of cloud platform, they should be taken into account such as isolation, security mirroring, security key protection, operation monitoring, virus prevention, and high availability.

For mainframe and virtualization security, the following security protection measures need to be implemented:

1. Isolation of physical resources and virtual resources should be provided so that each virtual machine can obtain relatively independent physical resources, and can shield virtual resource failures, to ensure that a virtual machine does not affect the host machine and other virtual machines in case of

![Figure 2. Cloud platform security architecture.](image-url)
a crash; different Isolation of CPU instructions, memory isolation, network isolation, and storage isolation between virtual machines, virtual machines, and host machines should be guaranteed.

(2) Monitoring methods should be used, such as setting up monitoring on the Hypervisor or lower level, output information such as configuration, process, and access logs, to effectively detect intrusions; mandatory access control measures taken to limit tenant virtual machine resource access permissions and timely measure Hypervisor integrity.

4.2.3. Cloud Management Platform Security. For the cloud management, the security technical measures of the platform include access control, security audit, communication security, interface security, web protection, residual information protection, etc.

The following security protection measures need to be implemented with emphasis:

(1) The cloud management platform must be accessed only by the access key authentication.

(2) The internal components communication of the cloud platform should adopt secure communication methods such as HTTPS, and the transmission channel should be encrypted by TLS.

(3) Anomaly detection for HTTP requests can effectively prevent malicious network intrusion behaviors such as webpage tampering, information leakage, and Trojan implantation.

(4) The memory of the virtual machine needs to be cleared before released or reallocated to other virtual machines. The virtual machine user’s disk needs to be cleared before released or redistributed to other users.

4.3. Cloud Platform Security Services

The cloud platform security service adopts the method of pooling security resources to deliver the original hardware security equipment in the mode of cloud service, and drains through the core switch to draw the cloud service traffic of cloud platform users to the security resource pool for cleaning and filtering [7].

By security resource management, public security services such as virtual firewalls, web application firewalls (WAF), virtual application vulnerability scanning systems, virtual bastion machines, virtual database audit systems, and virtual host protection components are provided on the basis of cloud platforms.

(1) Virtual firewall

The capabilities can be accomplished, such as dynamic packet filtering capability based on state detection, access control capability based on application layer, and policy control capability on data flow in virtual environment.

(2) Web application firewall

For the Web server, they are performed such as Http/Https traffic analysis, protection against SQL injection, XSS and other attacks, achieving CSRF, website stealing and other Web unauthorized access protection, achieving Web malicious code protection capabilities.

(3) Virtual application vulnerability scanning system

Vulnerabilities detection and discoveries are implemented for application-layer security: supporting web vulnerability libraries commonly used, be capable of web application security vulnerability detection, Webpage-Trojan and dark chain detection.

(4) Virtual Fortress

It implements multiple audit capabilities such as character protocol, graphics protocol, file transfer protocol, database protocol and so on.

(5) Virtual database audit system

By analysis of database protocols, special audits are conducted on database operations.

(6) Virtual host protection component

For the physical host and virtual host carrying cloud computing resources, the anti-virus capability of the host can be realized, that is timely detection and discovery, timely isolation, and then timely killing.
4.4. Cloud Platform Security Operation Management
Cloud platform security operation management mainly includes cloud platform situation awareness, security OM (operation & maintenance), and security audit.

1) Situational awareness
Sort out all assets and business systems in the cloud platform, analyze the version and operating status of assets, analyze network behavior based on security logs and network traffic data, and realize unified management and global monitoring for security events [8].

2) Safe operation and maintenance
Provide a unified and automated secure OM portal.
Provide unified account management, unified ID authentication, unified authority management, and unified interface management. Prevent illegal users from accessing and controlling core instructions and etc. by safe OM.
Prevent malicious operations and misuse.

3) Security audit
Centralized management and analysis are conducted to review the environment and activities of operational events with the help of the security audit mechanism that each component distributed on the cloud platform.

5. Conclusion
Power cloud is an important infrastructure for the digital transformation of power plants, and plays a huge role in power plant construction, OM, management services, customer service, etc. Power cloud security protection is the key work of power monitoring system security, which is related to economic development and social stability, closely related to the production and people life. This paper analyzes the security risks of power cloud construction in terms of network security, host security, application security, data security, management responsibilities, etc., and proposes a security protection architecture for power cloud platforms based on private cloud deployment models, focusing on the cloud platform itself security, the cloud platform provides security services for tenants, and the cloud platform's secure operation and maintenance management explains and proposes security recommendations.

Acknowledgments
The projects funded by this paper are: National Key Research and Development Program (2018YFC0807105, 2018YFC0807106); Shanghai Science and Technology Talent Program (17XD1420400).

References
[1] GB/T 35279 2017 Information Security Technology Cloud Computing Security Reference Architecture.
[2] Shen L, Wang D and Xuan J 2018 Cloud security risk analysis and evaluation technology of electric power information system Telecommunication Science 34 (02) 153-160.
[3] Li B, et al. 2018 Research on the resource security management mechanism for trusted cloud computing Journal of Cyber Security 3 (02) 76-86.
[4] Tian Z and Yan L 2019 Research on security risk issues based on cloud computing applications China Internet (10) 50-51.
[5] GB/T 31167 2014 Information Security Technology Cloud Computing Service Security Guide.
[6] Zhang J, Tang H, Liu W, et al. 2020 Reference architecture of the telecom network security protection system for cloud network convergence Telecommunication Science 36 (05) 10-15.
[7] Lu K, Yu Z and Huang B 2020 A requirement-aware security service platform based on virtual-physical integration Information Technology and Network Security 39 (04) 19-23.
[8] Li Q 2019 Design of Security Situation Awareness System Based on Cloud Platform (Tangshan: North China University of Science and Technology).