An analysis of power grid enterprises' information security system under cloud environment

Hongjie Shen[1], Min Li[1] and Zhuoqun Li[2,a]

[1]*Information and Communication Branch, State Grid Jiangxi Electric Power Company, Nanchang, Jiangxi, China*
[2]*Business School, University of Shanghai for Science and Technology, Shanghai, China,*

Abstract. This paper, in combination with power grid enterprises' information construction guidelines in China's 13th Five-Year Plan, and based on the realization of cloud computing in the enterprises, conducts an in-depth analysis of the scope and security risks for enterprises to implement cloud computing, to propose a key technology applications-based cloud security framework of power grid enterprises. In addition, the paper expounds how to construct the cloud framework, and analyze the methods of applying key technologies, thus offering reference for state-owned enterprises of the same kind to construct a security system under cloud environment.

Keywords: cloud; cloud environment; power grid; enterprises; information security system.

1 Introduction

Cloud computing, which is a new model of network resources use and delivery, is now vigorously promoting the great changes in information technology; also it will inevitably exert direct influence on the development process of information security, and promote another major innovation of it[1,2,3]. The traditional protection system, whose theoretical basis is security model analysis and verification, whose major component is information security product, and whose main goal is safety domain construction, will be under great shock. After the Stuxnet Worm Event[4], cyberspace is also increasingly seen as the "fifth space" in addition to after land, sea, sky, outer space, and its security has risen to the national level[5]. Under the cloud environment, centrally-managed cloud computing center will become a key objective of malicious attackers, and it will face security risks more severe than ever due to the large size of the system and unprecedented degree of openness and complexity.

2 Application of cloud computing technology in power grid enterprises

State Grid Corporation of China (hereinafter referred to as SGCC), as a pillar enterprise of national energy, spared no effort and has accomplished the construction of the "SG-ERP" platform[6], which, based on the concepts of centralized platform, business integration, decision-making intelligence, and safe use, implements information system technology throughout the 6 major core links of smart power grid, namely, power generation, transmission, distribution, use and control. In a word, information system has become an indispensable link that sustains the development of smart power grid[7].

[a] Corresponding author : dandanli2002@163.com

During the 13th Five-Year period, power grid enterprises will forge "SG-ERP V3.0", to achieve the integration of business, data and information. As the focus of information construction, cloud computing is as defined as new technology that can promote corporate technical reform and innovation. During this period, cloud computing technology is needed to realize intensive management, flexible extension, and demand-based distribution of basic resources, to achieve the goal of infrastructure as a service, improve resource use efficiency and lower business costs; besides, cloud computing technology is needed to realize platform virtualization, modularization and servitization, to achieve the goal of platform as a service and offer swift support for business applications; furthermore, cloud computing technology is needed to establish business application cloud, to achieve the goal of software as service, conduct business cloudization, and meet the need of business innovation for multi-scene application. The core is to achieve the integrated platform that supports “SG-ERP V3.0" system, and the cloud services of business application system.

3 Analysis of the cloud security of power grid enterprises

To realize the cloudization of integrated platform and business application system, in essence, is to use virtual technologies to conduct quick deployment of basic resources including network, hosts, terminals, business application system, and system data resources, so as to provide the dynamically-created and highly-virtual application services and data resources to the 6 major links of smart power grid production and operation. Therefore, for power grid enterprises, cloud security means the realization of the security of integrated platform and business application system.

3.1 Analysis of the cloud security of integrated platform

Power grid enterprises should forge the integrated platform in accordance with the concept of "1 network, 1 portal and 9 components". Its contents should include basic resources like network and hosts, enterprise portals, identity permissions platform and visualized platform and other components. After the cloudization of these components, the security issues arising are mainly from physical layer, network layer, system layer, application layer, storage layer, and data layer.

As for physical layer, the security of machine room should be fully considered, including a total of six areas: room decoration, electrical systems, air conditioning systems, access control systems, surveillance systems, fire systems; as for network layer, the priority should be put on the confidentiality of the data transmission, network reachability, and then, defense against DOS / DDOS attacks, DNS spoofing identification, etc; as for system layer, full considerations should be given to the security of virtual machine, including its own security, access control security, permissions management, communication security, transfer security; As for application layer, consideration should be given to process integrity test, vulnerability management, code security review; as for storage layer, integrity and file / log management and disaster recovery management should be considered; as for data layer, consideration should be given to the security of database system itself, privacy and access control of enterprise business data, backup and destroying of important data.

3.2 Analysis of the cloud security of business system

During the 13th Five Year, the focus of business system construction of power grid enterprises is to build a “3 Clouds” system integrating production, enterprises and services. The core of cloud security of business system is to realize the security of business system data. Under the cloud environment, data of business system is usually stored in a shared virtual environment, which, on most occasions, can be accessed by anyone. Some malicious attackers can locate the service environment vulnerabilities through studying the basic framework and service software under the safe environment of cloud computing, and upload malicious codes; besides, internal employees may also intentionally or unintentionally destroy data, thus causing the unavailability of data. Furthermore, data under cloud

environment is featured by large size, complex access environment, various computing types, making it more easily exposed with vulnerabilities; once attacked, great damage will be caused.

On the business system side, while promoting the “3 Clouds” system, we pay full attention to the privacy, confidentiality, integrity and availability risks of system data.

4 Key technology applications-based cloud security of power grid enterprises

SGCC’s SG-ERP system, which covers the country's 25 provinces, autonomous regions and municipalities, is a huge information system network. During the 13th Five Year, its cloud computing technologies is characterized by wide range, various applications and large data volume. Thus, in accordance with its actual application situation, the author proposed “Key Technology Applications-Based Cloud Security Framework of Power Grid Enterprises”. see Fig. 1.

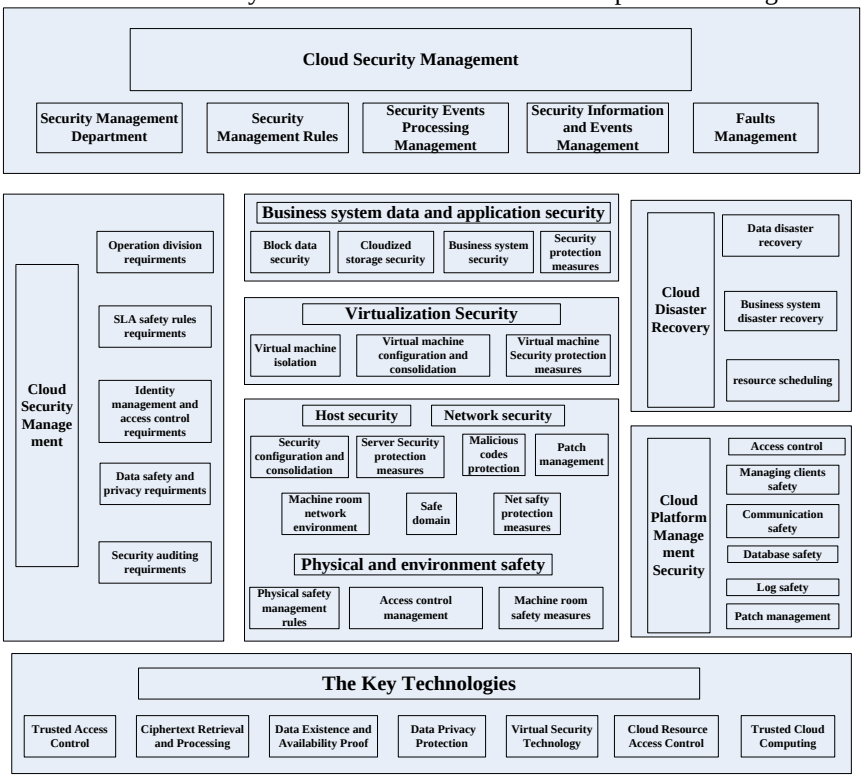

Figure 1. Key Technology Applications-Based Cloud Security Framework of Power Grid Enterprises

The framework, based on the actual application features of the construction, management and operation and maintenance of power grid enterprises, covers cloud security to security management, safe operation and maintenance, cloud disaster recovery, cloud management platform, business system and application security, virtualization security, integrated platform security (host security, network security, physical environment security), while key technologies is the mainline that goes throughout enterprise cloud security.

4.1 The construction of cloud security framework

The key of Cloud Security management is to prepare the new management system under cloud environment, establish security events processing procedures and standardize security information,

time management and fault management, with secure organization as the basis, and key technologies as the guide.

As for cloud operation and maintenance, we should select the established 3-line operation and maintenance mechanism as the basic framework, define the division of operation and maintenance responsibilities of various levels under cloud environment, and cloudize SLA security clauses and requirements; besides, we should establish the identity management and access control requirements of cloud model, and standardize data security and privacy management; Furthermore, we should determine cloud security auditing requirements, as well as its scope and process.

The focus of business system data and application security should be firstly on how to realize the cloudized storage of data under the premise of the security of stored block data, and construct the technical protection system of cloud storage security under the guidance of key technologies; and secondly on how to extract system security requirements, and prepare and apply the system security protection measures according the feature of progressive increase in distributed application of business system under cloud environment.

Virtualization technology is the foundation of cloud technology to be applied, and its own security should be focused on the following aspects: isolation, configuration and consolidation among virtual machines, safety management of virtual machine images, communications security under virtual environment, virtualization and the unified management of physical security equipments, visualization and the security protection measures of the virtual layer.

An integrated platform is the basic hardware support for power grid enterprises to deploy and implement information system. Under the cloud environment, security in 3 respects, host security, network security, physical and environmental security is its major component. To achieve the host security under cloud environment, basic security protection measures of servers should be established, the protection measures against malicious codes should be developed, and security configuration and consolidation, as well as patch update management should be executed as a routine. For network security, what we should care most should be the security of the network environment of machine room, including the temperature and humidity of equipment operation, and the execution of routine equipment inspection system; and then, we should divide safety domains that are adequate in number and easy to be managed according the actual situation of cloudized applications, to rely on security equipment, access control list so as to establish and constantly strengthen the protection measures among various safety domains. As for physical and environmental security, cloudized upgrade and improvement should be done on the established physical security management, including temperature and humidness control, backup power security, lightning protection, fire safety, to further tighten access control, to improve safety measures of machine room in accordance with the high requirement on centralized management under the cloud environment.

In terms of cloud disaster recovery, we should take the current regionally-centralized disaster recovery center in power grid enterprises as the basic framework, to consolidate the protection system for data disaster recovery technologies, improve the disaster recover ability of business system, and establish new resource scheduling mechanism in combination with the characteristics of cloud computing applications.

With regard to cloud platform management, while paying attention to communication security, database security, log safety and the other basic elements of platform security, we should improve the security capacity of access control, newly construct the security control mechanism for the client side, apply patch management into various levels of cloud platform management, and reduce the security risks caused by vulnerabilities.

4.2 Key technologies

4.2.1 Trusted access control

Trusted Access Control addresses the issue on how to implement access control of data object using non-traditional control means. Its core content is to achieve cryptography-based methods; the main

problem it is facing is to revoke permission. An effective plan is to create an online semi-trusted online authorization list in the CA center of power grid enterprises, which, based on the attribute of unique ID and Not gate structure of users, can realize the permission revocation of specific users. Under the cloud environment, it is an effective technical means to achieve trusted access control to, on the basis of cryptography, adopt the method of hierarchy key generation and allocation to implement access control, and use property-based encryption algorithms or proxy re-encryption methods.

4.2.2 Ciphertext retrieval and processing

Power grid enterprises, which are the pillars of national energies, involves relatively large amount of secret business data. Under the cloud environment, these data have become Ciphertext, making large amount of corresponding retrieval methods ineffective. Thus we should adopt the method of secure indexing, to establish secure indexes by ciphertext keywords, and retrieve indexes and consult whether the keywords exist. Then, we should conduct comparison of each word in ciphertext based on the ciphertext scanning method, so as to achieve accurate ciphertext retrieval and processing.

4.2.3 Data existence and availability proof

Under the cloud environment, the centralization of large-scale data of production and operation of power grid enterprises causes the massive upsurge in burden on communications. Users, on this occasion, will find it impossible to verify its correctness without downloading the data. Thus, we must judge with high-level confidence probability, to see whether remote data is complete, the typical work of which include: User-oriented method of separately verifying the data retrievability proof, publicly verifiable data holding certificate method (PDP).

4.2.4 Data privacy protection

The protection of cloud data privacy of power grid enterprises, involves not only every stage of data life circle, but also even the security management of the life circle of power grid production and business activities. American scholar ROY.I, proposed a privacy protection system Airavat, which prevents authorized private data from leaking in the process of calculating map reduce, while supporting the automatic deciphering of the calculation results. There, it is considered an effective method to achieve enterprise data privacy protection under cloud environment.

4.2.5 Virtual security technology

Virtual technology is the core of cloud computing. An effective but not highly efficient method is to assign each mapping file of virtual machine to each customer application. It must enjoy high integrity, and require of a mechanism that is provided with secure sharing. The mapping file management system realize the functions of file access control, source tracking, filtering and scanning, etc. and detect and fix security breach issues.

4.2.6 Cloud resource access control

In the power grid enterprise cloud security framework, different safety domains are reserved for different cloud applications. Each safety domain manages local resources and users. When users need cross-domain resource access, authentication service in the domain boundaries should be equipped, to carry out unified identity authentication management of users who access shared resources. For resource access that crosses many domains, as each domain has its own access control strategy, a public shared access control strategy should be developed to conduct resource sharing and protection.

4.2.7 Trusted cloud computing

In recent years, the hot spot of cloud security domain is to introduce trusted computing technology into the cloud environment, to create reliable ways of providing cloud services. The mainstream way is a trusted cloud computing platform, TCCP, proposed by the American Santos.N. Based on this platform, the cloud service side of power grid enterprises can provide terminal users with an execution environment similar to a sealed box, to ensure the confidentiality of customer virtual machines. Also it also allows users to check whether the services at service sides are safe before starting virtual machines.

The author, in combination with the internationally new key cloud computing technologies, proposed his insights on the above key technology applications of cloud security framework of power grid enterprises. In practice, however, we might need to act according to the differentiated features of cloud applications in various districts for rational matching, in order to build a suitable cloud security framework.

5 Conclusion

Cloud computing application is the key technology implemented by SGCC in its informatized platform "SG-ERP V2.0" during the 13th Five Year Period. Although it has broad prospects for development, the security problems it face, are unprecedented whether in terms of management level or technical level. The managers of enterprise informatization, should make efforts to explore corresponding solutions. Only when secure running of the cloudized system is ensured, can the security of power grid production be ensured, and the grand goal of creating a global energy network be possibly achieved.

References

1. Armbrust, Michael, et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010): 50-58.
2. Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." *Information Sciences* 305 (2015): 357-383.
3. Rittinghouse, John W., and James F. Ransome. *Cloud computing: implementation, management, and security*. CRC press, 2016.
4. PU. Shi, CHEN Zhouguo, Zhu Shixioang. “Analysis and Protection of Stuxnet virus.” *Netinfo Security* 2 (2012): 40-43.
5. Stark, Holger. "Stuxnet Virus Opens New Era of Cyber War." *Spiegel Online*8 (2011).
6. Wang Dewen, Song Yaqi, Zhu Yongli. “Information platform of smart grid based on cloud computing.” *Automation of Electric Power System* 34 (2010): 7-12.
7. JIANG Daoz huo , SHE NTU Gan g , LI Haixiang , et al .”Significance and roles of standardized basic information in developing smart grid.” *Automation of Electric Power Systems* , 33 (2009):1-6 .