Towards Cloud Computing Security Considerations in Smart Grid

Shouming Ma, Chunlei Yu, Wei Gu
Research and Development (Technology) Center
Shanghai Zhixin Electric Co., Ltd.
Shanghai, P. R. China
{mashouming, yuchunlei, guwei}@sgepri.sgcc.com.cn

***Abstract*—Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. The cloud computing technology is especially suitable for handling series of problems in smart grid. However, the development of cloud computing technology is currently at its infancy, especially with many security issues to be addressed. In this paper, we first present the overall architecture of cloud computing applications in smart grid. After that, we analyze some security risks that cannot be avoided in the private cloud environment. Finally, we propose a unified security protection system framework and give some practicable security protection suggestions.**

Keywords-cloud computing;cloud security; smart grid

I. INTRODUCTION

With the continuous development of strong smart grid technology, the future data and information in power system will show explosive growth, which will undoubtedly bring huge challenges for the running and advanced analysis of the system [1]. How to promote internal information aggregating and sharing among the State Grid headquarters and provincial companies and other organizations, and achieve unified configuration, precision management and multi-task concurrent computing so as to realize the conversion to service mode is a primary problem to be solved.

Cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet [2, 3]. Cloud computing could aggregate originally distributed resources together, and then provided as a service to the audience to achieve the group operation, intensive development, lean managements and standardized construction. How to promote internal aggregation and sharing of the State Grid Corporation headquarters and network companies, provincial companies and other organizations, unified configuration, precision management, teamwork, multi-task concurrent computing, data and application service mode conversion company information the problem to be solved [4, 5].

Therefore, the characteristics of the company's business applications are very much in line with the cloud computing service models and technology models. Adoption of cloud computing can be achieved not only the company's centralized data storage and sharing, and ultimately data mining, business intelligence, decision support analysis, the coordinated development of the business of production, can also help the company to convert the data services to enhance the value of services, information fusion.

Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. However, these new technologies also bring new information security issues [6, 7]. Through the constructing of the power system secure cloud computing platform, we can effectively integrate the existing computing resources to provide powerful computing and storage capacity to support a variety of analytical computing tasks.

This paper is organized as follows: section II introduces the application architecture of cloud computing in smart grid. Section III discusses security threats present in the cloud computing environment. Section IV presents a proposed secure architecture for cloud implementation based on our experience of implementing a cloud. Finally, section V gives the conclusion and possible future work.

II. APPLICATION ARCHITECTURE OF CLOUD COMPUTING IN SMART GRID

Without a doubt, the strong smart grid represents the future development direction of state grid. The construction of the strong smart grid is not just the traditional power grid upgrade and renovation of facilities, but a deeper, more comprehensive grid operation and business model upgrades. Fig. 1 shows the cloud computing applications overall architecture in strong smart grid.

The electricity infrastructure resources were pooled by virtualization technology and the infrastructure facilities were unified managed through IaaS. In accordance with the needs of the business system, the resources were dynamically assigned to the business system. Simultaneously, the PaaS support management platform abstracts and summarizes the common needs of the IT support system to form certain service capabilities, and provide these capabilities to business systems as API.

A. Basic Resources Layer

This layer is mainly the cloud computing physical and logical devices, including management tools, middleware, database, and virtual resources. A large number of physical devices in cloud computing were distributed in different geographical locations. The internal WAN of power system connects all of these devices.

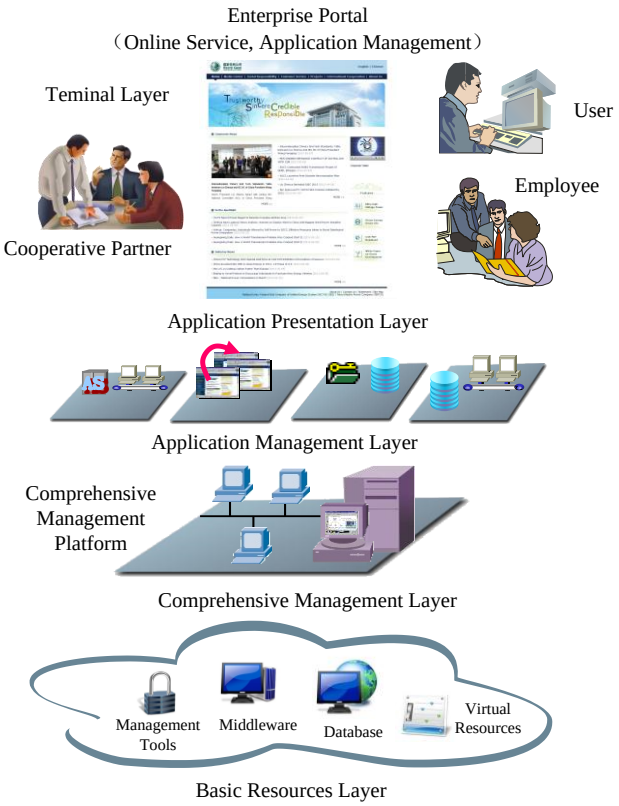

Figure 1. Overall architecture of cloud computing application in smart grid.

B. *Comprehensive Management Layer*

This layer through the integrated power management platform, based on virtualization and distributed software and hardware architecture, tries to integrate various management modules (such as security management module, billing management module, and self-service management module) at the same time without loss of flexibility.

C. *Application Management Layer*

This layer provides a wealth of innovative features for grid enterprise and simplifies the IT processes for users. The cloud computing in strong smart grid includes a wide variety of applications. It contains some standard applications, such as e-mail services, OA system, simultaneously also contains lots of custom service applications, such as the power interactive marketing, CRM, and ERP. Furthermore, it contains some advanced applications, such as smart grid cloud computing search engine, power scheduling, and decision analysis.

D. *Application Presentation Layer*

This layer provides a useful interface for power cloud computing users. It delivers a collection of various services, and was required to be able to coordinately complete these application functionalities.

III. SECURITY RISKS OF CLOUD COMPUTING IN SMART GRID

According to industry characteristics of Grid Corporation, the cloud computing construction will give priority to private cloud. The private cloud is usually constructed for sole client; consequently it can provide the most effective control to data, security and quality of service.

In case the construction of cloud computing in Grid Corporation starts from local or private cloud, the security issues can be reduced to some extent because the private cloud access is strictly regulated and the majority of the entire process stage is effectively covered by traditional security means. However, there are some security risks that cannot be avoided in the private cloud environment.

A. *Security Construction Strategy Risk*

During the period of “Eleventh Five-Year Plan”, by means of the SG 186 engineering implementation, the multi-layered information security layout was established in the management information region, and plays an increasingly important role in the information technology and business applications.

However, the construction and deployment of private cloud environments in the future will exert an influence on existing information security pattern. The private cloud is a large-scale distributed network environment, and their deployment may span multiple geographical partitions. This kind of private cloud deployment across multiple security regions will blur the existing information security protection boundary, and bring new security issues in information system protection. Therefore, before the construction and deployment of private cloud environments, those potential security risks should be take full account and scientific and rational constructing strategy should be carefully designed in the same way.

B. *Business Outsourcing Service Risk*

Without doubt, the construction of private cloud in smart grid is large-scale system engineering. Owing to enormous developing efforts and developing technical limitations, it is impossible to the Grid Corporation to entirely bear all the developing and deploying work. During the developing and constructing process of private cloud platform, part of the work will be assigned to some outsourcing companies. As a result, the security risk during the entire private cloud construction will greatly increase.

Therefore, those possible outsourcing services security risks should be fully assessed in the course of constructing a private cloud platform. Appropriate control measures must be developed to ensure the level of quality and security requirements of the developing tasks and to reduce those outsourcing services security risk.

C. *Virtualization Security Risk*

No matter public cloud or private cloud, virtualization is a core technology of cloud computing field. Those

virtualization products are also indispensable to the constructing and deploying of cloud computing platform.

The virtualization technology introduced two issues to the field of information security: on the one hand, virtualization technology improves the level of security of the traditional computing environment to some extent; on the other hand, some features of the virtualization technology bring new security challenges to traditional information security.

Among all security risks faced by the private cloud environments, the virtualization security is one of the biggest security risk differences with the traditional information security. Therefore, the advantages and disadvantages and the level of security of various types of virtualization technologies and products should be fully assessed before the constructing and deploying of Grid Corporation private cloud. Those mature technology solutions and related products should be chosen to reduce the virtualization security risk.

D. Important Data Leakage Risk

Similar to the public cloud, private cloud environments is also facing the risk of leakage of important business data. The important business data leakage in the private cloud environments occurs mainly at two places: First, the static data leakage risk; Second，the dynamic data leakage risk.

The so-called static data is that stored in the data center, cloud application memory and the terminal memory environment. These data can easily be accessed by the non-authorized user and lead to leakage problems. The so-called dynamic data is that in the transmission process in private cloud environments. The dynamic data also can leak by means of user account hijacking and network channel monitoring. Therefore, when the important business data migrates to a private cloud platform, both static data and dynamic data will face the leaking and tampering security risks.

E. Business Continuity Risk

At present, State Grid has completed the building of three disaster recovery center. A large number of business data was stored in these data centers. In the future, State Grid will achieve the goal of application-level disaster recovery. These measures greatly increase the availability of existing business data and applications, but they still cannot guarantee the permanent availability of business data and applications.

In the same way, the future private cloud environments will face the same business continuity considerations. When the important data was transferred to private cloud environments, how to ensure the private cloud environments continuously provides data access and applications running services is a major security risk.

F. Malicious Behavior Tracking Risk

Various types of security incidents are inevitable after the private cloud platform was established. So, how to analyze these security incidents and track the path of malicious behavior in order to discover the private cloud environments security threats and confirm the incidents responsibilities.

As previously mentioned, the private cloud is ultra-large-scale distributed network environments, which contains a large number of physical infrastructure, host system and business applications. In these environments, the traditional means of tracking malicious behavior may no longer meet the needs of the private cloud. Therefore, the tracking of malicious behavior in ultra-large-scale network and application system is another security risk. If this is not well handled, the tracking problem of security incidents will necessarily occur.

IV. CLOUD COMPUTING SECURITY SCHEME FOR STRONG SMART GRID

On the whole, to achieve the cloud computing security in strong smart grid, as shown in Fig. 2, at least five multi-level challenges need to be addressed: security standards, security technology, security assessment, security management and security legal construction.

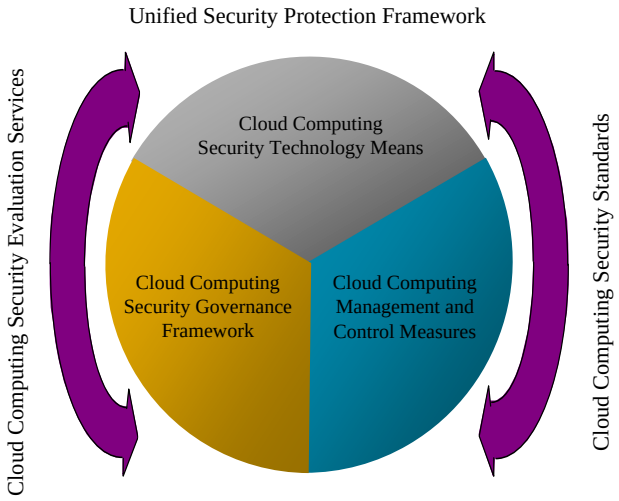

Figure 2. Unified security protection framework in smart grid

1) Cloud computing security standards system

The establishing of safety guiding criteria and evaluation system is an important pillar of the cloud computing security. Cloud computing security standards is an important criterion to measure the cloud computing secure service capabilities of service provides whether in line with the user security objectives. Moreover, it also is the major reference of security service provides to build security services.

2) Cloud computing security technology framework

The current cloud computing platform at all levels (such as the network layer, host layer and the Web application layer) exists diverse security threat. However, these common security issues have been adequate research in the field of information security, and have lots of mature product. Cloud computing security research needs to focus on analyzing and resolving those challenges of data security and privacy protection that posed by the cloud computing service model, virtualized dynamic management mode and multi-tenant shared operating model.

3) Cloud computing security management framework

Cloud computing is a double-edged sword. Generally speaking, security management framework includes user identity management, access control management, encryption key management, security event management, et al. Only by fully understanding their business model and features, carefully designing the security regulatory requirements, and establishing comprehensive and sophisticated management system, we can effectively take advantage of the advantages of cloud computing.

4) Cloud computing security governance framework

Cloud security governance includes five key control entries: governance and enterprise risk management, legal and electronic evidence discovery, compliance and audit, information life cycle management, portability and interoperability.

V. CONCLUSIONS AND FUTURE WORK

With the gradually strengthening of the power system interconnection and the continuous development of the long-distance transmission system, the ultra-large-scale power systems that can cover a wide area are emerging. As the constant expansion of the power system and the growing complexity of the system structure, the security assessment, security and economic operation, system control become more and more difficult. The rise of cloud computing is rapidly changing the landscape of information technology, and ultimately turning the long-held promise of utility computing into a reality. The constructing of cloud-based core computing platform of power system can effectively solve the important challenges of the future power system encountered in computing and information processing.

To construct the secure core computing platform in strong smart grid, we propose a detailed unified security protection system framework of power cloud computing. At last, we also give some practicable security protection suggestions. However, the construction of secure computing platform is a very complex problem in practice. Many security issues must be seriously premeditated. In the future, the development of a cloud computing security protection system prototype will promote relational research to deal with above-mentioned problems.

REFERENCES

[1] X. Li, W. Wei, Y. Wang, Z. Mu and W. Gu, "Study on development and technology of strong smart grid", Power System Protection and Control, Vol. 37, No. 17, Sep., 2009, pp. 1-7.

[2] M. Armbrust, "Above the clouds: a Berkeley view of cloud computing", UC Berkeley Technical Report, 2009.

[3] Q. Zhang, L. Cheng, R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, May 2010, Vol. 1, Issue 1, pp. 7-18.

[4] J. Zhao, F. Wen, Y. Xue, Z. Lin, "Cloud computing: implementing an essential computing platform for future power system", Automation of Electric Power System, Vol. 34, No. 15, Aug., 2010,pp. 1-8.

[5] Q. Li, M. Zhou, "Research on cloud computing in smart grid", Computer Science, Vol.38, No. 10A, Oct., 2011, pp. 432-434.

[6] A. R. Metke, R. L. Ekl, "Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, Vol. 1, No. 1, Jun. 2010, pp: 99-107.

[7] Y. Chen, V. Paxson, R. H. Katz, "What's New About Cloud Computing Security?", Technical Report, No. UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.