Research on cloud computing in the key technologies of railway intelligent operation and maintenance sharing platform

Shu-dan Yu

1School of Electron and Information, Nanchang Institute of Technology, Nanchang, 330044, China

*Corresponding author’s e-mail: ysd@nut.edu.cn (ORCID: 0000-0001-7364-5887)

Abstract. Cloud data center has become a trend and mainstream, and the first phase of the main data center of National Railway Group has been completed, and the main data center also adopts cloud computing technology. Compared with traditional data centers, cloud data centers bring great convenience of unified and flexible resource scheduling to railroads, but also bring many new security risks. Therefore, the study of security architecture and key technologies for cloud data centers becomes an important requirement for securing railroad cloud data centers. While cloud computing brings convenience to railroads, it also brings new security risks. By studying the information security model, we construct a cloud security architecture that meets the actual situation of railroads. In terms of responsibility, according to the level protection responsibility sharing model should be divided into cloud-based security protection and cloud platform foundation protection; in terms of construction, according to the sliding scale model, it should overlap and evolve, and gradually complete the security construction in several stages of infrastructure security, deep defense, active defense and threat intelligence.

1. Introduction

In the process of railroad informatization development, information technology has been widely used in various railroad industries [1]. However, with the increasing speed of train operation, the expanding scale of passenger and freight transportation, and the diversification of train operation environment, the requirements for intelligent railroad information system are also getting higher and higher [2]. With the continuous development of communications network technology, Big Data Cloud Computing has become one of the key technologies for innovation in various areas and provides a means of development for the intelligence of railway operations and maintenance in China. In actual railway operations, each relevant business system generates a large amount of business data that provides powerful data support for the smooth development of railway operations and maintenance work [3]. With the expansion of the scale of operation and the increase of train running speed, the requirements for railroad traffic safety and transportation efficiency are getting higher and higher, so each operation and maintenance system is also being expanded and upgraded to meet the daily maintenance needs [4]. Although the function of the existing operation and maintenance system is gradually improved, but there are still the following problems: ① electrical professional communications, signal systems for operation and maintenance management, there are a large number of information islands, the openness of the system is poor, professional, system interconnection and interoperability difficulties; ②
communications, signal system construction standards are not uniform, software/hardware, operating systems, a wide range of databases, repeat investment problems; ③ part of the system technology is old, the application of new technologies, flexible expansion difficulties, bandwidth limitations, mobile broadband access difficulties; ④ digitalization, intelligence is low, the level of intelligent perception is limited, the coverage is not comprehensive, restricting intelligent applications and intelligent decision-making aids [5]. In addition, the field maintenance personnel still mainly rely on manual completion of data collection, screening, analysis and other work when dealing with faults or carrying out daily maintenance, which is difficult to meet the expansion and the increasing amount of data operation and maintenance needs; at the same time, the large amount of data generated by the railroad systems in the long-term practical application process contains huge application value, which can provide strong data support for the future development of the railroad, relying only on It is difficult to exploit these data manually [6]. Therefore, an intelligent analysis platform is needed to integrate these data resources and realize automated analysis of daily maintenance and fault conditions, while deeply mining the value of these big data.

Comprehensive collection of intelligent operating and maintenance system computing and artificial intelligence and other technologies and data based on "technical and maintenance regulations" based on data from Big Data, cloud-based rail communications, signals and other related processes, By comprehensively identifying the system status for intelligent analysis and processing, we achieve synergies between personnel, equipment and the environment and lead the operation and maintenance of electric rail services in the mode of profound change [7]. The system has more comprehensive detection, wider networking, more accurate early warning analysis and more detailed intelligent processing functions for the construction of modern electrical systems that are safe, efficient, intelligent and environmentally friendly for the central monitoring of electrical processes. Maintenance, process control, planning orders and other functions to improve the daily operation and maintenance of railways, the ability to analyse and process errors quickly [8]. The intelligent operation and maintenance system of the railway is divided into five main parts. Figure 1 shows intelligent detection networks, broadband and ubiquitous connectivity, intelligent electrical operation and maintenance cloud computing centres, intelligent computing and maintenance centres, intelligent analyses and subsidiary decisions as well as the overall structure.
The intelligent operation and maintenance system of the railway collects surveillance data from the underlying intelligent sensor network and transmits data for processing and storage via ubiquitous networks to cloud computing centres to enable connection and interoperability between different systems. It performs comparative and correlation analyses using big data analyses to identify fault points quickly and accurately, and provides information for supporting decisions [9]. In addition, the system integrates the monitoring and detection data of each intelligent sensing network and conducts deep mining analysis on these data, which can predict the operation trend of related services and provide pre-warning for equipment that may fail [10]. The system can establish standardized templates, correlation analysis and deep learning based on multi-dimensional and multi-disciplinary data from the cloud computing center, which can achieve active learning and self-improvement [11]. In this paper, while cloud computing brings convenience to railroads, it also brings new security risks. By studying the information security model, the cloud security architecture that meets the actual situation of the railroad is constructed. In terms of responsibility, according to the hierarchical protection responsibility sharing model should be divided into cloud-based security protection and cloud platform foundation protection; in terms of construction, according to the sliding scale model, the evolution should be superimposed to gradually complete the security construction of several stages of infrastructure security, deep defense, active defense and threat intelligence.

2. Intelligent operation and maintenance system

2.1. Intelligent sensing network
Intelligent sensing network integrates sensing, information processing and communication, and disseminates information with a certain level of knowledge in a digital way, with self-diagnosis, self-
correction and self-compensation. The sensing technology is developing in the direction of intelligence, networking, miniaturization and integration. Railroad intelligent sensing network consists of train sensing network, station sensing network and line sensing network, etc., as shown in Figure 2. Each sensing network consists of monitoring and testing systems of each equipment, which obtains information on the operation status and working environment of the relevant equipment, and data the equipment information involved in operation and maintenance work, transforming from abstract working form to concrete quantifiable analysis data. With the rapid development of high-speed railroads, more and more information is needed for daily operation and maintenance, so the problem of insufficient coverage of the perception network becomes more and more prominent. The collection of big data in intelligent operating and maintenance systems and the development of intelligent perception networks go hand in hand, so that each perception system information about position, movement, vibration, temperature, Moisture and even changes in the wireless magnetic environment in the air are measured and transmitted. Time generates a huge amount of data, but since this data is the basic information of intelligent operating and maintenance systems, it is important to develop and apply intelligent perception networks.

![Figure 2. Railway Intelligent Sensing Network](image)

2.2. Broadband and ubiquitous connectivity

Broadband and ubiquitous connectivity enable users to use any network to exchange information with anyone or anything at any time and place, providing ubiquitous and omnipresent information services and applications based on actual application requirements and using existing and constantly updated network technologies. It is the nerve center connecting the intelligent sensing network and the cloud computing center in the system, and is the basis for interconnection and data convergence of all systems. The schematic diagram of broadband and ubiquitous connection is shown in Figure 3, which ends with various function-rich and wide-coverage perception networks. The ubiquitous basic network is the nerve system connecting the intelligent sensing network and the cloud computing center. It is through this nerve system that the intelligent sensing network and the cloud computing center can
effectively integrate data resources, efficiently interact and collaborate, and realize the working efficiency of intelligent operation and maintenance.

![Diagram of Broadband and Ubiquitous Connectivity](image)

**Figure 3.** Broadband and Ubiquitous Connectivity Diagram

3. Cloud computing security model

3.1. Hierarchical protection responsibility sharing model

Information systems using cloud computing technology are referred to as cloud computing platforms in the class's rules of protection. The cloud computing platform consists of facilities, hardware, resource extraction control layers, virtualized computing resources, software platforms and application software. Software-as-a-service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) are three basic cloud computing service models. In different service models, cloud service providers and cloud service customers have different controls over computing resources, and the scope of controls limits security accountability. In the infrastructure-as-a-service model, a cloud computing platform consists of a configuration, hardware and resource extraction control layer. In the platform-as-a-service model, cloud computing platforms include facilities, hardware, resource extraction control levels, virtualized computing resources and software platforms. In the software-as-a-service model, cloud computing platforms include facilities, hardware, resource extraction control levels, virtualized computing resources and software platforms. As the demand for dynamic and resilient network security is growing, it is widely acknowledged that there are no "magic drugs" in the area of network security defence that can kill at once." Silver bullet technology. Based on the "sliding scale" model proposed by the U.S. cybersecurity research institute SANS, several domestic capability vendors have extended and expanded after reaching a consensus, and further proposed a superimposed evolutionary cybersecurity capability model. The model divides network security capabilities into five categories: infrastructure security, defense in depth, active defense, threat intelligence and countermeasures, and clearly states that all categories of capabilities are necessary for a complete network security defense system. From the perspective of technical development, these five categories of capabilities have an objective order of appearance, but from the perspective of the actual confrontation, the various categories of capabilities are indispensable, and there is no possibility of "upgrade and replacement" between categories, but must be superimposed together and continuously evolve to ensure effectiveness,
integrity and sophistication at the same time; from the perspective of the value achieved by each type of capability, there is a support and dependency relationship between each other, and only when the more basic capabilities are better implemented, the higher-order capabilities can be guaranteed; from the perspective of construction and implementation, the construction conditions of the more basic capabilities will be relatively mature, and as the construction process evolves, the higher-order capabilities will have the construction conditions, for example, the enterprise must have experienced the basic For example, an enterprise must have experienced the construction of basic security and deep defense and achieved better results before it can build a situational awareness capability system that can effectively export. The countermeasures are not considered at the enterprise level.

3.2. Cloud data center security architecture

The cloud security architecture can be vertically divided into cloud platform foundation protection (orange) and cloud-based security protection (blue) based on the hierarchical protection cloud security responsibility sharing model. The cloud platform foundation protection is the security protection of the physical environment and physical equipment that constitute the cloud platform; the cloud-based security protection is the security protection of the logical network, virtualization, service delivery and data of the cloud platform. The green part is the unified security platform. According to the sliding scale model, the cloud security architecture can be horizontally divided into infrastructure security, deep defense, active defense, and threat intelligence, which are overlapping evolutionary relationships to form the cloud security architecture. Infrastructure security refers to the security mechanisms implemented in the structure of the enterprise IT infrastructure and its own components, as well as the security mechanisms implemented in the enterprise application systems. These mechanisms themselves have the dual meaning of security protection and system assurance, and although they are not directly "one-to-one" or "tit-for-tat" with threats, they can effectively shrink the attack surface of the IT environment and increase the depth of network security defense. It can also provide a solid foundation for other levels of network security capabilities in the dynamic integrated network security capability system. Combining this model with the annual profitability of the railroad sector will burst forth with amazing power, as shown in Figure 4, by analyzing the model, whose revenue generation and profitability rise year by year.

Defense-in-depth is a security mechanism that is attached to the infrastructure of IT infrastructures such as networks, systems, desktop environments, etc. to achieve systematic defense-in-depth capabilities. In contrast to dynamic active defense, it is a static defense mechanism, based on the basic principle of "failure-oriented design", which shrinks the attack surface layer by layer, mainly to effectively consume the attacker's resources and keep out some common attackers. It can provide basic capability support for dynamic active defense and intelligence-driven defense in the later levels. The centralized security management platform extracts the assets and performance information of the entire data center, including the cloud management platform; the security data platform aggregates the data from the cloud management platform and reports it to the situational awareness platform, which uses big data, artificial intelligence and other technologies combined with external threat intelligence research and analysis to send the perceived threats and security events to the centralized security management platform; after the centralized security management platform receives the threat information and security events, it conducts security event analysis and disposal and sends the security policy to the cloud management platform. After receiving the threat information and security events, the centralized security management platform analyzes and disposes of the security events and sends the security policies to the cloud management platform and other security devices for active defense. Through the above steps, a proactive defense posture is formed based on the external threat intelligence and internal information for research and judgment, threat perception, and automatic issuance of security policies for disposal.
Figure 4. Changes in O&M costs for management systems with security architecture

4. Conclusion

By studying the security risks faced by cloud computing, this paper proposes a security architecture for cloud data centers based on the responsibility sharing model and the sliding scale model of SANS, covering infrastructure security, defense-in-depth, active defense and threat intelligence. The architecture not only completes the design of the longitudinal defense of the virtualized dynamic network in the cloud environment, but also investigates the technical solution of active defense in the cloud environment in conjunction with the iron fence. The next work should continue to study cloud security in depth and combine with engineering in-depth practice to cope with new risks brought by cloud computing and ensure the safe and stable operation of the railroad business.

References

[1] Thoben, Klaus-Dieter, et al. (2017) "Industrie 4.0' and Smart Manufacturing—A Review of Research Issues and Application Examples." International Journal of Automation Technology, 11(1): 4-16.
[2] Du, Pei, et al. (2017) "Research and Application of a Novel Hybrid Forecasting System Based on Multi-Objective Optimization for Wind Speed Forecasting." Energy Conversion and Management, 150: 90-107.
[3] Wang, Jianzhou, et al. (2018) "Research and Application of a Hybrid Forecasting Framework Based on Multi-Objective Optimization for Electrical Power System." Energy, 148: 59-78.
[4] Wang, Zhijian, et al. (2019) "Research and Application of Improved Adaptive MOMEDA Fault Diagnosis Method." Measurement, 140: 63-75.
[5] Zhao, Jinxing. (2017) "Research and Application of Over-expansion Cycle (Atkinson and Miller) Engines - A Review." Applied Energy, 185: 300-319.
[6] Li, Hongmin, et al. (2018) "Research and Application of a Combined Model Based on Variable Weight for Short Term Wind Speed Forecasting." Renewable Energy, 116: 669-684.
[7] Wang, Jianzhuo, et al. (2017) "Research and Application of a Combined Model Based on Multi-Objective Optimization for Multi-Step Ahead Wind Speed Forecasting." Energy, 125: 591-613.
[8] Xiao, Liye, et al. (2017) "Research and Application of a Hybrid Wavelet Neural Network Model with the Improved Cuckoo Search Algorithm for Electrical Power System Forecasting." Applied Energy, 198: 203-222.
[9] Zhao, Liang, et al.(2019) "Research and Application of Acoustic Emission Signal Processing Technology." IEEE Access, 7:984-993.

[10] Zhao, Xuejing, et al.(2019) "Research and Application Based on the Swarm Intelligence Algorithm and Artificial Intelligence for Wind Farm Decision System." Renewable Energy, 134:681-697.

[11] Zhong, Rui, et al.(2018) "Research and Application of Pervious Concrete as a Sustainable Pavement Material: A State-of-the-Art and State-of-the-Practice Review." Construction and Building Materials, 183:544-553.