Brief Analysis for Network Security Issues in Mega-Projects Approved for Data Clusters

Shizhan Lan[1,2(✉)] and Jing Huang[3]

[1] School of Software Engineering, South China University of Technology, Guangzhou 510006, China
lanshizhan@gx.chinamobile.com
[2] China Mobile Guangxi Branch Co., Ltd., Nanning 530012, China
[3] EVERSEC (Beijing) Technology Co., Ltd., Beijing 100191, China

Abstract. Network security is an important guarantee for Mega-projects approved for data clusters. It is necessary to comprehensively improve the network security awareness, monitoring, early warning, disposal and evaluation capabilities of Mega-projects approved for data clusters. It makes a comprehensive analysis on the network security issues in Mega-projects approved for data clusters from dimensions of computing facility security, network facility security, combination and scheduling security, network operation service security, data security, network situation awareness, etc. It is set up gradually evolving atomic power security capabilities for building a ubiquitous security network computing brain. It identifies data assets in an active and passive ways, sorts out data assets through in-depth scanning and information completion, supports the formation of preset templates according to AI (artificial intelligence) models, regular matching, keywords, combination rules, etc., classifies and grades data according to data sensitivity, and visually displays them in the form of charts. It forms a multi-layer architecture system that includes the collaborative scheduling of computing networks on the control side, the perception of network convergence on the data side, management and the scheduling of computing resources on the service side, realizes the interaction and supervision of the whole process, all elements and the whole industry chain of computing scheduling, has functions of security perception, monitoring, early warning, disposal and evaluation, and improves the security perception and linkage monitoring capability of cross data center and clusters. Gradually, it builds a coordinated threat handling capability.

Keywords: Mega-projects approved for data clusters · Network security · Network situation awareness · Network security computing brain · Atomic security capability · AI model

1 Introduction

"Mega-projects approved for data clusters" refers to building a new computing power network system integrating data center, cloud computing and big data [1] to orderly guide the computing power demand in the east to the West. According to the demand of

W. Lu et al. (Eds.): CNCERT 2022, CCIS 1699, pp. 38–50, 2022.
https://doi.org/10.1007/978-981-19-8285-9_3

computing power, China promotes the echelon layout and overall development of data centers from east to west; Accelerates the gradual and rapid iteration of “Mega-projects approved for data clusters”. In order to comprehensively boost the development of new data centers, it builds an intelligent computing ecosystem with new data centers as the core, and gives full play to the enabling and driving role of the digital economy, the Ministry of industry and information technology has formulated and issued the three-year action plan for the development of new data centers (2021–2023) [2], and makes every effort to ensure the promotion of the “Mega-projects approved for data clusters” project.

Network security is the premise for the development of “Mega-projects approved for data clusters”. The "Mega-projects approved for data clusters" project urgently needs to improve the ability of network security perception, monitoring, early warning, disposal and evaluation in an all-round way, accelerate the security protection level of data resources in the whole life cycle, improve the ability of computing power security monitoring and scientific scheduling, and cope with the transformation of network attacks from static analysis to dynamic perception, post disposal to prior prevention, single point prevention and control to global joint prevention.

It is oriented to “Mega-projects approved for data clusters” and meets the scenarios of massive data processing and scientific computing; The training reasoning scenario of artificial intelligence model for east digital west training. Promote the successful implementation of the project of “Mega-projects approved for data clusters”, accelerate the transformation of data centers, and provide new momentum for high-quality economic and social development.

2 General Analysis of Computing Power security

For the construction of the security system of the “Mega-projects approved for data clusters” project, it is necessary to refine the security assurance objectives, clarify the access standards for security technical means such as security situation monitoring, traffic protection and threat disposal, deepen policy reform measures and major engineering suggestions in terms of data resource protection and computing resource monitoring and scheduling, and promote the application security of data resource circulation. As the core task of the construction and application of “Mega-projects approved for data clusters”, network security focuses on building a multi-level collaborative supervision platform and monitoring system for basic networks, data centers, data center clusters, cloud platforms and application enterprises, and improving the ability of “Mega-projects approved for data clusters” project to serve economic operation monitoring and industrial digital transformation monitoring.

The architecture of computing power network consists of three levels: computing power infrastructure, arrangement management and operation service. The infrastructure layer consists of computing infrastructure and network infrastructure to form a new computing network integration infrastructure, and build a flexible and agile computing base and a fully connected intelligent network at the cloud edge. The arrangement management layer realizes the unified arrangement and intelligence of the calculation network by building the brain of the calculation network. The operation service layer

creates a new operation service system and business model by using technologies such as computing power trading, multidimensional dimension and computing power grid connection. In this architecture, safety runs through the whole process, and improving safety endogenous capability has become an important development goal. This paper will analyze the relevant network security issues from the above dimensions.

The overall goal is to build a network security value system of "Mega-projects approved for data clusters" and provide refined, ubiquitous and original twin security services; Build a ubiquitous security computing network brain, provide synchronous "pay as you go" security experience, transform application-based into task-based, and realize differentiated security experience of more refined process. Realize near source defense mode based on twin computing power mode, and realize super edge plus near source side defense mode (Fig. 1).

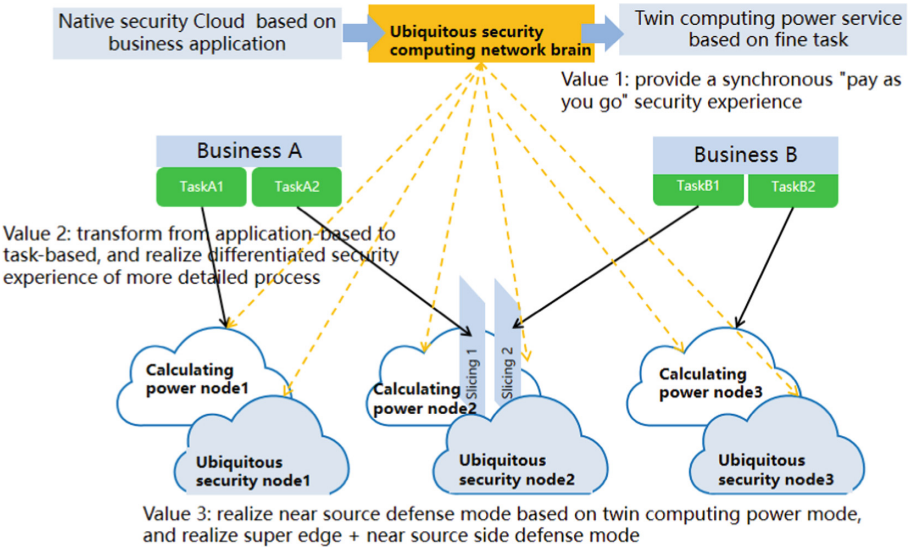

Fig. 1. Ubiquitous security computing network brain

With the rapid development of computing network technology and the continuous integration with Internet+, industrial Internet, big data, cloud computing and other new technologies, more and more information assets provide services with the help of Internet technology. At the micro security capability implementation level, they build a gradually evolving atomic capability security means to protect network security from all dimensions (Table 1).

Table 1. Atomic security capability table

Name of atomic security capability	Atomic security capacity of corresponding resource pool
Host asset discovery	Security asset management system -> host asset discovery
Software asset identification	Security asset management system -> software asset discovery
Web vulnerability scanning	Web vulnerability scanning
Host vulnerability scanning	Vulnerability scanning
Web page tamper proof	Web page tamper proof
Weak password scanning	Terminal detection and response -> weak password scanning
Webshell scan	Terminal detection and response -> webshell scanning
Baseline configuration check	Terminal detection and response -> safety baseline check
Terminal access control	Terminal detection and response -> host network access isolation
Configuration reinforcement (consolidated patch management)	Terminal detection and response -> configuration reinforcement
Document monitoring and protection	Terminal detection and response / Web page tamper proof
Terminal data leakage detection	Terminal detection and response -> terminal data leakage detection
Access behavior audit	Terminal detection and response -> access behavior audit
Terminal intrusion detection protection (combining terminal threat detection and host intrusion detection)	Terminal detection and response -> Terminal intrusion detection / protection
Backup recovery	Terminal detection and response -> backup and recovery
Host Forensics	Terminal detection and response -> host certificate
Terminal antivirus	Terminal detection and corresponding -> anti virus
Network access control (combined network attack suppression)	Next generation Firewall -> access control

(*continued*)

Table 1. (*continued*)

Name of atomic security capability	Atomic security capacity of corresponding resource pool
Network address translation (NAT)	Firewall -> network address translation
Network isolation switching	Firewall -> network isolation switch
Network Intrusion Prevention	Next generation firewall
Denial of service protection	Anti denial of service system -> denial of service protection
Sensitive data leakage prevention	Intrusion protection system -> sensitive data protection
Spam protection	Mail Security Gateway -> spam protection
Network virus defense	Network virus defense
Network threat detection	intrusion detection system
Network data leakage detection	Intrusion detection system -> sensitive data outgoing detection
Web application protection	web application firewall
Code audit	Code audit system ->code audit
Database audit	Database audit
Log audit	Log audit
Network security audit	Network security audit
Sensitive data identification	Data security system -> sensitive data identification
Desensitization of sensitive data	Data security system -> sensitive data desensitization
information service	Threat Intelligence Platform -> intelligence service
VPN access	VPN
Operation & Management access control	Fortress -> access control
Name of safe atomic capability	Honeypot -> network attack entrapment

3 Computing Facilities Securities

Computing infrastructure includes cloud computing, edge computing and end computing. While providing powerful computing technology support services for upper tier applications, it also faces many risks. It is necessary to build a comprehensive, systematic and three-dimensional protection means for cloud computing, edge computing and end computing.

In cloud computing, security protection should be provided for physics, virtualization, business, data, operation and maintenance management, etc. In terms of edge computing, security protection should be provided for network services, hardware

environment, virtualization, edge computing platform, applications, capacity opening, management, data, etc.

In terms of end-to-end computing, security protection should be carried out for physics, virtualization, application, capacity opening, management, data, etc.

At the same time, it is also necessary to do a good job in the security protection of cloud, edge and end interconnection, including identity authentication, traffic monitoring and audit, interface control, security situation monitoring and other security protection means.

Simultaneously carry out the basic system planning of computing network security. Based on the independent collaborative evolution stage of the computing power network, strengthen the construction of basic atomic capabilities. Start the standardization of computing security, formulate standardized interfaces and access criteria, and solve the problems of self security and interoperability of computing network. Meet the personalized and distributed computing power needs of customers, conduct technical pre research and pilot demonstration, and adopt decentralized and security identification/security slicing technology to make the security capability compatible with the distribution of computing power; Research on the application of dynamic intelligent network slicing technology to ensure differentiated network service capability.

4 Network Facility Security

SRv6 (segment routing IPv6) simplifies the network protocol type, has good scalability and programmability, can meet the diversified needs of more new services, provides high reliability, and has a good application prospect in cloud services. SRv6 and the new generation SD-WAN (software defined wide area network) are the core technologies to realize the convergence of computing and networking. The networking scheme combining the two can realize the network linkage between the backbone network and enterprise sites, and realize the interconnection and perception of computing power; Deterministic network technology provides quality of service guarantee for new services with ultra-large bandwidth, ultra-low delay and ultra-high reliability. However, the complex network environment, fuzzy security boundary and highly sensitive time delay have also brought new security challenges.

Traditional security solutions do not have the good scalability and programmability of SRv6 and the performance, flexibility or interconnection required for SD-WAN connection. The atomic security capability can support flexibility, interconnection, scalability and programmability, sense the changes of edge connections, and provide consistent policy implementation. This policy can isolate users, applications, workflows, or data based on many parameters to provide security over the entire transaction path. Traffic can be forced to follow specific behaviors, or isolated to specific users or destinations to ensure consistent policy application and execution.

5 Arranging and Scheduling Security

Facing the highly complex computing network environment, the arrangement management layer cooperatively schedules the resources of each domain of the computing

network according to the diversified and customized computing power requirements. The arrangement management layer perceives and cooperates with the arrangement of computing power users, computing tasks, network resources and computing power resources. The arrangement management shall have the ability to control the security of computing power and solve the problem of computing power abuse. The abuse of computing power includes illegal mining, violent cracking and other acts, which not only encroach on computing power resources, but also may use computing power to launch security attacks. Based on the self adaptation mode of the computing power network, establish the North-South linkage between security services and computing power, and promote the scheduling of security computing power. Considering the introduction of heterogeneous computing power nodes rather than completely self built, it is necessary to solve the identity and trust problems of computing power nodes, and conduct research and verification on technologies such as differential privacy and homomorphic encryption during the interaction between algorithms and computing power. Carry out the pre research on node collaboration. The computing power is in multiple nodes. The nodes need to have a synchronization mechanism. The nodes need to adopt an adaptive and self-organizing architecture. The "edge by edge collaboration" mechanism is used for local interaction of capability and performance information.

6 Operation Service Security

Operation service security is mainly to ensure the security of computing network services, including identity security, operation security and integrated application security. Among them, identity security ensures that the identities of computing nodes and users in the computing power network can be identified and verified; The operation security realizes the functions of security transaction, security monitoring, security audit, etc. The integrated application security provides flexible, dynamic and end-to-end business security for differentiated application scenarios such as digital life, intelligent production and digital society.

7 Data Security

Data security [3] runs through all levels of the computing power network, mainly including data asset identification, data security protection, data flow security, computing security, East West training, etc. which can effectively ensure that the data is in an effective and legitimate use state in the whole life cycle.

Data Asset Identification
Data asset identification combines initiative and passivity to discover assets including servers, relational databases, non relational databases, interfaces, etc., and complete the completion of data asset attributes through information completion and in-depth scanning. From the perspective of data assets, data is obtained from SMC/SMP and data resource scanning discovery, and the data is classified and managed at different levels. The classification and classification list management function mainly includes data classification and classification list, important data list and sensitive data list. Real

time display of classification and classification data information of different dimensions, data sorting of identified asset data, classification and classification mapping of data according to data sensitivity, visual display in the form of charts, and controllable storage of warm and cold data.

According to the data classification and grading rules of countries, industries or enterprises, preset templates can be formed according to AI models, regular matching, keywords, combination rules, etc. you can also configure classification and grading templates according to the needs of the current business.

East Digital West Training

The data value evolution path with knowledge as the core. Driven by technology, it develops artificial intelligence model training and reasoning, and constructs the overall technical framework of "East digital West training". Driven by technology, AI has become the base of new infrastructure technology, promoting the acceleration of artificial intelligence deployment.

AI modeling is different from data development. It has no hierarchical modeling restrictions. At the same time, it opens the way of data reading and warehousing, and supports free modeling; In addition to the basic data processing components, it also has built-in rich machine learning algorithms. It also supports user-defined processing components to help dig deep into data value.

Data Flow Security

Data flow involves data aggregation, data transmission between providers and users, as well as the use of data out of the control of owners. Data will face greater security risks, including personal information disclosure, data vulnerable to attack and disclosure, illegal over collection, analysis and abuse of data, etc. During the data flow process, the data shall be identified, the data flow node, operation, flow direction and other information shall be recorded, and a unified cross domain and cross system data flow identification shall be established to realize that the data flow direction can be controlled and the data flow can be perceived. In order to monitor the flow of data in real time, it is necessary to strengthen network security monitoring through technical means, especially automated security monitoring, and comprehensively monitor and analyze the data sharing platform and system through traffic, logs, configuration files, etc., so as to facilitate early warning and collaborative defense of network security events, and improve the overall security situation awareness, security decision-making and other capabilities.

8 Situational Awareness

Situational awareness integrates detection, early warning, response and disposal functions, and is the safety brain in the active defense system. It plans the security capability of the integrated computing service system of "Mega-projects approved for data clusters", integrates the existing data center security data, interoperability monitoring platform and supporting business systems, builds a data center level, data center cluster level and industry-wide computing security perception and monitoring platform, realizes the interaction and supervision of the whole process, all elements and the whole industry

chain of computing scheduling, and has the functions of security system [4] perception, monitoring, early warning, disposal, evaluation, etc., Improve the security awareness and linkage monitoring capability of cross data center and cross data center clusters. Gradually build a coordinated threat handling capability.

8.1 Situation Awareness of Network Security Quality Based on Data Network Collaboration

It will improve the monitoring system for computing network governance, promote the optimization of the network architecture and traffic routing of data centers in the eastern and western regions, promote the quality monitoring of data network collaboration, promote the networking of edge data centers, and continuously improve the network capacity of data centers (Fig. 2).

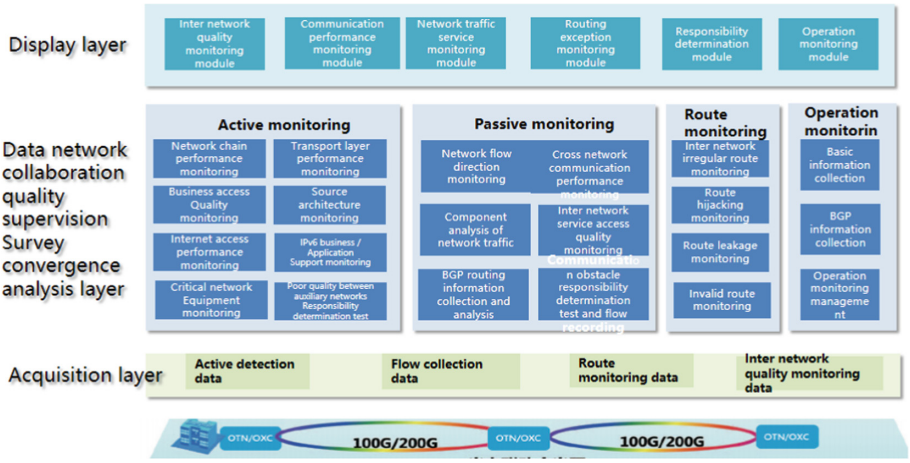

Fig. 2. Situation awareness of network security quality based on data network collaboration

8.2 Situation Awareness of Computing Capacity Security Improvement Evaluation

Take the cloud with the network and use the network to strengthen computing, realize the enhancement of computing power value based on the computing power network, and ensure the enhancement of computing power value with computing power security. Promote the development of computing power network from multiple demands, support the implementation of ubiquitous computing power with multiple technologies, and enhance the security value of computing power with multi-dimensional security situational awareness (Fig. 3).

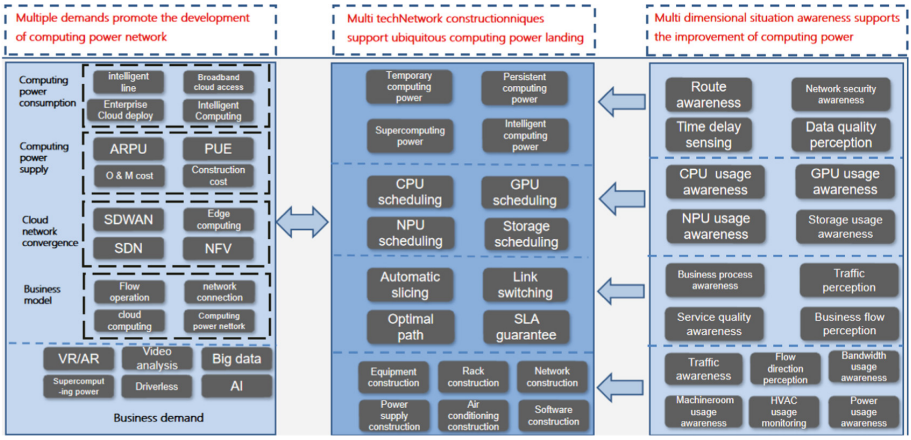

Fig. 3. Situation awareness of computing power security improvement evaluation

8.3 Situation Awareness of Industry Chain Security Enhancement Assessment

Accelerate the key technology and product innovation of the new data center operation security management and other software layers, as well as the cloud native and cloud edge integration security and other platform layers, and improve the software and hardware synergy; Establish and improve the new data center security standard system; Draw the security map of the whole industry chain of the new data center, promote the completion of key links, and carry out the security capability evaluation of the new data center (Fig. 4).

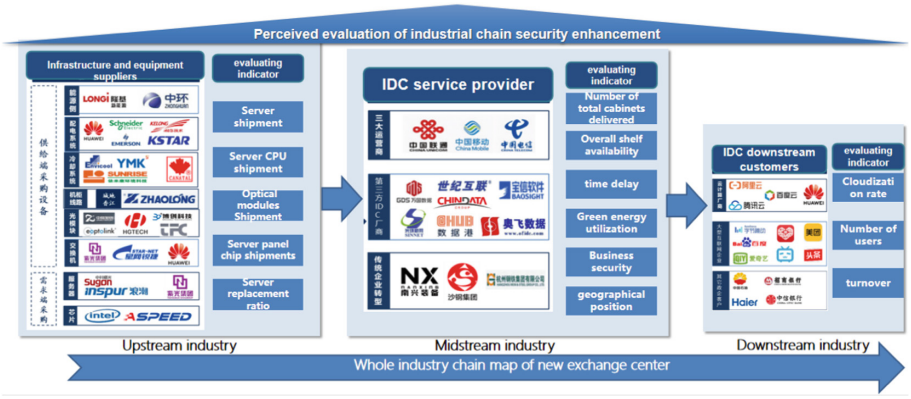

Fig. 4. Industry chain security enhancement assessment situation awareness

8.4 Situation Awareness of Green Low Carbon Assessment

The continuous deepening of the national "double carbon" strategy has put forward higher requirements for the green and low-carbon level of the data center industry, and the PUE, cue and other energy efficiency indicators are more strictly restricted. "Mega-projects approved for data clusters" is a powerful driving scheme for the data center to achieve "carbon neutralization and carbon peak". The collection and evaluation of energy consumption indicators saved after "Mega-projects approved for data clusters" can be used as one of the dimensions to evaluate the situation awareness of "Mega-projects approved for data clusters". In order to quickly achieve the "double carbon" goal, implement the notice of the Ministry of industry and information technology on printing and distributing the three-year action plan for the development of new data centers (2021–2023), and optimize the green development of the data center industry chain, it is necessary to establish and improve the green data center standard system (Fig. 5).

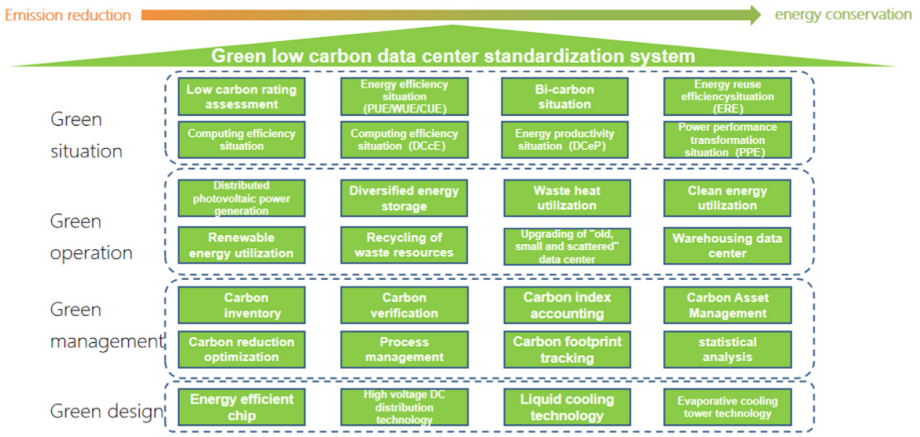

Fig. 5. Green low carbon assessment situational awareness

8.5 Situation Awareness of Security Assurance Assessment

In the important supporting support construction scheme of "Mega-projects approved for data clusters", it is clearly emphasized that from the aspects of data risk identification and protection, data security compliance assessment, to data encryption protection and related technical monitoring, it is necessary to "synchronously plan, construct and use security technical measures to ensure business stability and data security (Fig. 6).

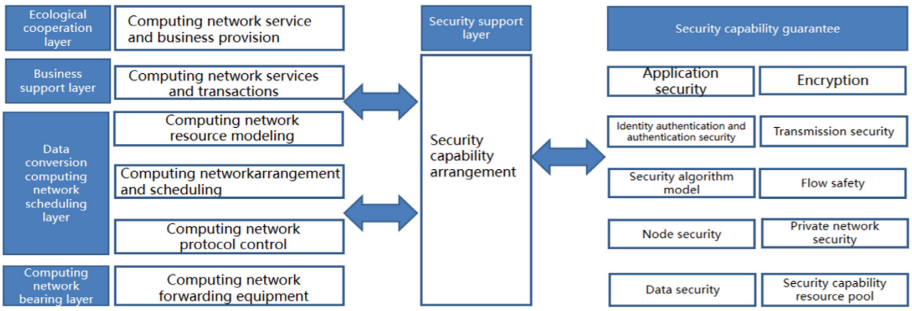

Fig. 6. Security assurance assessment situation awareness

8.6 Threat Collaborative Disposal Scenario

Based on the new data center security monitoring means, facing the "Mega-projects approved for data clusters" network threat collaborative disposal scenario [5], carry out closed-loop disposal and collaborative linkage of threat disposal, deposit the network security risk case base, emergency drill scenario base, emergency disposal plan base, emergency disposal expert base and emergency response tool set base, promote the transformation of threat disposal to risk early warning and pre prevention, and improve the scientificity, accuracy and timeliness of threat disposal, We will strengthen capacity-building for coordinated disposal.

9 Conclusion

The “Mega-projects approved for data clusters” project realizes “the network moves with the cloud, and the cloud moves with the needs”, forming a multi-layer architecture system including the computer network collaborative scheduling of the control plane, the network fusion perception and management of the data plane, and the arrangement of computing resources of the service plane.

The new architecture, new technologies and new services of the “Mega-projects approved for data clusters” network may have new security risks that need to be overcome, and need to be guaranteed by a new security mechanism adapted to it. There are potentially complex network risks and computing power node security risks in the infrastructure layer. The scheduling management layer involves scheduling security risks and computing power use out of control. The operation service layer faces problems such as accessing malicious nodes, untrusted transactions, insecure applications, etc. in addition, there may be data security risks such as uncontrollable data flow in the "Mega-projects approved for data clusters" network, which needs to be strengthened through an integrated whole process trusted mechanism.

This paper makes a comprehensive analysis on the network security problems in “Mega-projects approved for data clusters” from the aspects of computing power facility security, network facility security, scheduling security, operation service security, data security, situation awareness and so on. It is proposed to build a network-based ubiquitous

endogenous security system with ubiquitous security computing brain as the core, atomic security capability as the foothold, and intelligent orchestration as the link.

Guided by the security application, oriented to the new business mode of cluster scheduling, combined with the existing traffic protection and security monitoring means in the data center, it focuses on the realization of network security quality situational awareness, computing power security improvement assessment situational awareness, industrial chain security enhancement assessment situational awareness, green low-carbon assessment situational awareness, security assurance assessment situational awareness and other assessment systems for data network collaboration.

And then promote the network convergence, transmission, storage and integration application links for the cluster nodes of the data center to carry out the construction of traffic protection security means; In combination with active detection means and detection work, implement the construction of security situation capability and build the capability of threat collaborative disposal.

References

1. Reply of the national development and Reform Commission and other departments on Approving the Beijing Tianjin Hebei region to start the construction of the national computing node of the national integrated computing network. National Development and Reform Commission document No.(2022)212
2. Three year action plan for new data center development (2021–2023). Ministry of industry and information technology communication document No.(2021)76
3. Kwiecień, A., Maćkowski, M., Sidzina, M.: Data security in microprocessor units. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2013. CCIS, vol. 370, pp. 495–506. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38865-1_50
4. Zhang, Y., Jin, S., Cui, X., Yin, X., Pang, Y.: Network Security Situation Prediction Based on BP and RBF Neural Network. In: Yuan, Y., Wu, X., Lu, Y. (eds.) Trustworthy Computing and Services. ISCTCS 2012. Communications in Computer and Information Science, vol. 320. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-35795-4_83
5. Lotz, V.: Threat Scenarios as a Means to Formally Develop Secure Systems. Springer, Berlin Heidelberg (1997)