Research on System Data Security Under Network Technology

Hairong Lu\(^1\)*, Xutao Bai\(^1\)

\(^1\)Suzhou Nuclear Power Research Institute Co., Ltd., Suzhou, Jiangsu, China, 215004

*Corresponding author e-mail: xutaoa@snpr.org.cn

Abstract. Today's society is a digital society, all data can be stored digitally, which leads to the explosion of data growth. However, the security storage of cloud data is the primary problem that restricts the development of cloud storage. Malicious hackers, software and hardware vulnerabilities and so on will pose a serious threat to users' data stored in the cloud. This paper combines the typical big data system technical framework and builds the big data security technical framework around the security requirements of big data. Under this framework, the research status of key technologies of big data security is systematically summarized from multiple aspects, including the main security mechanisms involved in the technical framework of big data system. Finally, the core problems and development trends of big data security technology to be solved are summarized.

Keywords: Data, Big Data Security, Privacy Protection, Information Security

1. Introduction
At present, the development of the big data is still faced with many problems, the key problems of security and privacy problem is people accepted one. At present, people's behavior on the Internet are all in the hands of merchants on the Internet, including shopping habits, contact friends, reading habits, retrieval, habits, etc. A number of actual case shows that even the harmless, after data is a large collection of SiChuan will be exposed to individual privacy. As with other information, big data in the process of storage, processing, transmission and other faces many security risks, With data security and privacy requirements. To achieve data security and privacy protection, than in the past other safety issues (such as the data security in cloud computing) more difficult. This is because in cloud computing, although service providers to control the data storage and operation environment, but there are still some way to protect the user data\(^1\). Therefore, it is extremely difficult to restrict the use of user information and protect user privacy by technical means.

2. Data security technology framework
The establishment of an effective data security technology framework can provide guidance for the research and deployment of data system security technology. This section first introduces the current representative data security technology classification perspectives and contents, and on this basis, proposes a big data security technology framework\(^2\).
In 2015, NIST proposed the data reference architecture, which divided the participants of the big data system into data providers, data consumers, Big data application providers and big data frameworks. Application providers perform data collection, visualization, and access, and framework providers. Based on the NIST architecture, combined with the characteristics of big data business process and big data system technical framework, a security technical framework is proposed that conforms to the characteristics of big data business, as shown in Figure 1.

**Figure 1.** Data security technology framework.

Data security supervision is the guarantee of large data security, mainly to solve the data itself, data service and big data platform security monitoring and evaluation, including data regulation, platform, service regulation regulation and comprehensive security situational awareness(3).

The following chapters of this paper will introduce the research status and existing problems of each security technology in detail according to the proposed framework of big data security technology.

3. **System data platform security**

This section mainly introduces four aspects of data platform security: data processing security, data storage security, infrastructure security and big data access control.
3.1. Data processing security
The data processing framework defines the computing and processing methods of big data and provides necessary basic software support for big data applications\(^4\). In order to meet a wide range of needs from batch large-scale data processing to near-real-time data processing, big data platforms usually need to integrate multiple processing frameworks. While these frameworks are widely used, they are faced with many security threats such as unauthorized access and information leakage due to the lack of security considerations in their initial design. Therefore, how to give full play to the core functions and efficiency of the data processing platform while ensuring the security of processing task scheduling and execution, and realizing the credibility of processing results are the main problems facing the security of big data processing.

3.2. Data storage security
Data storage security is the top priority of data platform security. The main goal is to ensure the confidentiality, integrity and availability of stored data. Specific implementation mechanisms include data encryption, data integrity proof and data disaster recovery backup. Data encryption is the core technology to ensure the security of big data storage. The current research focuses include homomorphic encryption, searchable encryption, attribute encryption and reserved format encryption. These encryption mechanisms can not only provide data confidentiality protection, but also provide support for statistics, analysis, search and access control of dense data.

3.3. Data infrastructure security
The data infrastructure provides the computing, storage, and networking resources needed for the platform components to run, including physical resources and Virtualized resources. Due to the complexity of information system software, vulnerabilities and vulnerabilities are inevitable, and the security of data infrastructure faces great challenges. Its main security requirements are to deal with the security threats brought by resource sharing and virtualization, including the security of virtual machines and virtual machine monitors, virtual network SDN and NFV, etc.

3.4. Data access control
Access control is an important mechanism to ensure the security of multi-component and heterogeneous mass data in the data flow service\(^5\). In the data scenario, the scale of data, application and user surges, the access request of users is complex and changeable, the data sharing across data center and across security domain is more and more frequent, access control is faced with the challenge of fine-grained access control and cross-domain access control of massive data. ABAC and RBAC are the main access control models applied in the big data environment. In view of the above challenges, the current research mainly focuses on attribute-based access control and role mining.

4. Conclusion
As a subversive and innovative technology, data is a new stage. It influences the remodeling of social forms and changes people's way of life and work, and its huge value makes it easy to become a key target for attack. However, due to the massive, heterogeneous and high-speed characteristics of big data, traditional security technologies are difficult to meet the high efficiency, real-time, dynamic, cross-domain and other requirements of data security, and the security protection of data faces great challenges. At the same time, in order to realize efficient processing of data, the data platform introduces new data storage and process framework, which brings new security threats. However, the security mechanism adopted by these new frameworks is very weak, which makes the security problems faced by big data more serious. In recent years, big data security incidents occur frequently, involving citizens' privacy, military secrets and even political regimes. Therefore, it is urgent to study...
big data security technology. The major challenges of data security are mainly reflected in the following three aspects:

1. The level of security protection of big data does not meet the mission of The Times. Data platform is the centralized storage place of data, and platform security is the foundation to ensure data security, which should not only be protected from outside, but also from inside, and its core solution must rely on password.

2. The degree of data security sharing is incompatible with the important role that data should play. In order to realize the value of big data and improve the efficiency of big data, it is necessary to solve the problem of "unwilling, afraid and unable" sharing of big data caused by interest barriers and security trust. Blockchain technology is the key to solve the problems of incentive and value recognition, security and responsibility recognition, analysis and full-dimensional sharing, and provides a new way for big data security sharing and trusted services.

3. Data security supervision is incompatible with the important status of big data. In the face of the increasing massive heterogeneous data and data platform components, how to effectively supervise data, services and platforms to solve the problems of unclear data usage and unknown system security situation has become an urgent problem to be solved[6].

References
[1] Stephen Northeutt. Translated by Yu Qingni, Wang Xiaogang, Zhou Gang. An Analyst of Network intrusion detection, Beijing: Posts and Telecommunications Press, 2000-10.
[2] Wu Yan. Intruder Detection Beijing: Electronic Industry Press, 1997-07.
[3] Wang Huabin, Li Hao. Introduction to intrusion detection Systems (IDS). Shanghai Microcomputer, 2000, 8; 15 -16.
[4] Luo Guangchun and Zhang Jun. The history, present situation and research development of intrusion detection system. Computer Application research, 2003, 8:1 -3.
[5] Bai Xiaobing and Cao Yang. Network intrusion detection System based on artificial immune model. Computer Engineering and Applications, 2002, 38(9): 133-135.
[6] Dai Yingxia, Lian Yifeng. System security and detection. Beijing: Tsinghua University Press, 2002:86-87.