ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

Issues and Countermeasures of Information Network Security in the Context of Big Data for Higher Education Institutions

Yinqian Cheng[a,*], Shengzhong Zhang[b]

Information Network Center, China University of Geosciences (Beijing), Beijing, China
[a]chengyq@cugb.edu.cn, [b]zhsz@cugb.edu.cn
[*]Corresponding author

Abstract: *In today's society, we are entering the era of big data, where the field of higher education is actively embracing this wave of digitization. Utilizing big data technology to drive innovation in teaching, research, and administration. However, the rapid development of big data applications has also brought about new challenges for information network security in higher education institutions. Based on a thorough analysis of the impact of big data applications on information network security in colleges and universities, this thesis comprehensively examines common information network security issues in the context of higher education's big data environment, such as sensitive data leaks and privacy concerns, network attacks and malicious behaviors, data sharing platform security issues, and human operational errors. Against this backdrop, this paper proposes a series of effective information network security strategies, including comprehensive network security awareness education and training, establishment of a robust security system, reinforcement of access control and permission management, as well as the establishment of an emergency response mechanism. These strategies aim to assist higher education institutions in ensuring information network security in the era of big data, and to promote the sustainable development of higher education. Through in-depth analysis of the issues and the formulation of strategies, this paper provides valuable guidance and reference for the practical response to information network security in higher education institutions, offering theoretical and practical support for elevating the level of information network security in higher education in the age of big data.*

Keywords: *Big Data, Information Network Security, Higher Education*

1. Introduction

In today's society, we have entered the era of big data, and various industries are actively embracing the application of big data technology to drive productivity development and innovation in decision-making [1]. As an integral part of the national innovation system, higher education is actively integrating into this wave of informatization, using big data technology to deepen teaching, research, and management, taking solid steps towards improving quality and efficiency. Big data technology has penetrated into many areas of higher education, such as teaching management, research innovation, and campus services, opening up new avenues for the advancement of higher education.

However, along with these developments comes the new challenges that the application of big data poses to the information network security of higher education institutions. With the continuous expansion of the scale of information systems in universities, student, faculty, and research data are experiencing explosive growth, with massive data being stored in university information systems. The consequences would be unimaginable if data leaks or systems are attacked. Faced with this new situation, universities must attach great importance to information network security. The country has set the overall goal of "ensuring cybersecurity" at the strategic level and promulgated laws such as the Cybersecurity Law and the Personal Information Protection Law, providing clear policy basis for the implementation of information network security work in universities. Universities bear the responsibility of adopting practical and feasible technological and managerial measures to fulfill national policy requirements, strengthen information network security construction, effectively prevent and mitigate various security risks, and ensure the secure and orderly application and development of big data.

Based on a comprehensive analysis of the impact of big data applications on information network security in higher education institutions, this paper thoroughly examines the core issues currently facing

ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

information network security in universities. It proposes a series of countermeasures and suggestions, including strengthening network security awareness, establishing a comprehensive technical defense system, and improving regulatory mechanisms. We hope that this paper can provide powerful guidance for universities to ensure information network security under new circumstances, inject strong impetus into the development of higher education in the era of big data, and unite efforts from all sectors to comprehensively enhance the level of information network security in universities.

2. Common Information Network Security Issues in the Context of Higher Education Big Data Environment

2.1. Sensitive Data Leakage and Privacy Issues

In the context of higher education's big data environment, the rapid accumulation and processing of data have become an engine driving innovation. However, this has also brought new challenges to sensitive data leakage and privacy issues [2]. As data is extensively collected and stored across various aspects of educational, research, and administrative levels within institutions, it not only encompasses personal information of students and staff but may also include sensitive data such as academic records and medical history. Undoubtedly, this information has become a coveted target for attackers, as personal data has transformed into a valuable digital asset in the information age.

The severity of sensitive data leakage and privacy issues cannot be overlooked. Firstly, unauthorized access to these sensitive data directly threatens individual privacy rights and security. Attackers can exploit this information for identity theft, financial fraud, phishing, and other illicit activities, causing direct economic losses to individuals. More critically, malicious use of sensitive data can lead to damage in personal reputation, affecting one's social standing and credibility. Furthermore, the leakage of sensitive data also poses risks of academic misconduct. In the big data systems of educational institutions, students' academic achievements, paper outcomes, and other information are stored. Once these data are tampered with or maliciously manipulated, it can mislead the academic evaluation system and undermine academic integrity. Similarly, unauthorized access or tampering with research data and innovative outcomes of researchers could lead to intellectual property disputes, damaging the innovation environment and research reputation.

The emergence of sensitive data leakage issues is not solely from external malicious attacks; inadvertent actions by internal personnel can equally become sources of leakage. Employees, while handling data, might inadvertently disclose sensitive information due to insufficient security awareness. Inadequate measures in data processing, such as sharing passwords or unencrypted transmission, can lead to accidental leaks.

2.2. Issues of Network Attacks and Malicious Behavior

Network Attacks and Malicious Behavior have evolved into a serious security threat, with impacts extending far beyond data leakage. They have the potential to severely disrupt and damage various core activities of the entire school, including teaching, research, and management[3]. As the hub of information, the university's big data system is attracting various malicious activities, including but not limited to malware, viruses, trojans, worms, ransomware, etc. These threats quietly lurk within the digital campus network, ready to launch attacks at any moment.

The potential consequences of these network attacks cannot be underestimated. First and foremost, the risk of data leakage is the most significant and concerning. Attackers may gain access to sensitive data across various levels of the school through network intrusion methods. This includes personal information of students, faculty, academic research achievements, course content, etc. Once this data is accessed without authorization, personal privacy rights are seriously compromised. This also provides opportunities for unlawful activities such as identity theft and financial fraud, potentially leading individuals into economic and legal disputes, significantly impacting their lives and studies. Secondly, system paralysis is another major threat. The university's big data system is a crucial infrastructure supporting teaching and research. A network attack could lead to system crashes and service interruptions, seriously affecting online learning for students, experimental data processing for researchers, and administrative processes for departments. Particularly during critical periods such as academic conferences, exams, and course selection, system paralysis could cause chaos, disrupting the normal operation and order of the school.

ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

2.3. Security Issues of Data Sharing Platforms

The establishment of data sharing platforms has indeed facilitated information exchange, collaborative cooperation, and innovation; however, it has also brought about a series of serious data security issues, posing significant challenges to higher education institutions [4].

Firstly, the coexistence of data from different departments on the sharing platform may lead to issues of inadequate permission management. Higher education institutions encompass various types of data, including student information, faculty and staff information, research data, etc., all possessing varying degrees of sensitivity and privacy concerns. Nevertheless, if a data sharing platform does not establish strict permission control mechanisms, unauthorized individuals might gain access to sensitive data, potentially leading to privacy breaches and misuse of information. This could also result in the theft of academic achievements, infringements upon personal privacy rights, causing immeasurable harm to both faculty and students.

Secondly, the establishment of data sharing platforms also introduces the risk of data leaks. Given the platform's coverage of extensive data, malicious attacks or improper access could result in the theft, alteration, or abuse of a substantial amount of sensitive data. The school's research outcomes, teaching materials, student evaluations, and more could all be at risk of leakage, potentially damaging the institution's reputation and interests. Simultaneously, data leaks could trigger disputes over intellectual property rights, legal litigation, and other problems, subjecting the school to unpredictable legal risks.

Moreover, the presence of sharing platforms could give rise to issues concerning data quality and accuracy. During the process of data sharing, different departments or individuals may provide varying versions or qualities of data, potentially impacting the analysis and application effectiveness of the data. If data quality cannot be ensured, higher education institutions may be misled in their research and decision-making processes, potentially making erroneous judgments and affecting the accuracy of academic research and management decisions.

2.4. Issue of Human Error in Operations

Human error is a significant issue that cannot be ignored, which can lead to a series of adverse consequences such as data leaks, system failures, and chaos in information management[5]. Despite the many benefits that big data technology brings to higher education institutions, human error remains a potential risk that requires practical and effective measures to prevent and address.

Firstly, due to the complexity of the higher education institution's big data system, negligence and improper operations may occur during usage and operation. For instance, actions like accidental deletion, modification, or sharing of data can result in irreversible damage or leaks. Moreover, incorrect system settings and configuration operations could lead to system crashes or performance degradation. These human errors not only disrupt the normal flow of teaching, research, and management activities but also potentially cause unnecessary troubles and concerns for faculty and students.

Secondly, regarding information security in higher education institutions, human error represents a potential security vulnerability. For instance, employees handling sensitive data carelessly, failing to follow prescribed procedures, may result in the leakage or improper usage of sensitive information. Furthermore, without rigorous permission management and access control mechanisms, employee mistakes could grant unauthorized personnel access to sensitive information, leading to security risks.

3. Information Network Security Strategies for Higher Education Institutions in the Big Data Era

3.1. Comprehensive Network Security Awareness Education and Training

Comprehensive network security awareness education and training is an important measure to ensure the information network security of universities in the era of big data. With the rapid development of information technology, the threat to network security is constantly increasing, and faculty and students in universities are facing various potential network risks. Through comprehensive network security awareness education and training, the network security literacy of faculty and students can be enhanced, correct network security behaviors can be cultivated, thereby effectively reducing potential security risks.

Firstly, network security awareness education and training should cover a wide range of groups, including faculty and staff as well as students. Faculty and staff are the main users and managers of the

ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

university's information system, and their security awareness and operational behavior directly impact the security of the entire system. Students are the main users of the network, and they need to use the network for course learning, research activities, etc., so they also need to have a certain level of network security knowledge and skills. According to the characteristics and needs of different groups, universities can carry out network security awareness training at different levels and with different content.

Secondly, network security awareness education and training should focus on practicality and relevance. The training content should be close to reality and cover basic knowledge of network security, common security threats and attack methods, secure operation methods, and other related aspects. Especially for common network fraud, social engineering, and other methods, training should use case analysis and simulated operations to help faculty and students identify and prevent potential threats. Additionally, training can be combined with the school's internal network security policies and measures, allowing faculty and students to understand the school's security regulations and requirements.

Thirdly, network security awareness education and training should be continuous. Network security technology and threats are constantly evolving, so training content also needs to be updated and adjusted in a timely manner. Universities can regularly organize network security lectures, seminars, and other activities, inviting network security experts to share the latest security knowledge and experiences. At the same time, online courses, training videos, and other methods can be used to allow faculty and students to learn network security knowledge anytime and anywhere, enhancing their security awareness.

Furthermore, network security awareness education and training can be combined with practical exercises and drills. For example, emergency network security drills can be organized to simulate various security incidents, allowing faculty and students to learn response measures in a simulated environment and improve emergency response capabilities. Additionally, simulated network attacks can be conducted to help faculty and students understand various attack methods and defense measures, enhancing their practical operational abilities.

3.2. Establishing a Comprehensive Security Framework

Establishing a comprehensive security framework is a crucial component in ensuring information network security. With the rapid development of information technology and the widespread application of big data, universities face increasingly complex and diverse cybersecurity threats. Establishing a comprehensive security framework not only effectively mitigates potential threats but also enhances the school's emergency response capabilities, ensuring the stable operation of teaching, research, and management.

Firstly, establishing a comprehensive security framework requires a technological approach, utilizing advanced security facilities and protective measures. This includes setting up Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and intercept malicious attacks, configuring firewalls to control incoming and outgoing data traffic, and using antivirus and anti-malware software to promptly detect and remove malicious programs. Universities should select appropriate security technologies based on their specific situations, constructing multi-layered and multi-dimensional security defenses to ensure the security of information systems and data.

Secondly, establishing a comprehensive security framework also involves formulating detailed security strategies and policies. These strategies and policies should clearly define requirements for data access permissions, password policies, data backup requirements, and other aspects, ensuring that faculty, students, and staff adhere to regulations when using information systems and handling data to prevent improper operations and unnecessary risks. Additionally, security strategies and policies should include security requirements for external partners to ensure that external collaborations do not pose security risks to the university.

Thirdly, establishing a comprehensive security framework also emphasizes the confidentiality, integrity, and availability of information. Confidentiality ensures that sensitive information is not accessed by unauthorized individuals, integrity ensures that data is not tampered with during transmission and storage, and availability ensures the normal use of systems and data. Universities can employ data encryption technology, access control mechanisms, and other means to comprehensively safeguard the security and trustworthiness of information.

3.3. Strengthening Permission Management and Access Control

As the scale of high school information systems continues to expand and data accumulates rapidly,

ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

effective management of who can access what data and how they can access it becomes particularly important. Strengthening permission management and access control can effectively prevent unauthorized access, protect sensitive data from harm, and maintain the security of the school's information systems.

Firstly, enhancing permission management means ensuring that only authorized users can access specific information and resources. High schools should set different permission levels and access scopes based on users' identities, roles, and needs. For example, faculty and staff may have access to teaching and research data, but may not be able to access administrative management data; students may access course materials, but not faculty and staff work files. By subdividing permissions, unauthorized access to sensitive data can be avoided, reducing the risks of data leakage and misuse.

Secondly, strengthening access control means ensuring that users must be verified and authorized when accessing data. High schools can employ techniques such as multi-factor authentication, single sign-on, requiring users to provide multiple verification factors during login, such as passwords, fingerprints, mobile verification codes, etc., increasing the difficulty of identity verification. In addition, high schools can establish approval processes for specific sensitive operations, requiring approval and authorization for specific actions, ensuring that only legitimate operations are executed.

Thirdly, strengthening permission management and access control also requires the establishment of detailed operation logs and audit mechanisms. High schools should record each user's actions, including login, access, modifications, etc., to facilitate tracing and analysis in the event of security incidents. Audit mechanisms can help identify abnormal operations and potential risks, enabling timely measures to prevent problems from escalating.

Furthermore, strengthening permission management and access control also requires attention to the access permissions of external partners. When high schools cooperate and share data with external partners, it is also necessary to ensure that partners can only access necessary data, avoiding misuse of sensitive information. Access permissions for partners should be strictly limited and promptly revoked after cooperation ends.

3.4. Establishing an Emergency Response Mechanism

With the continuous evolution and escalation of cyber threats, universities need to be able to respond promptly and effectively to various security incidents, ensuring the normal operation of teaching, research, and management. Establishing an emergency response mechanism can help universities quickly detect, analyze, and address security incidents, reduce potential losses, and enhance the overall level of information network security.

Firstly, establishing an emergency response mechanism requires a clear division of responsibilities and a command structure. Universities should designate a dedicated cybersecurity team or experts to monitor, analyze, and handle security incidents. This team should consist of cybersecurity professionals with extensive security experience and technical expertise, capable of responding rapidly to various security threats. Additionally, universities should establish a clear command structure for emergency response, ensuring quick decision-making and action when security incidents occur.

Secondly, establishing an emergency response mechanism requires the implementation of a comprehensive security event monitoring and alerting system. Universities should deploy advanced security devices and tools to monitor network traffic, logs, and behaviors, detecting anomalies and issuing timely alerts. The alerting system can notify relevant personnel through methods such as SMS, email, and phone calls, enabling swift response measures. The monitoring and alerting system should be capable of real-time network monitoring, automatic analysis, and judgment of abnormal situations, enhancing the efficiency of detecting and responding to security incidents.

Thirdly, establishing an emergency response mechanism involves developing detailed emergency plans and procedures. Universities should prepare emergency plans in advance, specifying the procedures, responsible parties, and contact information for handling different types of security incidents. The plans should cover the entire process from incident discovery, alerting, analysis to response, ensuring a well-organized approach at every step. Furthermore, universities should conduct emergency drills to simulate various security incidents, testing the feasibility and effectiveness of the emergency plans.

Lastly, establishing an emergency response mechanism requires ongoing training and drills. Cybersecurity technology and threats are constantly evolving, and the members of the security team need to continuously enhance their technical and emergency response capabilities. Universities can regularly

ISSN 2616-7433 Vol. 5, Issue 13: 1-6, DOI: 10.25236/FSST.2023.051301

organize training and drill activities to help security team members stay updated on the latest security knowledge and techniques, familiarize themselves with emergency plans and procedures, and improve their ability to respond to security incidents.

4. Conclusion

With the advent of the era of big data, information network security in universities has become an essential and unavoidable issue. This paper delves into the challenges posed by the application of big data to information network security in universities, exploring key areas such as sensitive data leakage and privacy issues, network attacks and malicious behavior, data sharing platform security, and human operational errors. Based on this analysis, the paper proposes a series of effective information network security strategies aimed at helping universities effectively address various security risks and ensure the security, integrity, and availability of information systems and data.

Firstly, comprehensive cybersecurity awareness education and training are considered the cornerstone of enhancing information network security in universities. Through widespread training, the awareness of both faculty and students can be heightened, fostering proper cybersecurity behavior habits and thereby reducing potential security vulnerabilities. Secondly, establishing a robust security framework is crucial to ensuring information network security, encompassing both technological infrastructure and security policies. Strengthening permission management and access control helps prevent unauthorized access, safeguard sensitive data, and uphold the overall security of the university's information systems. Lastly, establishing an emergency response mechanism aids universities in promptly and effectively addressing various security incidents, minimizing potential losses, and ensuring the stable operation of teaching, research, and management.

In summary, the era of big data brings unprecedented challenges to information network security in universities, while also presenting ample opportunities for innovation and advancement. By adopting comprehensive security strategies, universities can maintain a leading position in the field of information network security, providing solid protection and support for higher education in the age of big data. As technology continues to evolve and threats evolve, universities must remain vigilant, continuously strengthen information network security efforts, optimize strategies and measures, and ensure the security and reliability of information systems, offering a secure and stable digital learning and working environment for both faculty and students.

References

[1] Y. Chen. Research on Computer Network Security Measures in the Context of Big Data [J]. Network Security Technology & Application, 2023, 06: 66-68.
[2] J. L. Yang. Research on Campus Network Information Security under the Background of Big Data [J]. Modern Information Technology, 2020, 4(12): 148-150.
[3] Y. Q. Guo. Analysis of Network Information Security Issues in the Context of Big Data Environment [J]. Network Security Technology & Application, 2022, 09: 58-59.
[4] Z. Y. Li. A Brief Analysis of the Application of Big Data Technology in Smart Campuses of Universities [J]. Information Recording Materials, 2023, 24(1): 110-113.
[5] F. Miao. Analysis on Network Information Security and Protection in Colleges and Universities under Big Data [J]. Shanxi Electronic Technology, 2020, 6: 52-54.