American Journal of Computer Science and Technology
2022; 5(2): 101-107
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220502.21
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Research on the Application of AI in the Cyberspace Security: A Case Study of Smart Campus Network Security

Wei Junxu, Tuyatsetseg Badarch*

Department of Information Technology, Mongolian National University, Ulaanbaatar, Mongolia

Email address:

ba.tuyatsetseg@mnun.edu.mn (T. Badarch)

*Corresponding author

To cite this article:

Wei Junxu, Tuyatsetseg Badarch. Research on the Application of AI in the Cyberspace Security: A Case Study of Smart Campus Network Security. *American Journal of Computer Science and Technology*. Special Issue: *Advances in Computer Science and Future Technology*. Vol. 5, No. 2, 2022, pp. 101-107. doi: 10.11648/j.ajcst.20220502.21

Received: April 8, 2022; **Accepted**: May 6, 2022; **Published**: May 24, 2022

Abstract: AI has a variety of educational applications such as smart campuses, personalized learning platforms, teachers and students in assessment, and facial recognition systems. In this paper, we focus on the common threats in cyber space of education. An AI system inherits security threats of traditional computer system, therefore, cybersecurity protection mainly helps computer's software and hardware, data store and transfer, as well as human activity. Therefore, we focus on the application of artificial intelligence technology to improve security protection and management capabilities in cyberspace security can further reduce the incidence of network failures and network attack accidents, and improve network system operation efficiency. We focus on the role of artificial intelligence and its applications through machine-learning systems. The general ways with the advancements of IT colleges and universities have adopted smart campus systems and they have become the mainstream. This paper introduces the design and implementation experience of a smart campus network, information security protection system, and points out that the implementation effects on providing teachers and students with a fast, safe, and reliable network. This environment makes teaching easier and students' learning more efficient. To this end, the article studies the role of artificial intelligence in cyber security, and hopes that this research can provide a scientific and reasonable reference for future related research.

Keywords: Artificial Intelligence, Cyberspace, Security, Campus Network Security, Information Security

1. Introduction

To ensure the reliability and security of a network, it is necessary to strengthen cyber security. Although the country's technical capabilities in this area are gradually improving, due to the tremendous usage of the Internet, there are many problems in network security. In this situation, it is necessary to fully apply advanced artificial intelligence (AI) technology to effectively deal with and solve the problems in this area.

According to several studies, we highlight many techniques based on AI for a more flexible, adaptable, and robust cyber defense systems that is capable of detecting a wide variety of threats in real-time [1-8]. In recent years, the adoption of artificial intelligence (AI) techniques started to improve the field of cyber security [9-11].

AI has a variety of educational applications, such as smart campuses to improve university standard, personalized learning platforms to promote students' learning, aid teachers and students in assessment, and use facial recognition systems to recognize students' behaviors. In the face of the current threats to college network and information security, we need to plan and design an integrated protection system for the network. We focus on the role of artificial intelligence and its applications through machine-learning systems.

In terms of network security defense, the full use of this technology has effectively improved the quality and effectiveness of cyberspace security defense, and played an important role in promoting the sustainable development of my country's network security field.

2. Threat Analysis of Information Security Existing in Smart Campus Network

An AI system inherits security threats of traditional computer system, therefore, cybersecurity protection mainly helps objects such as computer's software and hardware, electronic data, transfer area, as well as human activity. In addition, AI is also connected to physical spaces such as autonomous vehicle, intelligent virtual assistant, so AI-related crimes can harm people physically. In this paper, we focus on the common threats in cyber space. In general, the application of artificial intelligence technology to improve security protection and management capabilities in cyberspace security can further reduce the incidence of network failures and network attack accidents, facilitate security decision-making, and improve network system operation efficiency.

2.1. Operating System Vulnerability

To protect operating system, the possibility of knowing which specific version of an operating system is running on a device can be useful. This assists in penetration tests and monitoring the devices connected to the network. Traditionally, Nmap in IPv4 can be summed up in three steps: send specific probes to the target, recollect and parse the responses. Executing a set of tests using these steps can generate a characteristic signature, and the AI system can compare the stamp with every single entry of its database of preprocessed signatures in turn [12]. The network operating system is the most likely target in network security. The simple use of scanning tools and vulnerability scripts to launch attacks that can directly bypass the OS' own security is caused by technical problems such as the source code and setting errors of the operating system itself. Therefore, when building a smart campus network, we should pay attention to the construction of infrastructure equipment, select operating systems with good security, launch update patches during use, strengthen user login authentications, control user permission restrictions, and prevent illegal access and disclosure of important information. If these requirements are not met, there will be serious consequences.

2.2. Computer Virus's Vulnerability

There are various types of computer viruses, some are fast spreading or have a high resource consumption rate or created only to steal the users' private information, which brings great trouble to users. Advanced robot systems are more prone to a variety of cyber-attacks that target their data or (operating) their systems' confidentiality, integrity, availability, authentication, and/or privacy [27-29].

In the current nonlinear computer network topology environments, basic network security measure is to have the user install genuine and mainstream antivirus software, download qualified application software, and make basic deployment of terminal security protection. The effects of the protection process are not obvious, and it is impossible to trace the source of the problem and solve the problem fundamentally.

2.3. Human Resource Vulnerability

Recent study presents there are a number of legal issues and human rights challenges related to AI [30]. It is a common problem that managers do not pay enough attention to network and information security. In addition, if the as-is system is poor, the protection effect is low, therefore, network protection mainly relies on security equipment.

Especially in today's increasingly serious crime problem on the Internet, in order to protect the user's information security, the people must have strong response and defense capabilities. At present, the issue of network security is the focus of attention, because of the complexities of human responsibility and system capacity in cybercrimes, then cyber security methods are becoming more robust and intelligent. Smart campus refers to the facilities, applications and technologies needed to provide advanced applications and services to campus users who are people performing multiple tasks in campus life.

Refinements of the management strategy allow illegal logins on the network to a certain extent, and access rights can be obtained through trojan horses, and this ultimately leads to the leakage of key information.

3. Characteristics of AI Smart Campus

In recent years, AI has become a hot topic in the scientific community, and artificial intelligence technology has gradually entered fields such as vision, bringing convenience to people's education, production and life. These challenges of AI greatly increase the change of strategic decision making in campus management. Real-time data is also used to optimize the delivery of building services (heating, ventilation, lighting), thus saving energy [13].

3.1. On Trend of Smart Campus

Universities of the world are focusing on the rapid development of 'smart campus' to overcome challenges. Universities confront the uncertain demands of education facilities; therefore, they tend to use the AI based education technology to better manage them.

With smart campus tools, universities improve the efficient use of their facilities including buildings, laboratory tools, teaching spaces in the short term, by measuring the use of these spaces in real time and guide students and employees to available spaces that match their needs. There are high requirements for artificial intelligence with strong procedural thinking, which requires computer programs to have the ability to think similar to humans. Hence, this trend provides the best information technology selection and favorable infrastructure guarantees in colleges and universities in the new era.

3.2. On the Significance of the Security AI Smart Campus

The significance of the AI secure smart campus may be measured by achieving certain objectives. These services can improve environmental sustainability, reduce operational costs, make communication and education easier and better. Therefore, we define that the smart campus is not only about deploying smart platforms to effectively perform computer related services.

Ensuring the reliability of data within the system is the main goal of network security. Another function is to provide reliable services for campus users. With the continuous progress of science and technology, users are gradually becoming aware of network use. The benefits of the AI enabled campus system has put forward higher requirements for the network security environment.

With the increasing number of cybercrimes nowadays, to protect the user's information, the computer must have strong response and defense capabilities. Presently, the issue of network security is the focus of attention. Because of the complexities in cybercrimes, cyber security methods must become more robust and intelligent. Smart campus refers to the facilities, applications and technologies needed to provide advanced applications and services to campus users who are people performing multiple tasks in campus life.

In general, AI technology is a key guarantee for users' information security. More information data processing methods can use artificial intelligence skills, not only to efficiently monitor and process unknown information, but also to provide managers with information that aid in effectively maintaining network and information system security,

4. Capacity Analysis of AI Cyberspace Security Systems

4.1. Outstanding Fuzzy Information Processing Abilities

Through the comparative analysis with other cyber defense technologies, the processing of ambiguous information contents is still relatively obvious, and it can detect unknown problems [1]. Due to risks such as unknown sources and viruses, it is difficult to ensure the security of users' basic information during the actual operation of the Internet at this stage. However, AI technology can predict this unknown source, make the information content clear, realize scientific and reasonable identification on this basis, assist users to take scientific and reasonable response methods, and effectively avoid serious infringement of user information [2].

4.2. Highly Collaborative Abilities

In contemporary society, the scale of the Internet is expanding rapidly, and its structure is very complex, which makes Internet cyber defense more difficult [3]. It is difficult for relevant managers to comprehensively deal with related issues when they lack scientific and reasonable assistance when they are busy dealing other work [4]. During this period, the network security management situation shall be broken down, and relevant security practitioners shall be responsible for the work. Making full use of AI technology can strengthen the unity and cooperation among security practitioners, and it gradually improves the level of the cyber defense. This plays an important role in promoting the healthy and sustainable development of my country's Internet industry [5].

4.3. Has Nonlinear Capabilities

With the rapid development of Internet technology, the Chinese cyberspace structure is becoming complex, and there are still a series of problems and deficiencies in network security defense management [6]. If the network structure is scalable, it will cause the network to become a nonlinear object. For this phenomenon, traditional control methods are still unreliable. This requires the full application of AI technologies to assume the role of non-linear processing. AI technologies allow to endow border protections and terminals with more detailed control strategies and more accurate for killing capabilities in terms of prevention, defense, detection. In addition, AI base security technologies have responsibilities to improve the quality and level of network security defense.

4.4. Resource Consumption Capabilities

A comparative analysis with previous network security defense technologies shows that traditional network security technologies consume big chunks of energy, however, AI technologies have high quality and effects [7]. In the actual management process of network cyber defense at the current stage, it is necessary to make full use of advanced AI technologies, so that the cost and expenditure are relatively smaller than the traditional methods.

The application of AI technologies, calculation methods can be better controlled and managed [8], a one-time accounting of data information can be performed to ensure the use efficiency and quality of data information and better control of loss.

5. Analysis of AI Applications in Cyberspace Security

Through the extensive application of the following six technologies, the level of cyber defense has been effectively improved, and the information security of users has been better protected, which plays an important role in the comprehensive and stable development of China network industry [9].

5.1. Application of Intelligent Firewall Technology

Today, among many network cyber defense technologies in China, firewall technology is a relatively common. However, this method is also divided into many types, and only a few methods can play a role in practical applications [10]. If AI technology and firewall technology can effectively integrate, the problems and deficiencies of firewall technology can be better solved [11]. Therefore, relevant management should use intelligent methods to analyze data and information, and then make decisions accordingly. This way, the security access situation of data information can be set, and it can be protected in many aspects. It can also protect the network from the invasion of viruses [12]. Therefore, in order to ensure the level and effectiveness of network cyber defense, it is necessary to make full use of advanced intelligent firewall technologies to protect users' relevant information.

5.2. Application of Intrusion Detection Technology

The Intrusion Detection Technology (IDT) in the cyber space is diverse and rich, and the applicational value of AI technology becomes more important. Presently, intrusion detection software is favored by many Internet users, which effectively broadens the practical usages [12]. It is very important to use AI technology, and its advantages are obvious. The main feature is that, under the premise of effectively detect intrusion, administrators need to monitor and manage network information content in various aspects, and distinguish network information in a relatively short time. This gives room for viruses that steal data, tamper with system settings, etc [13]. Therefore, in order to effectively ensure the security and reliability of network information, when using intrusion detection technology, users should use IDT reasonably, and timely remind users when intrusions occur.

5.3. Application of Anti-spam System

The actual operation of network software adds many problems to users, the most obvious of which is spam [14]. If the user's network security defense measures are unscientific and unreasonable, criminals may also attack the user's computer. Such methods will not attract people's attention, and the effectiveness of hackers are very high. However, in order to better deal with this kind of attack phenomenon, it is necessary to generate corresponding intelligent reports in the process of network security defense, and directly transmit the report content to users [15]. By doing this, users can take reasonable measures to effectively improve their network security. Therefore, users should also apply the anti-spam system to the network defense to effectively improve the defense level and effect.

5.4. Application of Neural Network Technology

Trusted neural networks are usually composed of several simple information processing units, have strong fault tolerance and learning abilities, and can efficiently perform distributed access to information. The neural network can realize a variety of specific information and data processing requests in the application process, to achieve the autonomous combination of knowledge; At the same time, because the computing power between neurons in the neural network is relatively independent, and parallel all software can improve its processing performance. In the field of network intrusion detection, neural network technology is more used in network security defense. It can detect and process a large amount of spam or malware in the network [16]; in the agent decision algorithm, the application of neural network technology can significantly enhance the effectiveness of network detection, and can more effectively avoid many errors. In addition, the detection of network worms can also be solved by using neural network technology. Compared with the traditional detection method, this method is effective and accurate. Presently, the research on neural network technology is more and more in-depth, and some related fields have made significant progress. Its application in cyberspace security defense is becoming more and more common, which provides sufficient impetus for the development of network security defense [16].

5.5. Application of Multiple Agent System

Agent technology is a technology in distributed artificial intelligence. It has high intelligence and automation capabilities. It can use sensors to understand the changing trend of the surroundings. The multi-agent system technology has been quite perfect, and is more used in cyberspace security defense. Since these technologies have the functions of environmental cognition and planning, they are also more used in network trend cognitions, attack detections, and etc. Presently, multi-agent systems have begun to be used in security drills in cyberspace. For example, the DECIDE environment is a distributed environment that supports security decision-making drills in my country. People can use multi-agent technology to model the relationship between each other, and then carry out Interaction with people, etc. JIAC technology takes service as the main purpose, and builds a network security simulation environment. After a network attack incident, people can evaluate the development of the situation and find out appropriate preventive measures. At present, the use of agent technology can solve many problems in the cyberspace and further improve the network security defense capability [16].

5.6. Expert System

Expert system is a new type of artificial intelligence technology. It is generally used in the construction of knowledge bases and inference engines. It can logically reason professional knowledge in a certain field, and then analyze the problem by imitating the thinking methods of human experts. However, in the process of expert system reasoning activities, a relatively complete knowledge base must be built.

Artificial intelligence expert systems can only complete reasoning behaviors in the existing knowledge bases, so the reasoning behaviors have to be in the existing knowledge bases. Presently, in cyberspace security, the expert system has a lot of applications, and is also an important part of the development process of China's cyberspace security structure.

In recent years, with the advancement of information technology, the expert system has been constantly updated, which can flexibly use different data methods to analyze users, therefore forming a behavior description mode for user groups with different permissions, so as to facilitate network intrusions on user behavior through subsystems identification.

6. Design of Smart Campus Network and It's Information Security Protection System

We took a university for the subject of our case study. The university is jointly built by the provincial people's government, the State Administration of Traditional Chinese Medicine and the Ministry of Education. Its teachers and students are distributed in two different campuses, respectively equipped with network computer rooms, both of which are stable. The designed smart campus system architecture is shown in Figure 1. As a result of smart campus construction planning, the basic principles such as achievability, manageability, scalability, system balance, etc., are carried out from the aspects of network and information security, resource sharing and service, intelligent system control and operation and maintenance management.

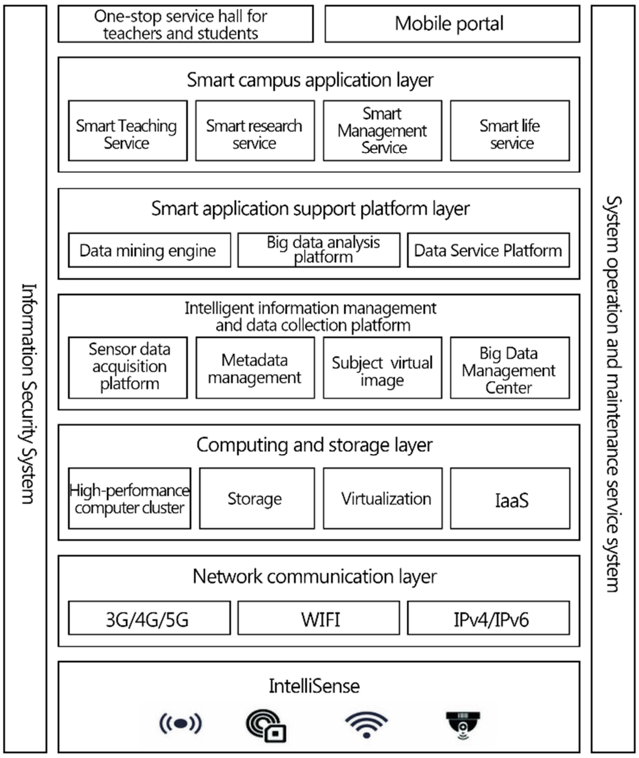
One-stop service hall for teachers and students
Mobile portal
Smart campus application layer
Smart Teaching Service
Smart research service
Smart Management Service
Smart life service
Smart application support platform layer
Data mining engine
Big data analysis platform
Data Service Platform
Intelligent information management and data collection platform
Sensor data acquisition platform
Metadata management
Subject virtual image
Big Data Management Center
Computing and storage layer
High-performance computer cluster
Storage
Virtualization
IaaS
Network communication layer
3G/4G/5G
WIFI
IPv4/IPv6
IntelliSense
Information Security System
System operation and maintenance service system

Figure 1. *Smart campus system architecture.*

The network and information security assurance system are divided into six aspects: management security, network security, host security, application security, data security, and other security assessments [17-18], as shown in Figure 2.

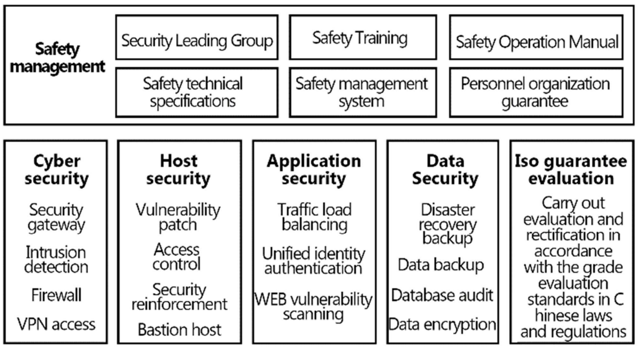

Figure 2. *Network and information security assurance system architecture.*

Combined with the architecture design of the smart campus and the construction of the information security assurance system, a dynamic and efficient security protection system is designed and deployed through the following three basic aspects.

6.1. Building an Artificial Intelligence Network Security Platform Architecture

By building an artificial intelligence network security platform, it can further penetrate into the cyberspace, deeply perceive potential risk factors in different cyberspaces, and can also adapt to higher-level security measures. In the process of configuring the AI network platform, it is necessary to accurately connect the AI system with the expert knowledge resource base, and gradually improve and optimize the functions.

Security provides a powerful, self-learning knowledge base. While building the architecture of the AI enabled security platform, it is also necessary to ensure the overall coordination between AI judgment and auxiliary decision-making capabilities. By building an AI network security platform with a unified data standard, it is possible to improve functions in the local cyberspace security system, and solve the security vulnerability threats and hidden dangers in the cyberspace in a timely manner.

6.2. Deployment and Configuration of Security System

Deploying and configuring AI systems with cyberspace security mechanisms can ensure the quality of security. Some security mechanisms in cyberspace may not be adapted to the current topology of homogeneous and heterogeneous computer networks. In this case, the hidden security problems may affect the implementation of the security system. By deploying and configuring security measures, it can further promote the process of AI, and ensure the stability of the user's network operating environment. Security measures, such as network firewalls and virus firewalls, can have strong effects, and can quickly adapt to the real-time sharing mode in cyberspace. Thus, laying a secure foundation for data collection, exchange and sharing. However, while deploying and configuring security measures, network users still need to pay attention to the security inspection steps of the computer network operating environment.

6.3. Security Hardening Models for Nonlinear Networks

The security enhancement mode of the nonlinear network can supervise the whole process of the application and ensure the stability of the local cyberspace operating environments. Non-linear networks have different processing modes for structured data and unstructured data. Both ends of communication data will carry security risks. Therefore, the security enhancement mode of non-linear networks can use the depth perception and classification judgment operations of artificial intelligence technology to centrally solve the hidden security problems in cyberspace.

7. Analysis on Application of AI in the Smart Campus Network

7.1. Smart Interception of Spam

The penetration rate of the Internet is getting higher, and the average user can use the campus Internet to connect to the network at any time. For common spam emails such as opening mailboxes of unknown origin that contain trojan horses, phishing backgrounds. These actions inevitably lead to greater security risks. The application of AI technology can deal with this problem more efficiently [19], using intelligent methods such as intercepting spam to make reliable big data analysis, evaluation of the content of users' emails, and send relevant interception reports to users, therefore, it can actively assist users to determine whether the mail is safe, nor greatly improve the convenience of users' daily use.

7.2. Smart Firewall

In network security management, firewall is also a fairly common technical solution, but the practice in recent years has proved that there are still very few safe firewalls [20]. With the addition of AI technology, the application of AI enabled firewall technology has a strong protective effect. In recent studies, comprehensive analysis came up, hence, intelligent strategies will be used to deal with security issues [21]. It can also be said that intelligent firewall plays an important role in the security protection system of the cyberspace structure.

7.3. Intrusion Detection

IDS is also a reliable technology to ensure network security and has broad application prospects in many industries [22]. At present, IDS technology has been explicitly introduced in China's relevant regulations on information security. In order to protect their key data, many colleges and universities have begun to equip intrusion monitoring tools, and the application of artificial intelligence technology has greatly promoted the application process of this key technology [22]. It can accurately judge various types of information on the network. Once the intrusion is found, it can be stopped in time, thereby preventing virus intrusion more effectively. Intrusion monitoring can use the combination of AI technology to help the entire campus network, so that the network can run smoothly and safely. It also greatly enhances the stability of users' Internet access, thereby reducing the risk of illegal intrusion and various economic losses [23]. IDS has achieved remarkable results in the development of artificial intelligence, and its wide application in cyberspace security protection also shows extremely high value [24].

7.4. Establish a Biometric-Level Identity Authentication Platform

There are also many problems in the traditional campus system, among them, the traditional login identification system is a more prominent problem. This system adopts the password authentication method. With the development of network attack technology and daily access records, the password authentication method is very easy to be stolen and cracked by criminals, and the risk of identity management is increasing with the passage of time. The introduction of the AI enabled biometric system in the new generation can just make up for the shortcomings of the campus. For example, using face recognition technology, when everyone accesses the campus Internet, the system will use hardware devices such as cameras to detect faces, and the background system will check if the face matches registered users. Now face recognition technology has begun to be widely used in various scenarios in China. With the increase in the number of school or campus Internet service modules, the requirements for user identity in the school Internet service are more stringent, and the risk of business identity to the access network is also greater.

8. Conclusion

Under the background of the Internet information age, the functions of computer network information systems are becoming more and more diverse, the structure is increasingly complex, and there are more threats. Any security attack will cause great losses. The security defense mechanism of cyberspace is also formed to combat these cybersecurity threats. With the vigorous development of AI technology, its dynamics and the effectiveness of its actions can effectively improve network security. Although this technology started late, it is particularly important to explore more advanced methods to solve network security issues. This paper takes A college as an example to introduce a smart campus network and information security protection system and its implementation process. Through this background, people can more clearly discover the value of artificial intelligence, network security technology. We will work on the topic continuously to develop an intelligent strategy to deal with a security issues that will connect to objects such as computer’s software and hardware, electronic data, transfer area, as well as human activity.

References

[1] Cao Xiaodong. The application of neural network in computer security, Science and Technology Innovation Herald, (36): 51, 2012.

[2] Li Huai, Zhang Yong. Application of artificial intelligence technology in cyberspace security defense, Electronic Technology and Software Engineering, (22): 256, 2017.

[3] Mao Zhiyong. Application of BP Neural Network in Computer Network Security Evaluation, Information Technology, (6): 45-47, 2008.

[4] He Qian. The application of artificial intelligence technology in the development of mobile Internet. Telecom Network Technology, (02), 2017.

[5] Wang Qingfu. Research on artificial intelligence technology based on computer network technology. Wireless Internet Technology, (10), 2016.

[6] Liu Fei. Research on the application of artificial intelligence technology in the field of network security, Electronic Production, (17), 2016.

[7] Liu Fang. Research on the application of artificial intelligence technology based on computer network teaching, Computer CD-ROM Software and Application, (03), 2014.

[8] Fang Binxing. Artificial intelligence security, Beijing: Electronics Industry Press, 2020.

[9] Jia Yan, Fang Binxing. Network Security Situational Awareness, Beijing: Electronic Industry Press, 2020.

[10] Pan Xiaolei, Zhan Zhenkun, Cai Haishan. Application of data security defense system in hospital information security, China Digital Medicine, 05 (9): 86-88, 2010.

[11] Ren Bin. On the construction of information security system in modern hospitals, China Information Industry, (4): 51-52, 2011.

[12] Chapter 8. Remote OS Detection Nmap. Available online: https://nmap.org/book/osdetect.html, 2021.

[13] Balaji, B., Koh, J., Weibel, N., & Agarwal, Y. (2016). Genie: Alongitudinal study comparing physical and software thermostats in office buildings. Ubicomp, 2016.

[14] Channel Network. New trends in the application and development of artificial intelligence in the field of network security, 2018.

[15] China National Defense Science and Technology Information Center. DARPA uses artificial intelligence to help commanders in 'gray zone' conflicts, 2018.

[16] Yu Tao. Application of artificial intelligence technology in cyberspace security defense [J]. Electronic World, (06): 208-209, 2021.

[17] Ma Liang, Wang Xiaodong, Lai Xiaobo. Implementation of Smart Campus Network and Information Security Protection: Taking Zhejiang University of Traditional Chinese Medicine as an example, China Medical Education Technology, 33 (06): 711-714, 2019.

[18] Li Gengxi, Yao Jian, Niu Chen. Campus network security construction practice based on hierarchical protection system, Information Security and Technology, (04): 72-74, 2016.

[19] NetEase Technology Report. Chatbot wars: AI hackers are taking over cybersecurity [EB/OL], 2016.

[20] Yin Haozhi, Liu Tiezhi. Interpretation of artificial intelligence strategies in various countries: Analysis of the US artificial intelligence report, Telecommunications Network Technology, (2): 52-57, 2017.

[21] Zhang Yilin. Discussion on computer network management and related security technologies [J]. Reading Digest, (04): 44, 2015.

[22] Zheng Zhenqian, Wang Wei. A brief analysis of the effect of virtual network technology in computer network security, Value Engineering, (35): 196-197, 2014.

[23] Wang Qi. Research on computer network security precautions, Electronic World, (14), 2014.

[24] Liang Bo. Existing problems and countermeasures of computer network security management in colleges and universities, Computer Knowledge and Technology, (27), 2014.

[25] Shen Haiying. Analysis of computer network security precautions, Netizens World, 14: 5, 2014.

[26] Li Hongmin. University Network Security Level Protection [J]. Science and Technology Information, (17): 31, 2017.

[27] Cerrudo, C., Apa, L.: Hacking robots before Skynet. Cybersecurity Insight, IO Active Report, Seattle, USA, 2017.

[28] Vuong, T., Filippoupolitis, A., Loukas, G., Gan, D.: Physical indicators of cyber attacks against a rescue robot. In: 2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 338–343. IEEE, 2014.

[29] Chowdhury, A., Karmakar, G., Kamruzzaman, J.: Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In: Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications, pp. 1426–1441. IGI Global, 2019.

[30] Rodrigues R, SIENNA D4.2: Analysis of the legal and human rights requirements for AI and robotics in and outside the EU, SIENNA project. 2019.