Application Strategies of Artificial Intelligence Technology in Computer Network Data Security Storage

Jun Liu[1, a], Xiulai Wang[1, 2, b, *]

[1] School of Computer, Nanjing University of Information Science and Technology, Nanjing, China

[2] Nanjing Jinling Hospital, Affiliated Hospital of Medical School, Nanjing University, Nanjing, China

[a]yuruxu1099@163.com, [b]wangxiulai@126.com

Abstract

With the rapid development of science and technology, computer network technology has made significant progress. Nowadays, the application scenarios of computer network technology are becoming more and more extensive, covering various aspects of people's daily life and work. However, with the continuous growth of computer network information data, network data security issues have become increasingly prominent, highlighting the importance of safe management of computer networks. As an emerging technological means, artificial intelligence technology can provide strong support for the security management of computer network data. By utilizing the intelligent and humanized management of computer networks through artificial intelligence technology, the level of security management of computer network data can be improved. This not only can ensure the information security of individuals and enterprises but also can provide greater convenience for people's life and production. This paper studies the application of artificial intelligence technology in computer network data security storage and presents corresponding views.

Keywords

Artificial Intelligence Technology; Computer Network; Data Security Storage.

1. INTRODUCTION

In the digital age, with the rapid development of internet technology and the widespread application of big data, network security has become a global hot issue. The security storage of computer network data plays a crucial role in ensuring the safety of information transmission, protecting personal privacy, and maintaining national security. Traditional network security defense measures face various challenges, including limited processing capacity, single response measures, lack of predictiveness and proactivity, etc. Against this background, artificial intelligence technology, with its unique advantages and capabilities, provides new thoughts and methods for the security storage of computer network data.

The application of advanced technologies such as machine learning, deep learning, and neural networks in artificial intelligence is gradually changing the traditional mode of network security defense. They can not only effectively improve the intelligence level of network security defense but also show significant advantages in processing large-scale data, identifying, and defending against complex network attacks. By deeply analyzing the characteristics, advantages, and application strategies of artificial intelligence technology in network data security storage, this paper aims to explore how artificial intelligence can play a crucial role in enhancing the stability of network systems, strengthening the security of network platforms, and improving the efficiency of network data processing, while also pointing out the issues and challenges that need attention in practical applications.

As technology continues to advance and applications deepen, the potential of artificial intelligence technology in the field of network security is gradually being tapped and realized. This paper will start from the basic characteristics of artificial intelligence technology, delve into its key role and application strategies in computer network data security storage, in hopes of providing more scientific and effective technical support for network security defense.

2. CHARACTERISTICS AND ADVANTAGES OF ARTIFICIAL INTELLIGENCE TECHNOLOGY

2.1. Test of grinding fineness

Analyzing the situation practically, traditional computational processes were generally complex and energy-intensive in decoupling. The advancement of artificial intelligence technology has significantly improved this scenario. AI technology employs a new computational method, namely, control algorithms, which solve tasks by finding optimal solutions in advance and completing calculations in one go. This method not only simplifies the process but also significantly saves time and human resources, effectively reducing resource consumption. In the context of network data security storage, the application of AI technology not only lowers energy consumption but also greatly enhances the efficiency of network security management and maintenance. With its ability to complete computational tasks at once, AI technology can quickly identify network threats and take appropriate measures, effectively protecting network security. Furthermore, AI technology continuously improves its performance and accuracy through learning and self-optimization, making it increasingly widespread in network data security storage and an important direction for the future of network security.

2.2. Learning and Reasoning Capability

In traditional computer network data security storage, the processing of network information involves considerable uncertainty due to the complexity and variability of network environments. Traditional security storage technologies are often passive in defense, lacking proactivity and predictability. However, with the continuous development of artificial intelligence technology, it can effectively avoid these issues, achieving a genuine integration of network defense and theoretical knowledge. AI technology, through techniques like machine learning and deep learning, endows network defense mechanisms with basic learning and reasoning abilities. This means it can proactively identify and respond to network attacks, rather than merely defending after attacks occur. Additionally, AI technology can predict future network attack behaviors by analyzing historical data, allowing for preemptive defense measures. With the rapid growth of internet users, a vast amount of data is generated, including personal information, business secrets, and national confidential data. Therefore, efficiently processing these data and preventing data leaks and attacks is a significant challenge in the field of network security. By leveraging its learning and reasoning capabilities, AI technology can enhance the efficiency of data processing and reduce the risk of data leaks.

2.3. Strong Capability in Processing Fuzzy Information

In today's rapidly evolving internet, we face numerous risk factors, including network attacks, data leaks, and identity theft. These risks threaten personal privacy and financial security and have a severe impact on corporate operations and development. Thus, preventing network data risks is an urgent problem to solve. The emergence of fuzzy information complicates this issue further. Fuzzy information refers to uncertain, imprecise information, such as rumors and false information on the internet. Such information is often difficult to verify for authenticity and credibility, posing significant challenges to preventing network data risks. The advent of artificial intelligence technology provides an effective means to address this problem. AI technology can identify and classify fuzzy information by analyzing and processing large amounts of data. Moreover, AI technology continuously optimizes its algorithms and models through machine learning and deep learning techniques, improving its capability to recognize and process fuzzy information. Compared to traditional network security technologies, AI technology employs more flexible data modeling and reasoning methods, effectively handling fuzzy information with new technical means like fuzzy logic reasoning.

3. PROBLEMS IN TRADITIONAL COMPUTER NETWORK DATA SECURITY STORAGE

3.1. Poor Stability of Network Systems

Primarily, high human involvement is one of the main reasons leading to instability in computer network systems. In these systems, human operations are inevitable, but errors due to human factors can cause system instability. For instance, improper operations or errors during network configuration or system upgrades may lead to system crashes or other issues. Secondly, the lack of intelligence in network diagnostic systems also contributes to the instability of computer network data security systems. Many current diagnostic systems can only perform simple troubleshooting and repair, lacking the capacity for in-depth analysis and prediction. This means that when faced with complex network issues, the systems often cannot quickly and accurately locate the problem, thus missing the optimal timing for resolution. Lastly, the absence of intelligent network systems and related expert knowledge bases is another cause of instability in computer network systems. Many network systems still operate in traditional ways, lacking intelligent and autonomous capabilities.

3.2. Flaws in Network Platform Security

With the widespread application of computer networks across various sectors, although people have more channels to access information, several issues arise. Personal information is prone to exposure or even online violence, causing significant distress to individuals' lives and work, and potentially leading to financial losses. The network, while convenient, can also be exploited by criminals for activities like virus attacks, account theft, and confidential information theft. Therefore, intelligent monitoring capabilities are necessary to analyze the legality of network information and ensure network security. Additionally, while the network provides an effective means of information dissemination for businesses and individuals, problems persist. For instance, the internet is flooded with spam emails and advertisements, not only wasting bandwidth but also potentially harboring viruses that threaten network security and cause financial losses to users.

4. APPLICATION STRATEGIES OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN COMPUTER NETWORK DATA SECURITY STORAGE

4.1. Implementing Effective Systems Around AI

The importance of early database construction has become increasingly apparent in practice. If database construction is inadequate or data are incomplete, identifying virus data promptly when a computer is attacked becomes challenging, leading to serious losses. This is mainly because the development stage of big data technology inevitably includes virus attacks, and many current virus database constructions face numerous issues, resulting in poor defense effectiveness and difficulty in effectively protecting computers. To ensure optimized mobile network communication, operators need to establish a corresponding virus defense system. This can be achieved by installing virus scanning software, regularly scanning internal computer files to promptly remove viruses and Trojans threatening computer security. Additionally, timely upgrades and maintenance of computer systems are essential to enhance system integrity and security, preventing exploitable vulnerabilities for hackers. Operators need to take a series of measures to achieve this goal, such as strengthening the construction of virus databases to ensure their completeness and accuracy. This can be accomplished by collecting and analyzing various virus samples, timely updating the virus database, and enhancing cooperation with other security institutions. Furthermore, improving the performance and accuracy of virus scanning software through continuous optimization of software algorithms, introduction of new technical means, and enhanced software testing is crucial. Operators also need to enhance user security education to raise awareness and defensive capabilities. Moreover, strengthening the management and maintenance of computer systems can be achieved by regularly checking for system vulnerabilities, timely repairing them, and enhancing system security.

4.2. Enhancing the Stability of Computer Network Data Systems with AI

With the continuous development of artificial intelligence technology, its application in computer network systems is becoming increasingly widespread. Leveraging AI technology can significantly reduce human involvement and minimize errors caused by human factors, thereby enhancing the stability of computer network systems. Firstly, reducing errors caused by human factors is essential. In computer network systems, errors due to human involvement are a significant factor in system instability. Introducing AI technology can significantly reduce human participation and minimize errors. For example, in network security, AI technology can prevent network attacks and virus intrusions effectively through intelligent recognition and automatic defense, ensuring the safety and stability of computer network systems. Secondly, building intelligent network diagnostic systems is crucial. Network diagnosis is an essential aspect of maintaining computer network systems. Traditional diagnostic methods often require manual troubleshooting and repair, which are inefficient and error-prone. Introducing AI technology allows for the creation of intelligent network diagnostic systems capable of autonomously monitoring, analyzing, and diagnosing computer network systems, quickly and accurately identifying fault causes, and providing solutions. This not only improves diagnostic efficiency but also reduces manual intervention and maintenance costs. Lastly, constructing intelligent expert knowledge bases related to networks through AI technology can provide robust support for the maintenance and upgrade of computer network systems. For instance, in server maintenance, intelligent expert knowledge bases can predict and prevent failures based on server operational status and historical data, ensuring stable server operation.

4.3. Improving Network Data Processing Efficiency with AI

Firstly, intelligent big data information retrieval through AI technology can significantly reduce human involvement. Natural language processing and image recognition technologies enable AI to quickly and accurately retrieve required information from vast amounts of data, improving retrieval efficiency and saving time and resources for businesses and individuals. Secondly, intelligent network resource scheduling facilitated by AI technology can adapt to system resource changes in real-time, offering higher efficiency and flexibility. This is particularly beneficial for cloud computing and IoT applications, improving resource utilization and reducing operational costs. Thirdly, intelligent information sharing enabled by AI technology allows for efficient and multidimensional sharing of big data information. Data mining and knowledge graph technologies enable intelligent and efficient information sharing, enhancing information utilization and facilitating business collaboration for enterprises.

Fourthly, complex big data analysis performed by AI through machine learning and deep learning technologies can analyze vast amounts of data intelligently, uncovering valuable insights to drive technological innovation for businesses and research institutions.

4.4. Application of Neural Network Technology

As the internet becomes ubiquitous and information technology advances rapidly, network security issues have become increasingly prominent. Neural network technology, widely applied in network security defense, plays a significant role due to its strong discrimination and learning abilities. It can accurately identify various network intrusion behaviors through autonomous learning, enabling rapid response to network attacks. Additionally, neural networks continuously learn and optimize, improving their recognition accuracy. They can train based on historical data and new attack samples, updating their models to adapt to evolving network attack methods. For instance, neural networks can detect DDOS attacks by monitoring network traffic anomalies, identifying DDOS attacks promptly, and taking defensive measures to ensure stable network system operation. In the domain of spam email and junk message filtering, AI technology has also been widely applied. Neural networks can effectively filter spam emails and messages by analyzing textual content, sender information, and reception time, enhancing the email usage experience for users.

5. CONCLUSION

In summary, as an emerging advanced network technology, artificial intelligence plays a significant role in computer network data security storage. To maximize the benefits of AI in network security, it is necessary to research its specific technologies and methods in practical applications, continuously improving the security and efficiency of computer network operations. At the same time, attention must be paid to the development trends and challenges of AI technology, actively addressing potential future problems and challenges.

REFERENCES

[1] Wen Xianglin, Liu Quan. Application of Artificial Intelligence Technology in Computer Network Data Security Storage. Digital Communication World, 2023; 11: 148-150.

[2] Liu Wangning. Computer Network Security Defense System based on Big Data and Artificial Intelligence Technology. Network Security Technology and Application, 2023; 10: 67-69.

[3] Ma Yao. Design of Computer Network Security Defense System Based on Big Data and Artificial Intelligence Technology. Information and Computer (Theoretical Edition), 2020; 32(4): 208-209.

[4] Xu Chuyuan. Analysis of Computer Network Security Defense System Design Based on Big Data and Artificial Intelligence Technology. Digital Technology and Application, 2023; 41(07): 216-218. DOI: 10.19695/j.cnki.cn12-1369.2023.07.66..