Research on Information Security Technology under the Background of Artificial Intelligence

Li Xiaohong

Xi'an Eurasia University, 710065

Keywords: artificial intelligence; network; information security technology

Abstract: With the extensive use of information security technology and networks in people's daily production and life, people are increasingly relying on computer network technology, and it gradually evolved into an important basic support technology for industry development. Artificial intelligence technology is a new technology derived from computer and intelligent technology. The information security technology in the context of artificial intelligence can ensure the security and authenticity of information to a large extent. Based on this, this paper mainly analyzes the information security technology based on artificial intelligence background.

1. Advantages of artificial intelligence technology

1.1. With the ability to deal with uncertainty and agnostic problems

The safe use of information needs to eliminate all kinds of threats timely, so as to ensure the safe and efficient operation of the network system. Network information changes rapidly and can be quickly acquired and updated information. Information security obviously requires that no problems can occur when the information is used. If it occurs, it must be solved in time. In many cases, information is uncertain, but after the introduction of artificial intelligence, it can be scientifically and effectively dealt on the basis of ambiguous information. Artificial intelligence has the ability to handle uncertain and incomprehensible problems, it can realize resource management and control according to these so-called uncertain and inaccurate information, so as to improve the information processing ability.

1.2. With the good learning ability and non-linear problem handling ability

Different from the early information security mode, the outstanding advantage of artificial intelligence is that it has good learning ability and can gradually improve its comprehensive ability. Because of the complexity of information, if you want to quickly and accurately obtain the required information in massive information, you must have good learning ability and then obtain effective information from it. Among them, we can screen massive information, learn skills from it, learn to distinguish the simple information, deduce high-level information based on the information, and realize network information security control based on high-level information. Moreover, the degree that artificial intelligence sets is more complex, which can improve the security of information technology directly. The artificial intelligence theory can only be derived from the simulation of human beings, and its nonlinear problem processing ability is very strong, which is also the main factor for the wide application of artificial intelligence technology in information security.

1.3. Relatively low computer consumption cost

The cost must be considered when everything carrying out. Through the introduction of artificial intelligence technology, not only can improve the overall performance of the computer, but also can greatly save resource consumption. The artificial intelligence control algorithm, namely the fuzzy control method calculate very fast, and it can complete the task through the optimal solution, so as to save the resources and realize energy saving and environmental protection. Through the control algorithm, it can also optimize the information security technology and create a good precondition for its promotion and application.

2. Features of information security

2.1. Feature of integrity

Information security has distinct characteristics. The integrity feature means that the data can't be changed without authorization. Information storage and transmission should be protected from tampering or losing. This is the basic feature of information security.

2.2. Feature of confidentiality

In the information security characteristics, confidentiality is also very significant, that is, information cannot be leaked to the unauthorized users or entities and should ensure the information is sufficiently secure.

2.3. Feature of usability

The feature of usability means it can be accessed by an authorized entity and strictly in accordance with actual needs, that is, whether the required information can be stored when needed. As for the meaning of information security, it will change gradually due to different development and perspectives, and there also exists understanding difference of the information security between the administrators and users.

3. Information security threats under the background of artificial intelligence

3.1. Ethical security threats

The arrival of the era of big data has promoted the evolution of knowledge learning, cross-media collaborative processing, group integrated intelligence and autonomous intelligent system into the key to the development of artificial intelligence, and the brain-like intelligence inspired by the achievements of brain science is ready to be developed. Under the rapid development of artificial intelligence, people will get in touch with more devices and machines with autonomous control characteristics in daily production and life and face the challenges from existing laws and social ethics. In addition, the development of artificial intelligence may lead to the disappearance of some simple and repetitive types of work, which makes the employee feel resistant.

3.2. Privacy and security threats

Because of the great promotion and application of big data and sensor technology, the comprehensive portrayal of social management and economic operation entities such as human, objects, organizations starts to be derived. As far as people are concerned, independent and partial personal information extends to travel trajectory, social interaction and other related information, and real-time data acquisition and summary based on smart phones, Internet and sensor devices make the above comprehensive description data realize dynamic development. Once the data of the person being portrayed is exposed, there will be no so-called personal privacy.

3.3. Overall systematic security threats.

In the artificial intelligence system, massive data information is stored in the Cloud. After the big data analysis, the instructions are sent to the control terminal, which is a closed-loop system that integrates sense, transmission, intelligence and application. If it attacked or broke down, the security impact will be comprehensive. Even partial security risks may spread gradually which lead to more serious security threats.

3.4. Social order destroys security threats

Unlike traditional information systems, devices or machines can be controlled automatically and intelligently through artificial intelligence technology. First of all, robots, unmanned cars, airplanes and other devices or machines controlled by artificial intelligence systems have certain autonomous behaviors. When they are threatened by security, they will directly destroy the social order. Typically, if the unmanned cars are out of control, they will make serious damage to the transportation system. Secondly, the artificial intelligence system machine behavior brings unforeseen interference and influence to people in the same system, which may cause serious damage to the existing order.

4. Information security technology under the background of artificial intelligence

4.1. Security detection technology of spam mail

With the wide application of Internet technology, people use mailboxes more and more frequent, mail has become the main way of information file transmission especially at work. Moreover, when using mail, there will be some lawbreakers to exploit the vulnerabilities to transmit illegal information. If the mail is received in a way that opens the mail link, it will lead to various security threats such as computer crash or information leakage. For spam information security protection, we should use artificial intelligence to effectively protect the monitoring through the intelligent anti-spam system application can prevent the garbage tank into the internal network system. In addition, based on the garbage heuristic scanning engine, the statistical rating email information can be analyzed, and the intelligent garbage tank system can comprehensively delete the mail information in combination with the rating and organization strategy, and when the spam is detected, it will be deleted directly, so that it can prevent human error operations and effectively reduce information security threats.

4.2. Firewall security technology

In the effective application of information security technology, the firewall technology based on artificial intelligence is used as isolation control technology can compulsorily access to the internal and external communication through predefined mandatory security strategy. There are many sub-technologies in this security protection technology, such as state monitoring technology, packet filtering technology and so on. Among them, the application of packet filtering technology is mainly the selection of data packets in the network layer, the security of the data packet, the source address, the target address, etc. are detected according to the filtering logic set by the system, and finally decide whether to let it pass. Then, the application of the state detection technology is a connection state detection mechanism. In the technical application, all the data packets belonging to the same connection are used as the overall data flow, thereby forming a connection state table, which has good flexibility and security, and can effectively protect the main sentence and the security of the data.

4.3. Clonal selection fuzzy clustering algorithm detection technology

In the application of information security technology under the background of artificial intelligence, intrusion detection technology is the most critical. The application of detection technology is mainly to collect and analyze information, and take effective defense measures in time when malicious or violation of security policy behavior information is found. The effective application of clonal selection fuzzy clustering algorithm anomaly detection technology has strong intrusion detection control ability, which can improve detection efficiency to a certain extent and reduce false positive rate. As far as clustering analysis is concerned, it is mainly based on the maximum internal similarity of network information and the inter-subclass reality, grouping and establishing a clustering analysis data model. Cluster analysis is based on the sample characteristics of the sample set to construct a variety of clustering methods. It is also very important in clonal selection, mainly based on the selection algorithm constructed by the biological immune system. It combines random search and evolutionary search to establish a cloning operator, and the convergence speed is very fast. The unpredictable risk detection rate in the network information is actually a key indicator of the anomaly detection mode. When detecting, the main attack categories are Probing, U2R, and Dos. According to the specific detection results, the first two effects are better. Therefore, the Dos intrusion camouflage becomes a legal identity for information attack, which is convenient for normal data information, so the detection rate is poor, which is helpful for detecting information security unknown intrusion behavior.

4.4. Artificial neural network system and fuzzy recognition system

In the implementation of information security assurance measures, the effective application based on artificial neural network system plays an important role in ensuring information security. Therefore, the system has good resolving power, which can identify intrusion with noise or distortion, and has good self-adaptive ability. However, artificial neural network systems have different adaptation scopes from expert systems. They are based on the development of biological neural networks, so they have the ability to learn, understand, and calculate. They are faster in storing, processing, and identifying information, and can also be constructed in time series. Based on the predictive model, it can significantly improve the efficiency and level of detection of invading viruses. At the same time, the effective application of the fuzzy recognition system can quickly identify the virus and determine the type of virus accurately, which is beneficial to obtain more accurate results and ensure the security of information.

5. Conclusion

In a word, information security technology under the background of artificial intelligence is a new form of technology, which covers a wide range. And in modern society, information security has earned positive attentions from all sectors of society, and people are more and more relying on information security technology. Artificial intelligence has its unique advantages, so the organic integration of it and information security technology not only can improve the security level, but also can monitor the intrusion virus in real time, then quickly identify and control it through firewall technology, intrusion detection technology and so on, with the aims to ensure the information safe.

References

[1] Song Yang, Wang Xiaofeng, Qi Xin. Directly Facing Artificial Intelligence Information Security Threats [J]. New Economy Weekly, 2018(5):25-27

[2] Wang Haitao, Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology [J]. Network Security Technology and Application, 2018(3)

[3] Liu Fei, Application Research of Artificial Intelligence Technology in Network Security [J]. Electronic Production, 2016(17:32-33)

[4] Zhu Yanjun, Song Wenjing, Zhang Zhujun. Thoughts on Artificial Intelligence and Information Security [J]. Confidential Work, 2018(4):12-15

[5] Xiao Min, Liu Baozhan, He Xiaochen. Application of Artificial Intelligence in Information Security Risk Assessment [J]. Resource Conservation and Environmental Protection, 2016(2):148-148