Computer Network Information Security Protection Measures Based on AI Intelligent Technology

Peng Liao
Shangrao Preschool Education college, Shangrao, China
zhaoqiang20191@163.com

ABSTRACT

ABSTRACT: At present, computer network is the main application object in people's work and life. Computer network in the halo of many advantages, there are still disadvantages, because the network system is vulnerable to external and internal factors, plus their own vulnerable to attack the characteristics of the network security problems appear very easy. So you need to fully know in the implementation of the elements affecting the safety of computer network, the actual situation at the same time fusion, using scientific protection scheme, raising the level of computer network security and the user's personal property security, relates to the smooth functioning of the society, adverse effects will serious losses to the state and society all benefit. This is one of the things that makes network security information so compelling. The anxiety of network users is greatly aggravated by the frequent occurrence of various network information security incidents. Study based on the nature of network information and the protection scheme, the analysis of the network information security management research focus on the distinction between the network information, importance, security crisis source, etc., aims to help the Internet police first theoretically collecting illegal crime trace and attack network crime, smooth construction of the network environment, the security of user information security and the healthy development of the virtual space.

KEYWORDS

Big data, Artificial intelligence, Network information security

ACM Reference Format:
Peng Liao. 2020. Computer Network Information Security Protection Measures Based on AI Intelligent Technology. In *The 3rd International Conference on Information Technologies and Electrical Engineering (ICITEE2020), December 03–05, 2020, Changde City,Hunan, China, China.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3452940.3453070

1 INTRODUCTION

The application operation of human intelligence through computer simulation and expansion is called artificial intelligence. In the process of using artificial intelligence, human intelligence can be enhanced to expand, improve the sensitivity of computers, and serve people's work and life requirements through optimization. The current artificial intelligence needs to rely on computer technology for development, so that artificial intelligence can be brought into full play to drive social productivity. While artificial intelligence and computer technology are expanding hand in hand, major breakthroughs and achievements have been made in computer technology, which has promoted the update and development of computer technology. Artificial intelligence and computer technology interact and develop together. Artificial intelligence is now commonly used in social management and production. Computer network security is mainly reflected in the use of the corresponding technology in daily operation to ensure the computer system information, reduce the associated data from malicious attacks, system obstacles and other elements, to avoid information data tampering, damage, loss, etc., to ensure the smooth and safe operation of the computer system. Computer network security involved in information security, computer technology, password technology and other requirements are very high, the application of computer in the information age more and more high demand for network system, so in the information age computer network security is facing a new breakthrough. In practice for computer network security and efficiency must focus on the advance prediction of protection.[1]

2 ALGORITHM PRINCIPLE

The main theory of BP calculation method is to simulate the learning process into a virtual network with n nodes and L layers, so that each layer unit and the output information unit of the upper layer and the input information unit of the lower layer have one-to-one contact, and Sigmoid type becomes the characteristic of each unit or node. The operation flow is made simple and efficient by setting the output y. Set N samples (xk, yk)(k= 1,2... , N), assuming that the output of a node I on the sample is Oi, the input is Xk, yk represents the network output, and the output of node I is Oik. At the present stage, the JTH unit on the first layer is analyzed, and the input of node J is when the KTH sample is input.[2-3]

$$net_{ij}^{I} = \sum_{j} w_{ij}^{I} o_{jk}^{I-1}$$
$$o_{jk}^{I} = f(net_{jk}^{I})$$

Where JK represents net layer, when sample K is input, the node output of JTH cell is JK. The error function is shown below

$$E_k = \frac{1}{2} \sum_{l} (y_{lk} - \bar{y}_{lk})^2$$

ICITEE2020, December 03–05, 2020, Changde City,Hunan, China, China

ACM ISBN 978-1-4503-8866-5/20/12…$15.00
https://doi.org/10.1145/3452940.3453070

Wherein lk y is the actual output of unit J. The total error is shown in the formula

$$E = \frac{1}{2N}\sum_{k=1}^{N} E_k$$
$$\delta_{jk}^{l} = \frac{\partial E_k}{\partial nrt_{jk}^{l}}$$

So

$$\frac{\partial E_k}{\partial w_{ij}^{l}} = \frac{\partial E_k}{\partial net_{jk}^{l}}\frac{\partial net_{jk}^{l}}{\partial w_{ij}^{l}} = \frac{\partial E_k}{\partial net_{jk}^{l}} o_{jk}^{l-1} = \delta_{jk}^{l} o_{jk}^{l-1}$$

If node J is the output cell, then

$$\delta_{jk}^{l} = \frac{\delta E_k}{\delta net_{jk}^{l}} = \frac{\partial E_k}{\partial \bar{y}_{jk}}\frac{\partial \bar{y}_{jk}}{\partial net_{jk}^{l}} = -(y_k - \bar{y}_k) f\prime(net_{jk}^{l})$$

If node J is not the output unit, then

$$\delta_{jk}^{l} = \frac{\partial E_k}{\partial net_{jk}^{l}} = \frac{\partial E_k}{\partial \bar{y}_{jk}}\frac{\partial o_{jk}^{l}}{\partial net_{jk}^{l}} = \frac{\partial E_k}{\partial o_{jk}^{l}} f\prime(net_{jk}^{l})$$

To summarize the above results, there are

$$\delta_{jk}^{l} = \sum_{m} \partial_{mk}^{l+1} w_{mj}^{l+1} f\prime(net_{jk}^{l})$$
$$\frac{\partial E_k}{\partial w_{ij}^{l}} = \delta_{jk}^{l} o_{jk}^{l-1}$$

The process of crossover and mutation of the control code is obtained through the calculation of genetic algorithm. When a neuron is eliminated in the variation calculation, the corresponding weight index code will be reset to 0; when a neuron is added in the variation calculation, the corresponding weight index code will start random initialization. Because weighted exponents are programmed with floating-point numbers, new mutation operators and crossover operators need to be reset, and intersecting individuals are filtered with the probability of CP. Set the case of an individual and I first I see 1 individual conduct cross each other.[4-6]

$$\begin{cases} X_i^{i+1} = c_i \cdot X_i^i + (1 - c_i) \cdot X_{i+1}^i \\ X_{i+1}^{t+1} = (1 - c_i) \cdot X_i^t + c_i \cdot X_{i+1}^t \end{cases}$$

In the formula, tt X, Xii+ is the pair of individuals before the intersection; 111, ttXXii+++ is the one after the intersection; C I is a uniformly distributed random number in the interval [0, 1]. The algorithm implementation process is shown in Figure 1

3 SYSTEM DESIGN

The supporting platform is composed of eight units, such as management control, capital screening, online detection, security incident detection, infiltration detection, malicious code detection, vulnerability detection and security trend prediction and assessment, etc., as shown in Figure 2[7]

Because the subsystems of the supporting platform built this time are all independent individuals, which can cope with the complicated and changeable security detection and evaluation process, the flexibility of other applications of the supporting platform is improved. It is mainly reflected in the platform display that hosts each subsystem and hardware separately. In addition, each subsystem can run independently on its own computer, and start the establishment and operation of the inspection and evaluation work. This plan sets the commonly used interfaces as control, data, and

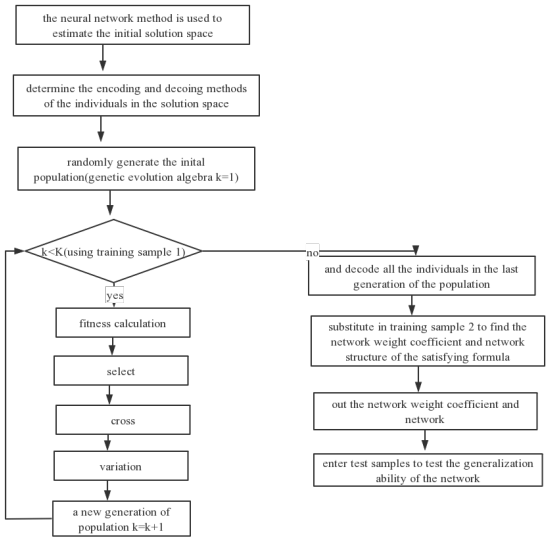

Figure 1: Flowchart of algorithm implementation

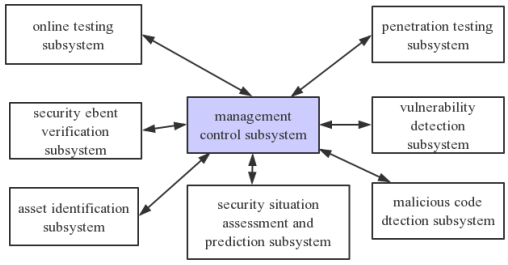

Figure 2: Components of the supporting platform

collaboration. The new support platform has a wide coverage and is generated through these subsystems and interfaces. Meanwhile, the sound third-party detection and evaluation method and the supporting platform can also be integrated. The file transfer method can use mobile storage (such as USB flash drive) as the medium to embody the two interfaces of control and coordination, and the interaction between subsystems can be represented by XML. TCP/IP protocol based on the use of data interface to transmit detection evaluation of the data.

4 SYSTEM TESTING

Gathering the required information from the rest of the tested subsystems before the subsystem starts the security event inspection is called a penetration test. Penetration testing subsystem in addition to the online detection of weak output subsystem IDS, firewall and other safety equipment information, but also provide the subsystems of malicious code detection spyware, trojans and other threaten data, and need for system provide weak weak sex

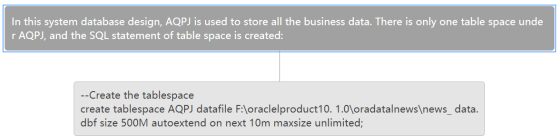

Figure 3: code

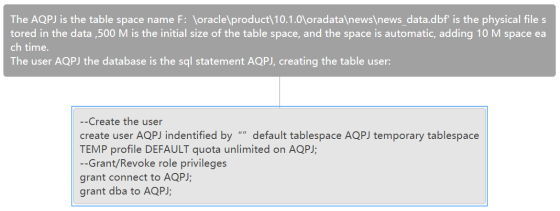

Figure 4: code

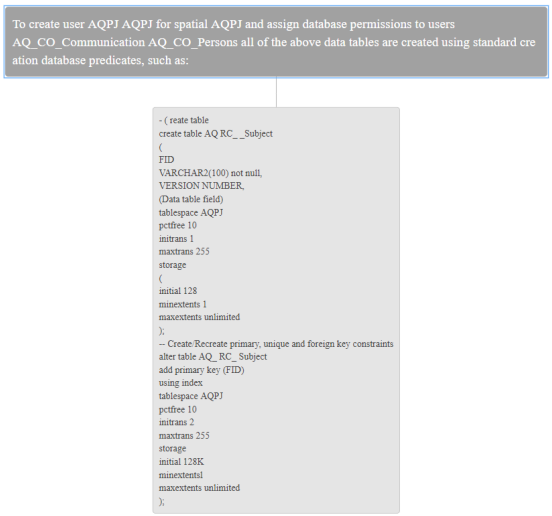

Figure 5: code

in vulnerability safety screening data offer our IDS and anti-virus system warning information and client information.

The implementation algorithm based on the above database structure is shown in Figure 3-5 as follows:

On the whole, the content of network security assessment is described, which is mainly composed of supporting platform architecture, network security assessment unit, work plan and system action unit, etc.

5 CONCLUSION

Network information storage is widely used in people's work and life. Network security should also be updated with the rapid development of network technology. Because of the previous detection efficiency, coverage area, detection system mismatch and other factors make intrusion detection become the primary focus. Now through the information identification in the artificial intelligence, expert system, neural network and the information mining system and generate a new invasion of the regulatory system to perfect the previous defects, potential network security threats and malicious invasion of the highest level can be used in detection analysis evaluation, as well as protection against malicious software invading virus harmful to computer users, improve the detection accuracy. Computer network security defense for the rapid development of artificial intelligence technology is particularly important, artificial intelligence technology to malware and effectively block, enforce the protection of computer virus invasion, to build higher quality safety protection system, artificial intelligence in computer network security using further practice and expand.

REFERENCES

[1] Yi Liu, Xingliang Yuan, Zehui Xiong, Jiawen Kang, Xiaofei Wang, Dusit Niyato. Federated Learning for 6G Communications: Challenges, Methods, and Future Directions[J].China Communications,2020,17(09):105-118.
[2] Ping Zhang, Xiaodong Xu, Xiaoqi Qin, Yiming Liu, Nan Ma, Shujun Han. Evolution Toward Artificial Intelligence of Things Under 6G Ubiquitous-X[J].Journal of Harbin Institute of Technology(New Series),2020,27(03):116-135.
[3] Yuyang Bai, Yanhao HUANG, Siyuan Chen, Jun ZHANG, Baiqing LI, Feiyue Wang . Cloud Edge Intelligence: Edge Computing method for Power System Operation Control and its Application status and Prospect [J]. Journal of automation,2020,46(03):397-410.
[4] Wenjun Wu, HUANG Tiejun, Gong Ke. Ethical principles of artificial intelligence in China and development of its governance technology [J]. Engineering,2020,6(03):212-229.
[5] Xingyuan Chen, Yuanzhao GAO, Huilin Tang, Xuehua Du. Research progress of big data security technology.[J]..Science of China: information science,2020,50(01):25-66.
[6] Linyao Yang, Siyuan Chen, Xiao WANG, Jun ZHANG, Chenghong WANG . Digital twins and parallel systems: current status, comparison and prospects [J]. Acta acta chemica sinica,2019,45(11):2001-2031.
[7] Ji Zhou,Yanhong ZHOU.Bai WANG.Zang .Cun Ji.Yuan.Human-information-physical system (HCPS) for the new generation of intelligent manufacturing [J].Engineering,2019,5(04):71-97.