Retraction

Retraction: Application Analysis of Artificial Intelligence Technology in Computer Information Security (J. Phys.: Conf. Ser. 1744 042221)

Published 16 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction.

Retraction published: 16 September 2022
Application Analysis of Artificial Intelligence Technology in Computer Information Security

Qian Ren*
School of Software Engineering, JiangXi University of Software Professional Technology, Nanchang, China

*Corresponding author e-mail: renqian_jx@ncpu.edu.cn

Abstract. With the rapid development of computerization of the network, the internet has brought an unprecedented amount of information to people and the security of computer information has become increasingly prominent. As a way to solve computer information security issues, artificial intelligence has attracted a lot of attention in recent years. Thus, through a survey, some citizens were surveyed so that people have a more realistic understanding of information security when using computers. Based on the research results, a new information security system based on artificial intelligence is proposed. Two important features have been added to the new system: intrusion detection and intelligent firewall. It efficiently detects and handles related behaviors that can impair system operation over time, protecting against advanced and complex viruses on a computer network. In addition, this article uses data mining technology and data fusion technology to strengthen the application of computer network security management. Based on the objectives of calculating information security, the safety test and the performance analysis of the schema are provided to prove the accuracy and validity of the schema. Experimental results show that the information security solutions proposed in this article effectively protect users' information, respond to information security issues in a timely manner, and respond approximately 50% faster, providing an important reference for the use of artificial intelligence in the Field of Security

Keywords: Artificial Intelligence Technology, Computer Information Security, Information Security System, Data Mining Technology

1. Introduction

With the continuous evolution of the global information process, cloud computing has become a new Internet service mode after distributed computing, parallel computing and grid computing, which has been widely concerned by the industry and the government [1-2]. Cloud computing is a computing method based on Internet. In this way, the shared software and hardware resources and information can be provided to various computer terminals and other devices as needed [3-4]. With the continuous development of computer technology, its security has gradually attracted people's attention. Many users are worried that their private data stored in computers will be leaked or illegally used [5].
Emerging artificial intelligence technology can effectively solve the problem of computer information security, so it is necessary to study the application of artificial intelligence technology in computer information security [6-7].

With the continuous evolution of the global computerization process, cloud computing has become a new model of internet services, following distributed computing, parallel computing, and grid computing, which has received broad attention from industry and government [1-2]. Cloud computing is an internet-based computing. In this way, shared hardware and software resources and information can be provided to multiple terminals and other devices when needed [3-4]. As computer technology evolves, YOUR security also gradually attracts people's attention. Many users fear that private data stored on their computer will be compromised or used illegally [5]. As artificial intelligence becomes increasingly effective in solving computer information security issues, research on the application of artificial intelligence in computer information security issues is required [6-7].

To address these problems, many researchers, both at home and abroad, have conducted in-depth studies on this and achieved certain theoretical and practical results [8]. In foreign countries, Kageyama achieved the purpose of verifying the integrity of the whole data by randomly sampling some data during the experiment, and the cloud server gathered the verification evidence into a smaller value and sent it to the verifier, thus effectively reducing the communication overhead and computing overhead. However, this scheme can only be used to verify static cloud data, and cannot support updating, adding or deleting data stored on cloud servers [9]. In China, Jin Xiaolong proposed a data integrity verification scheme supporting privacy protection. In the scheme, the basic function of integrity verification is realized based on RSA public key homomorphic label technology. After TPA initiates the audit request, the cloud server embeds the random mask into the verification evidence, and then sends the evidence to TPA, thus preventing TPA from calculating the original data information from the verification evidence [10].

The purpose of this paper is to analyze the application of artificial intelligence technology in computer information security. In this paper, firstly, through consulting relevant materials, questionnaires and other methods, we can truly understand the information security problems when people use computers. The scheme supports the data owner’s key update operation through artificial intelligence technology and proxy re-signature technology, which can effectively solve the information security problems such as identity privacy leakage caused by group sharing data. It has important reference significance for the further application and development of artificial intelligence technology in computer information security.

2. Application of Artificial Intelligence Technology in Computer Information Security

2.1 Artificial Intelligence Technology
Artificial intelligence is a branch of computer science that tries to understand the nature of intelligence and produces a new intelligent machine that can respond in a similar way to Human intelligence. Research in this area includes robots, language recognition, image recognition, natural language processing and specialized systems. Since the birth of artificial intelligence, its theories and technologies are increasingly mature and its applications continue to expand. As you can imagine, the technological products brought by artificial intelligence will be the "containers" of Future Human Intelligence. Artificial intelligence can simulate the information process of human consciousness and thought. Artificial intelligence is not human intelligence, but can think like a human and can IR beyond human intelligence.

(1) Collaboration ability
With the rapid development of science and technology, the scope and scale of computer networks continues to expand and the network structure becomes increasingly complex. A single network management no longer meets the needs of computer network development. With artificial intelligence technology, computer networks can be managed hierarchically, with levels that can be combined to further enhance network management and coordination across network management.
(2) Information processing capability
After data collection, another artificial intelligence technology, access to data, will continue to work. It associates databases, facilitates the storage of raw data in quick use, and collects and uses. Then there is the infrastructure, such as transport data storage and distributed file storage, which are common.

(3) Learning capacity
In addition to these two advantages, artificial intelligence processing has the ability to learn new knowledge, and artificial intelligence, as it is applied to computer network technology, can enter less difficult data and make logical calculations and inferences to obtain higher levels of data information, as well as significantly reduce the search time of network information and at the same time, increase the convenience of network management and further speed up network operation.

2.2 Information Security System
(1) Smart firewall
Smart firewalls provide a more efficient security check to resolve various operational issues. In addition, the application of intelligent firewalls in the security management of computer network technologies can enable advanced defense and processing of complex viruses in computer networks through its own intelligent recognition technology, which efficiently processes large volumes of data in a system, efficiently identifies and processes behaviors that could compromise system operation.

(2) Intrusion detection
Intrusion detection is an important part of network security in computer network systems and plays a very important role. Intrusion detection is primarily used to detect the security of Data Resources on computer network systems, ensuring the integrity, security, and confidentiality of computer data information features. Intrusion detection on computer network systems can use OS information and data collection and filtering capabilities to timely and effectively reflect the security status of computer network operations. Currently, artificial intelligence has been widely used in artificial neural networks and diffuse recognition.

(3) Intelligent anti-spam system
The application of an intelligent anti-spam system in computer network technology allows users to detect and manipulate spam in a short period of time, eliminating information that is easily harmful to computers and better protecting OS computer network systems from spam interference.

2.3 Technical Algorithm of Information Security System
(1) Data mining technology
Data mining technology and data fusion technology also play an important role in the application of computer network security management. The first is data mining technology. Data mining technologies enable AUDIT programs to accurately analyze and describe the characteristics of a network connection and intelligently memorize the rules relevant to the correct operation of the network, accurately identifying harmful intrusions and maximizing intrusion detection when combined with other functions.

For itemset \( X \subseteq I \), the frequency of occurrence of support itemset \( x \) in \( d \) is written as

\[
Support(X) = \frac{\text{count}(X \subseteq T)}{|D|}
\]

In which \( \text{count}(X \subseteq T) \) is the number of \( x \) contained in transaction database \( D \).

Association rule \( R : X \Rightarrow Y \), the confidence of rule \( R \) refers to the ratio of the number of transactions in which \( X \) and \( Y \) appear at the same time to the number of transactions that only appear, which is written as
Credibility reflects the probability that Y will appear simultaneously in a transaction if X is included in the transaction. The threshold of the minimum confidence level is recorded as $\text{min}_\text{conf}$. 

(2) Data fusion technology

Data fusion technology, developed based on Human ability to process your own information, and able to leverage data combinations to get more resources, enabling collaboration of Network Information Resources. The application of artificial intelligence in the management of computer network security technology allows multiple used OS to be coordinated and work together as they should, allowing each sensor system to be effectively improved, ensuring the integrity and accuracy of intrusion detection results.

The main problem solved by the fusion function is in what way and algorithm the data will be fused. The simplest methods are average method, maximum (minimum) method, intermediate method, etc. Of course, there are also more complex algorithms, which depends on the specific fusion requirements. Assuming that there are n sensor nodes in the multi-sensor data fusion system, and their output data are $X_1, X_2, ..., X_n$, the fusion function of the system can be expressed as:

$$F(X_1, X_2, ..., X_n) = y$$

In the above formula, $f$ represents the fusion function, and $y$ represents the data fusion result of these n nodes. Among them, the fusion function should have three properties: commutativity and monotony of idempotent function.

The tolerance function, as its name implies, describes the degree to which data collected by two or more tactile sensor nodes can be fused, which means the similarity of node data. The higher the similarity of data, the closer the data is, the greater the value of tolerance function. The value of the allowable function is specified in the interval $[0,1]$. When multiple data are waiting for fusion, the tolerance function is defined as follows:

$$R : X \times X \times ... \times X \rightarrow [0,1]$$

$$R(x_1, x_2, ..., x_n) = \min \{ R(x_i, x_j) \}$$

$R$ stands for the tolerance function, $R(x_i, x_j)$ stands for the tolerance results of two sensor nodes, and $R(x_1, x_2, ..., x_n)$ stands for the overall tolerance results of n sensor nodes. It can be seen that the tolerance values of multiple sensor nodes are obtained by comparing the tolerance values of every two nodes and then taking the minimum value.

3. Experimental Research on the Application of Artificial Intelligence Technology in Computer Information Security

3.1 Experimental Data

In this paper, 100 citizens were randomly investigated during the experiment, and they were counted whether they had encountered computer information security problems and which computer information security problems they had encountered. During the experiment, some dangerous information and 500 spam messages were prepared to test the intrusion detection and anti-spam system performance of information security system.

3.2 Experimental Process

First, this article conducts a survey of randomly selected citizens to obtain data on OS computer information security issues that these 100 citizens have encountered, to better understand the impact of
computer information security issues on people. Then use the information security system presented in this article to detect and process some dangerous information, as well as spam, and use the traditional computer security system to test experiments under the same conditions.

4. Experimental Analysis of the Application of Artificial Intelligence Technology in Computer Information Security

4.1 Impact of Computer Information Security on People
This article uses the questionnaire method to conduct a survey with 100 randomly selected citizens. To get data about whether they had computer information security issues and what computer information security issues. Then let OS use the information security system proposed in this article for a period of time and investigate again. The goal of the first questionnaire is to understand the types of computer security issues that people face, and the second questionnaire is to understand how computer information security issues affect people. The survey results are shown in Table 1 and Figure 1.

Table 1. Types of Computer Security Problems

| Type              | Information disclosure | Information destruction | Information virus | Access security | No problem |
|-------------------|------------------------|-------------------------|-------------------|----------------|------------|
| Not used          | 65                     | 72                      | 45                | 63             | 16         |
| After application | 24                     | 19                      | 15                | 26             | 85         |

Figure 1. Influence of Computer Information Security on People
It can be seen from the survey data that most of the citizens surveyed have encountered computer information security problems without using the information security system proposed in this paper. The most serious one is information damage, followed by information leakage. However, only 16 people have never encountered information security problems, which is very few. Computer information security issues have many impacts on citizens, mainly computer jamming. However, after using the information security system proposed in this paper, this situation has been greatly improved, and the number of citizens who encounter information security problems has decreased significantly. This is because the artificial intelligence technology used in the information security system proposed in this paper can effectively and timely detect the security problems existing in computers and deal with them.

4.2 Performance Analysis of Information Security System
In this paper, the computer with information security system can detect and process some dangerous information and spam. Under the same conditions, the ordinary computer can also carry out detection experiments, and the detection and processing effects are counted every 5 seconds. We visually express the performance of two groups of computers in detecting and processing junk files, and fit curves according to the mean value. As shown in Table 2 and Figure 2.

Table 2. Treatment of spam by two groups of computers

|                  | 5seconds | 10 seconds | 15 seconds | 20 seconds | 25 seconds | 30 seconds |
|------------------|----------|------------|------------|------------|------------|------------|
| Information      |          |            |            |            |            |            |
| security         | 65       | 124        | 195        | 270        | 345        | 452        |
| system           |          |            |            |            |            |            |
| Ordinary         | 32       | 60         | 102        | 136        | 158        | 195        |
| system           |          |            |            |            |            |            |

Figure 2. Progress of two groups of computers in processing junk files

As you can see from the experimental results, OS computers that use the information security system proposed in this article are very fast and more than double the speed of ordinary computers. This is because the detection features in the information security system apply - if AOS Artificial Intelligence information processing capabilities. Therefore, the information security system proposed in this article can identify and process unwanted files in a short period of time, based on the efficiency of information security during network operation, eliminating information that can cause computer damage, effectively avoiding spam interference, and better protecting computer network systems.

5. Conclusions
This article aims to analyze the application of AI technology in computer information security. Based on the computer's practicability, this article addresses the status of the application from the computer and summarizes the security issues of the operating system information in the computer application. Then, based on research and research results, a new information security system has been proposed by AI technology in the USA. The new system adds two important features: intrusion detection and intelligent firewall. It detects related behaviors that harm the system process in a timely manner and operating system processes effectively. In addition, this article uses mining data and fusion technologies to enhance the application of computer network security management. The development of artificial intelligence and extensive applications play a very important role in the development of...
computer network technology. Supported by AI technology, this article provides information security systems that effectively protect user information, resolve information security issues in a timely manner, and provide an important reference to the application of AI technology in computer information security.

References
[1] Kageyama, Yuuki, Maruta, Tatsuya. On the construction of Griesmer codes of dimension 5 [J]. Designs, Codes and Cryptography, 2015, 75(2):277-280.
[2] Jin Xiaolong, Wah, Benjamin W., Cheng, Xueqi, Wang, Yuanzhuo. Significance and Challenges of Big Data Research [J]. Big Data Research, 2015, 2(2): 59-64.
[3] Eisenstein, Michael. Big data: The power of petabytes [J]. Nature, 2015, 527(7576):S2-S4.
[4] Guha, Pritha. Application of Multivariate-Rank-Based Techniques in Clustering of Big Data [J]. Vikalpa, 2018, 43(4):179-190.
[5] Agunov, A. V., Titova, T. S., Kruchek, V. A., On the construction of power quality control systems [J]. Russian Electrical Engineering, 2016, 87(5):251-255.
[6] Goodin, Amie, Delcher, Chris, Valenzuela, Chelsea, Wang, Xi, Zhu, Yanmin, Roussos-Ross, Dikea, Brown, Joshua D. The Power and Pitfalls of Big Data Research in Obstetrics and Gynecology [J]. Obstetrical & Gynecological Survey, 2017, 72(11):669-682.
[7] Cook, Simon J. The Peace of Frodo: On the Origin of an English Mythology [J]. Tolkien Studies, 2015, 12(1):59-76.
[8] Nagy, Attila. Remarks on the paper “M. Kolibiar, on a construction of semigroups” [J]. Periodica Mathematica Hungarica, 2015, 71(2):261-264.
[9] Federer Lisa. Research data management in the age of big data: Roles and opportunities for librarians [J]. Information Services & Use, 2016, 36(1-2):35-43.
[10] NISHIMURA, Ataru, NISHIMURA, Kunihiro, KADA, Akiko, IHHARA, Koji. Status and Future Perspectives of Utilizing Big Data in Neurosurgical and Stroke Research [J]. Neurologia medico-chirurgica, 2016, 56(11):655-663.