Scholar Publishing Group
International Journal of Multimedia Computing
https://doi.org/10.38007/IJMC.2025.060101
ISSN 2789-7168 Vol. 6, Issue 1: 1-18

Investigation of Computer Network Information Security Supervision and Protection Strategies based on Internet of Things

Lian Xue[1,a*]

[1]*School of Computer and Computing Science, Hangzhou City University, Hangzhou 310015, Zhejiang, China*

[a]*xuel@hzcu.edu.cn*

[*]*Corresponding author*

Keywords: Internet of Things, Information Security, Protection Strategy, Security Supervision

Abstract: With the rapid development of Internet of Things (IoT) technology, the supervision and protection of computer network information security (NIS) has become particularly important. In view of backward technology problems, difficult management, and weak user security awareness in the supervision and protection of information security in traditional computer networks, this article discusses the corresponding supervision and protection strategies through the information technology (IT) of the IoT. In this paper, an effect model is established using horizontal regression and the differences between different classification levels are calculated. Regression loss is obtained through the loss function, a network intrusion detection model is established, and finally the encryption process and the output ciphertext are calculated to verify the feasibility of the model in practical applications. This paper is based on the comparative experiment of establishing traditional defense methods and NIS protection methods under the information technology of the IoT. The results show that the new security protection system under the IoT information technology has increased the perception of information security risks by 8%. The regulatory accuracy of the method studied in this paper is greater than 93. 77%, while that based on deep learning (DL) is below 92. 93%. This research not only helps to improve the protection ability of computer NIS in the IoT environment, but also provides a useful reference and reference for research and practice in related fields.

1. Introduction

Information technology has penetrated all walks of life and has gradually become an important means of enterprise management today. This has greatly promoted the improvement of production and operational efficiency. However, due to people's lack of awareness of computer network security (NS) and the increasingly frequent exchange of information in the network environment, some companies have encountered problems such as computer viruses, data leakage, and information loss or leakage. This has put a serious test on network information security engineering. This requires relevant departments to strengthen their attention and research on computer security protection and improve the security of computer systems. Therefore, it is essential to supervise and protect the information security of computer networks under the IT of the IoT.

Due to the widespread application of IoT technology, the supervision and protection of computer NIS in the IoT environment has gradually become a hot topic in research. In the IoT environment, the supervision and protection of computer NIS are facing a series of challenges. How to ensure the effectiveness of the authentication and data encryption of IoT devices, prevent data leakage and tampering, and design reasonable access control strategies? To this end, this research aims to propose effective security supervision and Protection Strategies to meet information security challenges in the environment of the IoT. The research purpose of this article is to explore computer NIS supervision and Protection Strategies under the IoT information technology and to provide effective solutions to ensure that IoT devices, sensors, and communication networks are protected from various attacks and threats. Additionally, attention will also be paid to issues such as encryption algorithms, security protocols, and key management of communication networks to ensure the security of information transmission.

The contribution of the research on computer NIS supervision and protection strategies under the IT of the IoT is mainly reflected in the following aspects：

1. Improve security: Through the security supervision and protection of the IoT information technology computer network, security threats can be discovered and resolved quickly, and the overall security of the network can be improved. This helps to protect data and information security and prevent the leakage of personal information and the loss of sensitive corporate information.

2. Enhance network stability: In the context of the IoT, computer networks need to process large amounts of data and information. Through research and implementation of protection strategies, stable network operation can be ensured and network failures caused by excessive data traffic or malicious attacks can be avoided.

3. Promote technological development: This research can support the development of IoT information technology. By solving computer NIS issues, progress and innovation of related technologies can be promoted, to better serve various fields.

2. Literature Review

Many scholars have conducted research on NIS. Chen J X analyzed factors affecting computer NS from the aspects of natural factors, man-made damage, misoperation, malicious attacks, etc., and proposed security precautions and countermeasures for computer network information under big data [1]. Zhao M used carrier aggregate (CA) technology, driver software, and access authentication technology to analyze the wireless sensor network based on the Transmission Control Protocol / Internet Protocol (TCP / IP) protocol, and performed network access restriction and access authentication functions [2]. Kansal L proposed a method based on adaptive depth detection. The intrusion detection system model was combined with the support vector machine, which could better detect the NIS monitoring system and improve early warning and defense against cyber attacks and threats [3]. Deb R proposed a comprehensive prevention strategy based on multi-source information integration technology, and introduced a multi-criteria decision-making mechanism to help network administrators determine risk indices in advance. During implementation, appropriate countermeasures were taken to avoid and reduce cybersecurity issues

[4]. Yin C combined virtualization technology and cloud computing in school NIS management and established an extensible access control model. Identity authentication and authority management were performed on all users on the virtual private network, which ensured the security protection of some important information [5]. NIS is the foundation of modern information construction, which has a huge and far-reaching impact on all of social and economic development.

IoT technology plays an important role in the field of NIS, and many scholars have done research accordingly. Wang Z studied the application of IoT information security in sports training and education informatization and proposed a video surveillance system scheme for sports teaching based on IoT security technology. Real-time transmission and storage of the movement process through the wireless network could achieve effective protection of important information resources, such as servers [6]. Yao Y developed a security authentication and management platform based on encryption and decryption algorithms. With the support of the core controller and the reconfigurable control platform, the reconfigurable encryption and decryption functions were realized, which improved the efficiency of use and the flexibility of the system [7]. Li M proposed an organizational information security framework for the human factor of IoT. Based on this security strategy, a layered data-centric security model was designed to help prevent or reduce information leakage events caused by human factors [8]. Yhl A proposed an asymmetric information encryption algorithm based on elliptic curve cryptography, and used compressed sensing to compress and reconstruct data to improve the storage speed of information in the IoT, guaranteeing information security and storage performance [9]. Liang N used asymmetric encryption algorithms and a data transmission method based on multiple access technology to propose a new packet switching mechanism in communication systems, which allowed network users to choose appropriate protocols for information exchange according to their needs and ensured the privacy of information and the efficiency of data communication [10]. The powerful advantages of IoT technology make it of great significance in privacy protection, information sharing, and security.

The research on the supervision and protection strategy of computer NIS based on the IoT IT and the methods based on DL and machine algorithms each have their own advantages, and which method to choose depends on the specific application scenarios and requirements. The method based on IoT IT focuses more on ensuring information security by monitoring and controlling system devices, such as controlling network traffic, monitoring abnormal behavior, device authentication and access control, etc. This method can make up for the deficiency of traditional security technology and is more suitable for large-scale, complex, and heterogeneous IoT systems. Based on the encryption and decryption algorithm and the adaptive depth detection method, it emphasizes the use of big data analysis and ARTIFICIAL intelligence technology to detect and defend against network attacks. This method can monitor network traffic in real time, quickly identify abnormal behaviors, automatically adjust defense strategies, etc., with high adaptability and real-time. In general, both have their own unique advantages, and in practical application, the two methods, through DL and machine algorithm to the IoT system security monitoring and protection, and using the IoT IT to control and protect the system equipment, in order to improve the security and reliability of the whole system.

With social and economic development and people's increasing demand for information, NIS is an inevitable trend of social development, and traditional protection systems can no longer meet the increasingly complex cyberspace needs. Therefore, new IT is needed to support its operation. As an emerging security protection method, the IoT has a broad range of applications in NS. Based on this, based on the IT of the IoT, this paper would analyze the NIS supervision (NISS) in the IoT environment in detail from three aspects of security management, business application, and data security, and propose corresponding protection countermeasures.

3. Investigation of NISS and Protection Strategy

The flow chart studied in this paper is shown in Figure 1.

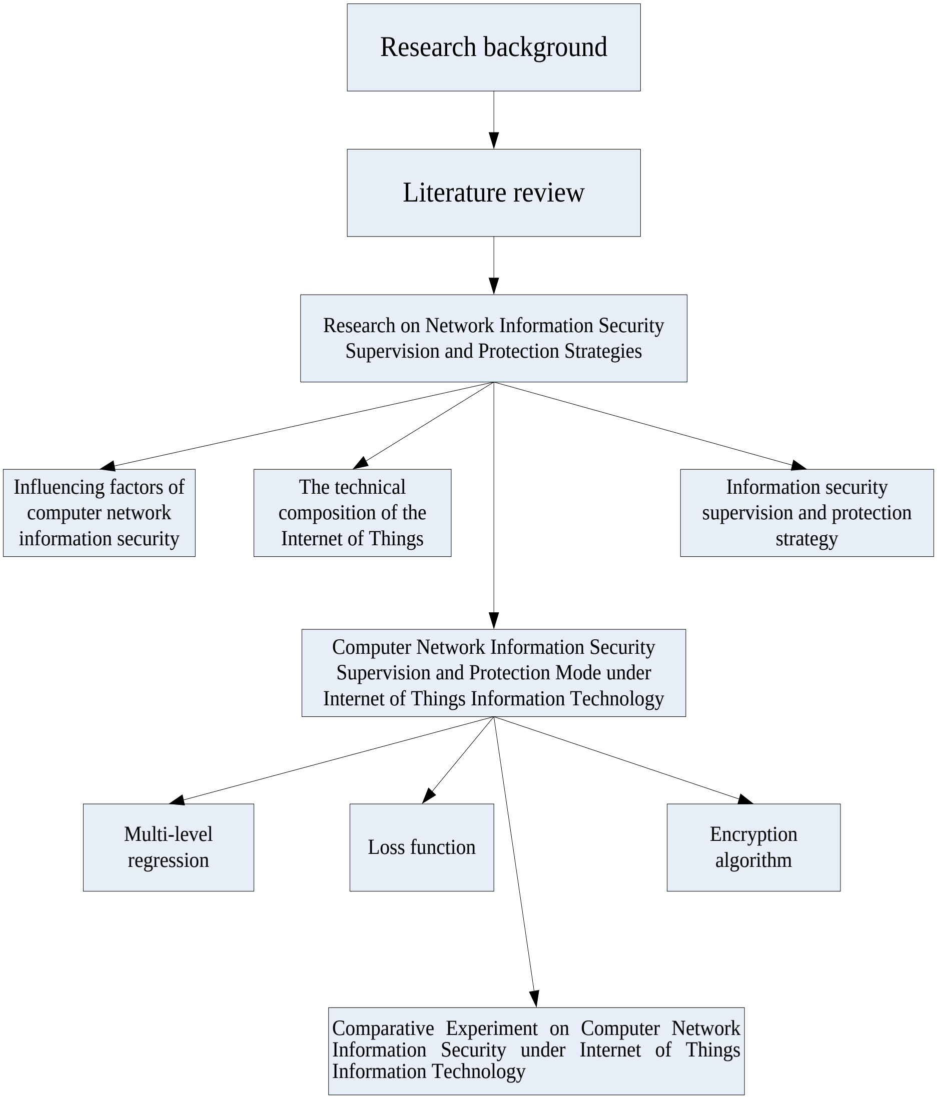
Research background
Literature review
Research on Network Information Security Supervision and Protection Strategies
Influencing factors of computer network information security
The technical composition of the Internet of Things
Information security supervision and protection strategy
Computer Network Information Security Supervision and Protection Mode under Internet of Things Information Technology
Multi-level regression
Loss function
Encryption algorithm
Comparative Experiment on Computer Network Information Security under Internet of Things Information Technology

Figure 1: Flow chart of the study in this article

Under the background of IoT IT, the research problems of computer NIS supervision and protection strategy research mainly focus on the following aspects: 1. How to ensure the security of data in the process of transmission and storage, and prevent the data from being illegally obtained, tampered with or damaged? 2. How to conduct effective authentication and access control of iot devices to prevent unauthorized devices or personnel from accessing the network. 3. How to prevent IoT devices from becoming entry points to cyber attacks and how to quickly detect and respond to cyber attacks. 4. How to protect users' privacy and prevent personal information from being abused or leaked. These research questions require a comprehensive consideration of the characteristics of IoT technology, the current situation, and future trends of NS, as well as the needs and challenges of practical applications. Through in-depth research and exploration, technological progress and application development in the field of animal Internet information security can be promoted.

(1) Influencing factors of computer NIS

With the continuous development of computer technology, NS technology is also constantly improving and progressing, and its core contents include cyberspace security and information security assurance capacity building. Due to the complex network environment, computer NIS is still a key issue in network research. In practical work, it is necessary to pay attention to the application and maintenance of NS technology to ensure the safe and stable operation of computer systems [11]. The main influencing factors of NIS are shown in Figure 2.

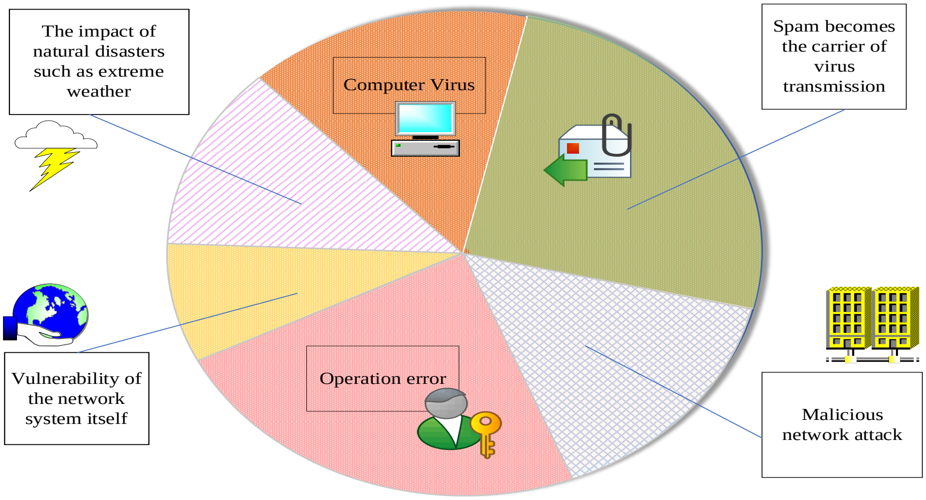
The impact of natural disasters such as extreme weather
Computer Virus
Spam becomes the carrier of virus transmission
Vulnerability of the network system itself
Operation error
Malicious network attack

Figure 2. Influencing factors of computer NIS

As shown in Figure 2, there are many factors that affect NIS. Among them, malicious network attack refers to the process in which hackers obtain important information and use it by invading computers or other electronic devices, thereby causing losses to users. Users may also cause NS problems due to their unfamiliarity with computers or momentary operational errors; computer virus is stealthy and aggressive and can destroy a system to a state of paralysis in a short period of time. At the same time, it can also scan, copy, modify, and other operations on the computer to achieve the purpose of stealing data information. Therefore, when using computer networks, protection must be paid attention to avoid the harm caused by computer viruses; spam may also become a virus carrier, and its main transmission route is to send viruses to target users through emails or text messages, or to modify and delete emails by using some malicious software on the Internet; the impact of natural disasters such as extreme weather can also cause power outages, network sluggishness, etc. In severe cases, it would cause irreparable losses to the computer system and personal safety; the network system itself may also have some loopholes, such as poor firewall function, insufficient antivirus software, etc. These all provide attackers with opportunities to cause security incidents. NIS is an important part of modern information construction and an indispensable part of enterprise management. Therefore, it is urgent to establish a sound NS mechanism, strengthen security protection measures, and improve security awareness [12].

(2) The technical composition of the IoT

In the new age characterized by computer technology and networked information technology, IoT has become one of the most active and developing fields in the information society due to its own advantages and unique functions. The IoT technology has the characteristics of strong perception, low cost, wide coverage, and strong real-time performance. It realizes information exchange by collecting and processing objects, which can not only realize real-time monitoring of objects, but also realize mutual communication with other related systems and complete the remote control of environmental status and related events. Its basic composition is shown in Figure 3.

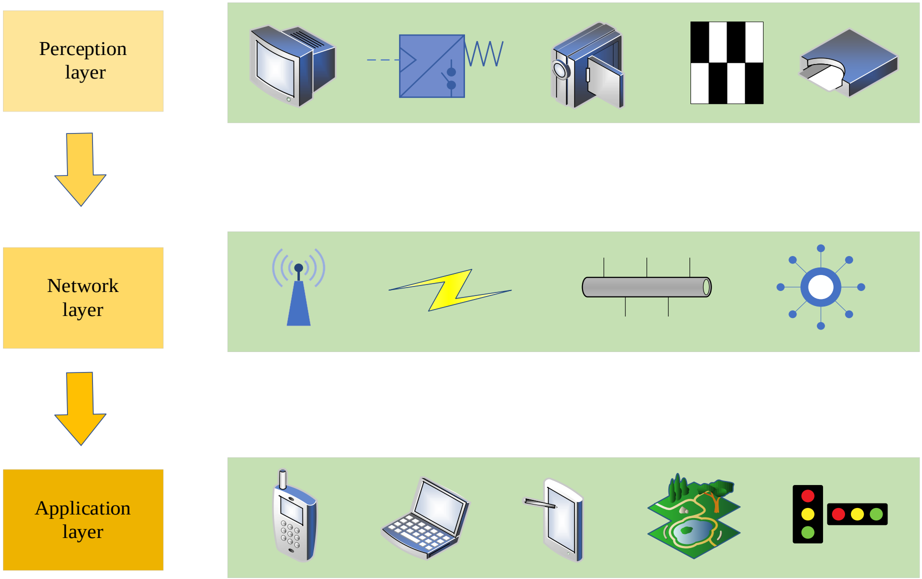

Figure 3. Basic Components of IoT Technology

IoT mainly includes three parts: perception layer, network layer, and application layer. The perception layer is the basis for information acquisition and is also the channel that connects data flow between all levels. Its main technical means are two-dimensional code labels and readers, sensors, cameras, etc., the network layer provides data access and transmission services for various sensors through transmission networks such as telecommunication networks, the Internet, and private networks; the application layer transmits the network to downstream devices to control and manage various terminals. As the core component of IoT applications, the perception layer also includes radio frequency identification (RFID) technology and communication equipment. RFID is used mainly in two aspects: One is to perform identity authentication based on RFID, and the other is to communicate with other devices through radio frequency or other means to complete data transmission, item tracking, positioning, and other functions; communication equipment is the hardware carrier of the IoT, which can transmit various information to users in real time, and is the most convenient and effective tool for connecting people and machines. The IoT technology is expanding rapidly and has a wide range of applications. The construction of a NS protection system based on IoT technology can realize control of the whole process, from data collection and transmission to analysis processing and security management. It can also reasonably combine different types and types of equipment and encrypt the data through the corresponding protocol, to achieve the purpose of effectively protecting user data and improving security [13].

The IT of the IoT has a wide range of applications in the supervision of computer NIS. Through the IoT technology, the transformation and construction of information engineering can be realized, and existing risks and security issues can be supervised in a timely manner. First, IoT technology can increase the number of public keys in nodes to prevent network attacks, thus ensuring information security and facilitating security monitoring. This can improve the security protection capabilities of the network and effectively prevent malicious attacks and data tampering. Second, IoT technology can choose suitable routes and respond to nodes scientifically to make the delivery of information and data more timely and accurate. At the same time, according to the characteristics of the wireless perception computer system and the technical requirements of the IoT, the analysis of the determined secure routing application protocol can avoid the negative effects of bad network attacks and improve the security capabilities of the IoT technology. In addition, data fusion in IoT technology is the core means, but in the process of data fusion, if the node is damaged, the fusion node may not be able to distinguish between normal information and malicious data. Therefore, it should analyze the application of information security when integrating data from the IoT. To this end, suitable fusion management measures can be formulated to strengthen the verification measures of data and information, so that users can still distinguish between normal information and malicious data even if the node is damaged. Finally, the IoT technology can also be applied to the safety supervision of specific items, the safety supervision in production, the safety monitoring of important equipment, and the emergency handling of accidents. Through the integration and application of intelligent perception, identification technology, universal computing, and ubiquitous networks, comprehensive coverage and timely response to security supervision can be achieved.

(3) Information Security Supervision and protection strategies

With the rapid development of computer technology and IT, people pay more and more attention to NS issues. NIS is a complex system engineering, which requires the support of good hardware equipment, advanced and perfect software technology, and professional talents. The NIS supervision and protection strategy under the IoT technology is shown in Figure 4.

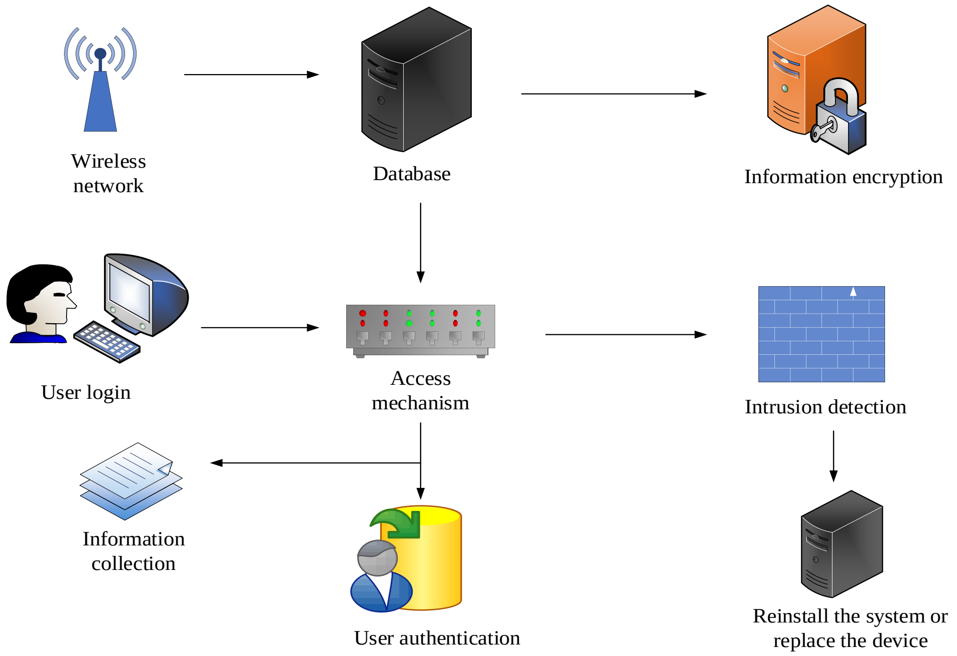

Figure 4. Supervision and protection of NIS under IoT technology

Encryption technology has been an emerging research direction in computer science and cryptography in recent years. Protects data from being stolen or tampered with through digital signatures and encryption protocols, which enable information encryption, decryption, and other functions. At present, it has been widely used in finance, telecommunications, and other industries, which has become an important development trend of computer security technology; access control is an important part of computer application system, which is mainly composed of three parts: user rights management, process access control, and network monitoring. The three restrict each other to a certain extent, but they are the premise of each other and jointly guarantee the normal operation of the entire computer software system; identity authentication is an important link in electronic communication, which can effectively prevent forgery and tampering of electronic data. Its safety and effectiveness directly affect the normal operation of the electronic system; intrusion detection and prevention are a new NS protection system developed in recent years. Its function is mainly reflected in the protection of information, the prevention of being attacked and destroyed, and helping the system repair in time after being attacked. The IoT technology is used to supervise and protect information security in the network, which can improve the efficiency of network operation and the level of security to some extent.

In the IoT environment, data security protection is crucial. Effective data encryption, backup, and recovery measures should be taken to ensure the confidentiality, integrity, and availability of the data. At the same time, the protection of sensitive data should be strengthened, and access control and audit tracking means should be adopted to prevent data leakage and abuse.

The advantages and disadvantages of the research method of computer NIS under IoT IT are analyzed as follows: Advantages: 1. Real-time monitoring: Through the IoT technology, it can collect all kinds of data in real time, find out the NIS problems in time, and improve the efficiency of security monitoring. 2. Comprehensive coverage: The distributed characteristics of the IoT enable it to cover a wider range of areas, monitor various equipment and systems, and improve the overall guarantee capacity of information security. Disadvantages: 1. Data security: The wide application of the IoT technology makes a large amount of data transmitted between various nodes. How to ensure the security of these data has become a difficult problem. 2. Privacy leakage: With the popularity of the IoT technology, a large amount of personal information is collected and processed. If this information is illegally obtained and used, it may pose a threat to personal privacy. In general, the research method of computer NIS under IoT IT has the advantages of real-time and comprehensiveness, but there are also challenges such as data security and privacy leakage. Therefore, in practical application, the corresponding security strategies and management measures should be formulated according to specific situations to ensure the security of information.

4. Research on NISS Computers under the IoT IT

Formal security analysis under the random Oracle model (Random Oracle Model, ROM) can provide a more stringent and reliable guarantee for the computer NIS supervision and protection strategy. First, identify the information assets and security goals that you want to protect. This may include confidentiality, completeness, availability, traceability, etc. Define the ability, motivation, and target of an attacker. Consider different types of attackers and use the features of random Oracle to provide a security proof for your security strategy and mechanism. This can be done with the reduction method, which proves that your security policy is safe in the ROM, and also in real environments. Through the above steps, using the random Oracle model for the formal security analysis, it can provide a more rigorous and reliable guarantee for the computer NIS supervision and protection strategy. This helps to reduce security risks, improve the security of information systems, and ensure the security and privacy of user data.

(1) Multilevel regression

Multilevel regression is a new type of statistical method, which is based on the study of the relationship between data and obtains the degree of correlation through the existence of causal relationships between variables in the original data. It has certain advantages in the design of prediction models.

Physical security of network devices can affect NS, and NS can affect data security. This hierarchical relationship cannot be handled simply by traditional regression analysis methods, and the multilevel regression analysis method is just an effective tool for this problem. Moreover, the multilevel regression analysis method is also able to consider interactions and effects between different levels in the model, in order to better explain and predict dynamic changes in information security in computer networks.

When the dependent variable n is continuous, the mixed effects model is established as follows:

$$d_{ij} = \partial_0 + \partial_1 n_{ij} + \lambda_j + a_{ij} \quad (1)$$

When the dependent variable does not conform to a normal distribution, the random effects models are obtained.

$$D^{-1}(\pi_{ij}) = \partial_0 + \partial_1 n_{ij} + \lambda_j \quad (2)$$

$$\pi_{ij} = E(d_{ij}) \quad (3)$$

In the formula, λ_j is the random intercept, and its value range is a natural number; D^{-1} is the link function.

When the dependent variable is binary, the logit link function is used and the formula is as follows:

$$\log(\frac{\pi_{ij}}{1-\pi_{ij}}) = \partial_0 + \partial_1 n_{ij} + \lambda_j \quad (4)$$

Among them, ∂_0 is the log probability of d=1 when n=0 and λ =0; ∂_1 is the cluster-specific effect, which represents the effect of ∂_0 for every 1-unit increase in n when the value of λ is the same.

The difference between the different grades for each category is calculated as follows:

$$C_{ij} = \frac{S_j}{J_i} \quad (5)$$

In the formula, S_j represents the number of real targets in class j; J_i is the reference base of class i.

Common experimental platforms include a variety of IoT devices and systems, such as smart home systems, intelligent agriculture systems, intelligent transportation systems, etc. These platforms can be used to test and validate the effects of various regulatory and protection strategies for information security. Data set: In the experiment, various data sets need to be used, including sensor data, network traffic data, user behavior data, etc. These datasets can be collected through experimental platforms or actual IoT systems, or using publicly available or self-built platforms.

(2) Loss function

The loss function refers to the quantitative relationship formed by the mutual connection and interaction between one or more results generated by an event under certain conditions. When a system fails, external factors cause changes in system parameters, which is a measure of risk [14]. The formulas are expressed as follows:

$$L = (Y, f(x)) \quad (6)$$

$$\theta = \arg\min \frac{1}{N}\sum_{i=1}^{N} L(y_i, f(x_i, \theta) + \alpha(\theta) \quad (7)$$

Network loss is defined as:

$$P(c_{ij}, d_{ij}) = \frac{1}{N_k}\sum_{i=0}^{I}\sum_{j=0}^{J} P_k(c_{ij}, c_{ij}^*) + \mu \frac{1}{N_r}\sum_{i=0}^{I}\sum_{j=0}^{J+1} R_{ij}^* P_r(d_{ij}, d_{ij}^*) \quad (8)$$

$$P_k(c_{ij}, c_{ij}^*) = c_{ij}^* \log(c_{ij}) + (1 - c_{ij}^*)\log(1 - c_{ij}) \quad (9)$$

$$R_{ij}^* = \{0,1\} \quad (10)$$

In the formula, P_k is the classification loss; c_{ij} is the prediction probability of the technology of the i-th class j-class technology; when c_{ij}^* is 1, it means that the j-th class and the cardinality of the i-class are positive samples; when c_{ij}^* is 0, it represents a negative sample; d_{ij} is the regression result of the predicted value relative to the base level i of class j.

The regression losses are calculated as:

$$P_r(c_{ij}, c_{ij}^*) = S(c_{ij} - c_{ij}^*) \quad (11)$$

$$d_{ij} = \log(\frac{S_j}{J_{ij}}) \quad (12)$$

$$d_{ij}^* = \log(\frac{S_j^*}{J_{ij}}) \quad (13)$$

According to the above calculation model, an intrusion detection system can be constructed. In the event of information leakage and other problems, it would automatically send warning messages to users. For the system to perform as it should, continuous improvements are required to ensure data integrity and security and prevent false positives and false negatives while improving performance.

In the supervision and protection mode of computer network information security(CNIS) and protection under the IoT IT, the reason for choosing the loss function is that it can effectively measure the difference between the prediction results of the model and the true value, so as to evaluate the security performance of the model. Specifically, the function of the loss function is as follows. The loss function can evaluate the accuracy and prediction effect of the model by calculating the difference between the prediction results of the model and the true value. The smaller the value of the loss function, the closer the model predicts to the true value, the better the performance of the model. The loss function focuses not only on the prediction accuracy of the model, but also on the risks that the model may produce. In some scenarios, the model needs to trade off accuracy and security, and choosing the loss function can help us better measure this balance.

Accuracy is calculated as follows:

$$A = \frac{MN + MT}{PN + PT + MT + MN} \quad (14)$$

The detection rate (DR) is calculated as follows:

$$DR = \frac{MT}{PN + MT} \quad (15)$$

The False Positive Rate (FPR) is calculated as:

$$FPR = \frac{PT}{MN + PT} \quad (16)$$

In the formula, MN means that the predicted value is the same as the actual record; PT means that the predicted value is abnormal and the record is normal; PN means that the predicted value is normal but the record is abnormal; MT means that both the prediction and the record are abnormal.

Evaluation criteria are used to measure the performance and effectiveness of information security regulatory and protection strategies. Common assessment criteria include precision, recall, F1 score, AUC-ROC, etc. In addition, other evaluation criteria can also be considered, such as time of strategy implementation, resource consumption, security, etc. In the experiment, it should be necessary to pay attention to the following points: 1. To ensure the fairness and repeatability of the experiment, that is, the experimental conditions and parameters should be clear, the experimental process should be open and transparent, so that others can repeat the experiment and verify the results. 2. Ensure the authenticity and integrity of the data, that is, the data used should be the real data of the actual IoT system and the data should not be tampered with or damaged in the collection and processing process. 3. Compare experiments and benchmarks, that is, with other known or commonly used methods, to evaluate the performance and effect of the proposed new strategy.

(3) Encryption algorithm

The IoT security encryption algorithm is based on traditional cryptography methods, with the aim of ensuring the security and reliability of IoT applications to ensure data security. The encryption algorithm SM_4 has the advantages of confidentiality, high scalability, and high availability. Currently, most enterprises have adopted this encryption protocol as a system-level solution. However, in practical applications, targeted design and optimization must be carried out for different application environments [15].

The deserialization transformation method is defined as follows:

$$A(a_0, a_1, a_2, a_3) = (a_3, a_2, a_1, a_0) \quad (17)$$

Encryption process:

$$Q_{n+4} = F(Q_n, Q_{n+1}, Q_{n+2}, Q_{n+3}, ic_n) \quad (18)$$

$$Q_{n+4} = Q_n + T(Q_{n+1} + Q_{n+2} + Q_{n+3} + ic_n) \quad (19)$$

The output ciphertext is:

$$(Z_0, Z_1, Z_2, Z_3) = A(a_{32}, a_{33}, a_{34}, a_{35}) = (a_{35}, a_{34}, a_{33}, a_{32}) \quad (20)$$

Among them, ic_n is the round key and $i = 0,1,2,...,31$.

5. Comparative Experimental Analysis of CNIS

(1) Experimental method

From network users, 50 participants in the questionnaire are randomly selected to conduct a computer NIS survey. The results of the survey are analyzed and are shown in Table 1.

Table 1. Analysis of the survey

Age distribution	Number of people	Percentage
under 20 years old	3	6%
20~35 years old	19	38%
35~50 years old	21	42%
over 50 years old	7	14%

The questionnaire survey population is divided into 4 categories according to age. Among them, there are 3 users under the age of 20, accounting for 6% of the total; 19 users between the ages of 20 and 35, accounting for 38% of the total; there are 21 users aged 35-50, accounting for 42%; 7 users over the age of 50, accounting for 14%. However, after the age of 50, people's attention to safety issues would gradually decrease. Overall, users of different age groups have relatively different needs in terms of network access security, and users in the 20-50 age group are the main group of people in this survey. Therefore, this paper selects two representative age groups, 20-35 years and 35-50 years, as the data source group.

The two representative age groups of 20 to 35 years and 35 to 50 years were chosen as data source groups due to significant differences in the use of networks and IT. The 20 – 35 age group is generally more familiar with new technologies and social networks, while the 35 – 50 age group may be more focused on safety and stability. By comparing the data of these two age groups, we can better understand the behavior and awareness of users of different ages in NS, to develop more targeted security strategies. Traditional defense means may include firewalls, intrusion detection systems, virus protection, etc. These methods are widely used for their defense against cyber attacks. With the development of technology, new defense means are also emerging, but traditional means still play an important role in the field of NIS.

According to the results of the analysis, 40 valid questionnaires are obtained. The 40 people are equally divided into 4 groups to design comparative experiments, which are named A1, A2, B1, and B2, respectively. Among them, A1 and A2 are called group A, which uses traditional defense means to manage NIS. B1 and B2 are called group B. The security protection system under IoT IT is used to compare the two management systems in terms of perception capability, response level, and satisfaction. The experimental data are recorded and analyzed.

(2) Data analysis.

1) Perception ability

Research on the supervision and protection strategy of computer NIS supervision and protection strategy under the IoT IT is an important topic in the field of IT. As an important performance index for IoT devices, perception ability is crucial to ensure the security application of IoT IT. Measure the accuracy of IoT devices to identify external information. Evaluation criteria can be set as accurate identification rate, misidentification rate, and other indicators. The perception ability of the four groups of information security risks is compared and the score is set from 1 to 5 points. The score results are shown in Figure 5.

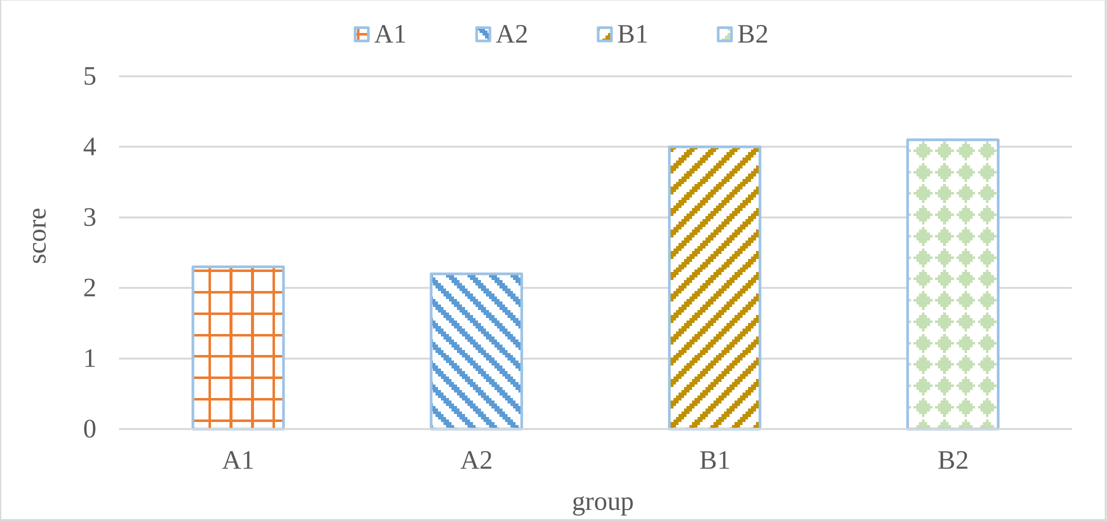

Figure 5. Comparison of risk perception abilities of the four groups

As shown in Figure 5, it can be seen that the A1 and A2 scores are around 2 points; the B1 and B2 scores are around 4 points. Overall, the score for group B is much higher than that for group A. After calculation, the average score of group A1 is about 2. 3; the average score of group A2 is about 2. 2; the overall average score of group A is about 2. 25. The average score of group B1 is about 4; the average score of group B2 is about 4. 1; the overall average score of group B is 4. 05. Therefore, group B has a stronger perception of information security risks, and group B's perception of risks is 8% higher than that of group A.

The new security protection system under the IoT IT has improved the perception of information security risks by 8%, which means that the security protection system can identify and prevent potential information security risks earlier and more accurately. This improvement can help organizations better cope with risks such as cyber attacks and data leakage and reduce the occurrence of security incidents, thus protecting their reputation and financial interests. To ensure the security of the IT of the IoT, the protection system must be continuously updated and improved to improve the perception of information security risks. At the same time, this improvement should be constantly measured and evaluated to ensure that the organization's NS is effectively guaranteed.

2) Response level

By analyzing a large amount of user data, we can understand users' reactions and behavior patterns to the information security of the IoT. Users can analyze behavior data in the face of security threats, understand their response speed, operation habits, etc., so as to evaluate their response level. When the risk is felt, the response level of each group is assessed and the score is set from 1 to 10. The results are shown in Figure 6.

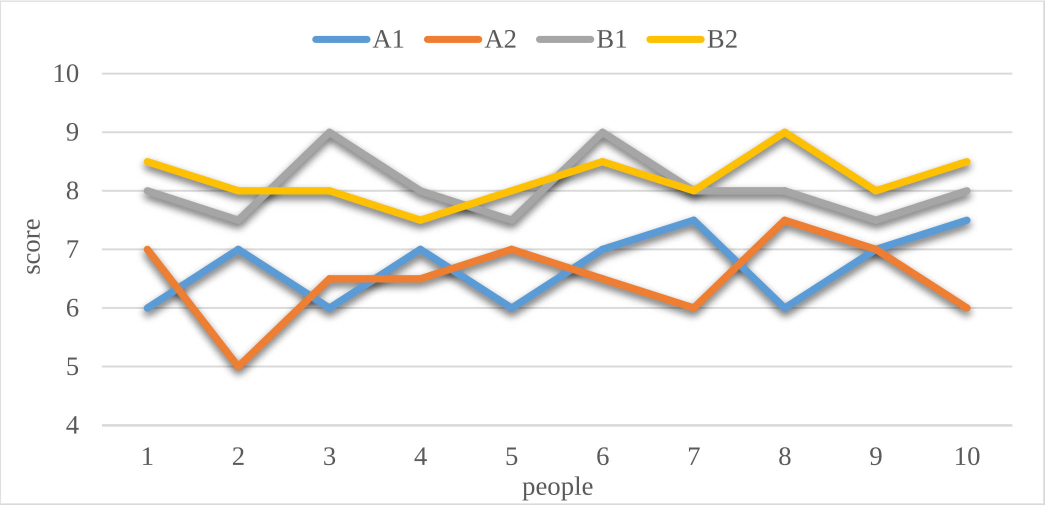

Figure 6. Comparison of risk response levels among four groups

As shown in Figure 6, it can be obviously seen that the curve of group B is distributed above group A. The scores of group B range from 7. 5 to 9 points, with a fluctuation range of 1. 5 points. In contrast, the scores for group A range from 5 to 7. 5 points, with a maximum difference of 2. 5 points. The lowest score for group B is greater than or equal to the highest score for group A. Therefore, on the whole, when an external intrusion is detected, group B responds more quickly to the risk than group A, and the defense is in place more. However, the curve of group A in the figure is flatter and the score curve of group B fluctuates more. Therefore, the response level of group A is more stable and the supervision and protection system of group B still needs to be strengthened. The standard deviation is a common indicator to measure the size of the data fluctuations. The standard deviation of the curve of the A1 group is 0. 68, while the standard deviation of the B1 group of approximately 1. 8 earlier is significantly smaller than that of the B1 group, indicating that the curve of the A1 group is flat. And by direct observation, we can find the morphology of the two curves. If the curve in group A1 is relatively smooth, while the curve in group B1 has large fluctuations.

3) Satisfaction

The satisfaction of each group with the information security protection system used by itself is counted, and the results of the scores are shown in Figure 7.

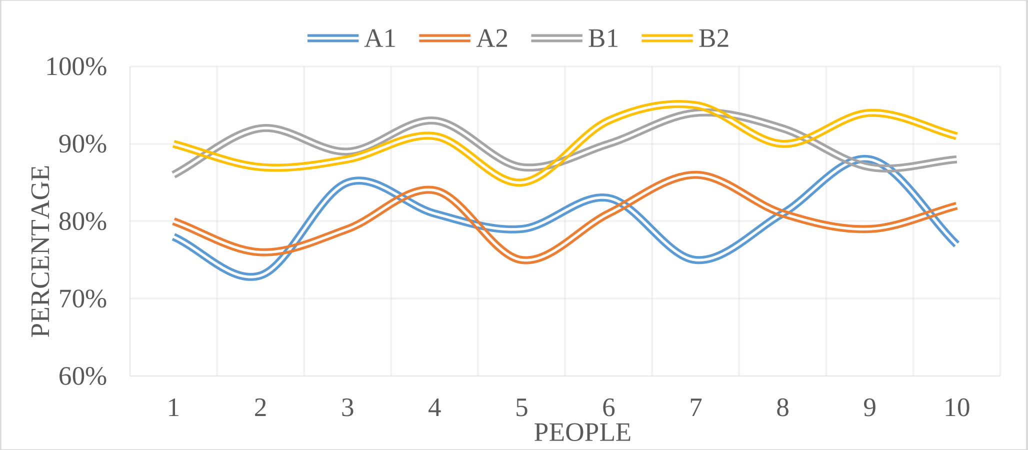

Figure 7. Comparison of satisfaction among the four groups

It can be seen in Figure 7 that the curves of group B are distributed above group A. Therefore, the user satisfaction of group B is higher and the satisfaction range of group A is between 70% and 90%. There is great controversy among users about the protective effect of traditional defense methods. The accuracy rate of group B ranges from 85% to 95%. It obtains the unanimous opinion of users and the overall satisfaction level is high. After calculation, the average satisfaction of group A is about 80% and the average of group B is about 90%. The user satisfaction with the protection system under the IoT IT increases by about 12. 4%. The computer NIS supervision and protection strategy based on the IoT IT has improved the satisfaction of users in various ways, and can provide personalized services according to the needs and scenarios of different users. For example, customized solutions for a specific industry or enterprise can better meet your business needs.

4) Comparison of general protection effects

Based on the data from the above three aspects, a comparison is made between the traditional information security protection system and the security protection system under the IoT IT. To facilitate comparison, the satisfaction data is expanded 10 times to obtain data 8 in group A and data 9 in group B. The comparison of the overall protection effect is shown in Figure 8.

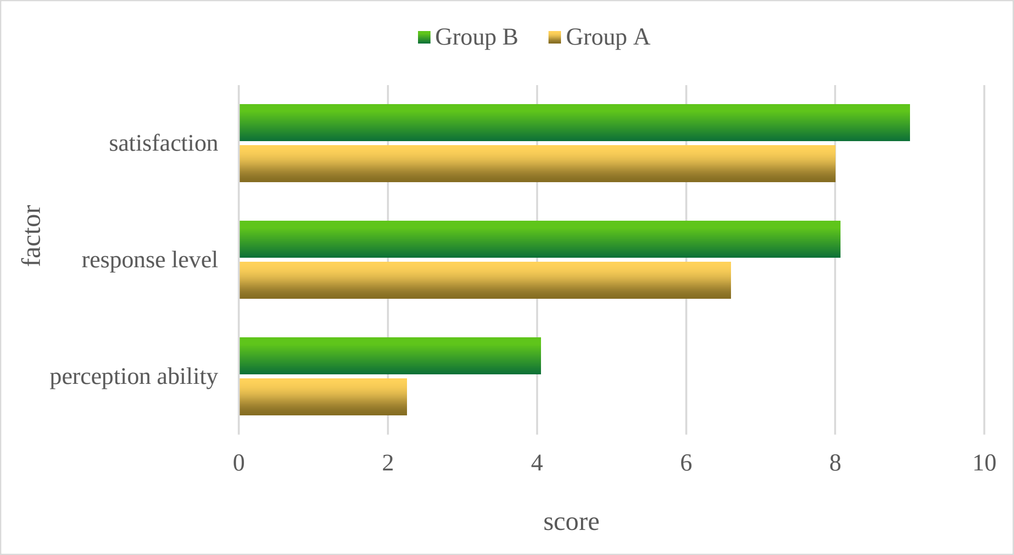

Figure 8. Comparison of the protection effects of the two systems

As shown in Figure 8, the overall performance of group B is significantly better than that of group A. The experimental data of groups A and B in the three aspects of perception ability, response level, and satisfaction are weighted to get the average of group A around 5. 62 and the average of group B around 7. 04. In the comprehensive assessment, both groups A and B differ to some extent. However, in general, the overall protective effect of group B is significantly better than that of group A. After calculation, the protection effect of group B is improved by about 25. 3% compared with that of group A. Therefore, in practical applications, the NS protection system under IoT technology can play a better role and effectively reduce the risk of network viruses or information leakage. In the IoT environment, compatibility between various devices and systems is a key issue. Some systems may better support various types of devices and platforms, while others may only accommodate specific systems and environments. The study system in this paper has better compatibility and future scalability.

Based on the IoT, IT technology can be very good regulation of computer NIS, effectively improving the accuracy of the regulation, in order to further reflect the superiority of regulation, the DL algorithm, machine learning (machine learning, ML) algorithm comparative study, and the random computer network information data for 10 experiments, specific experimental results as shown in Figure 9.

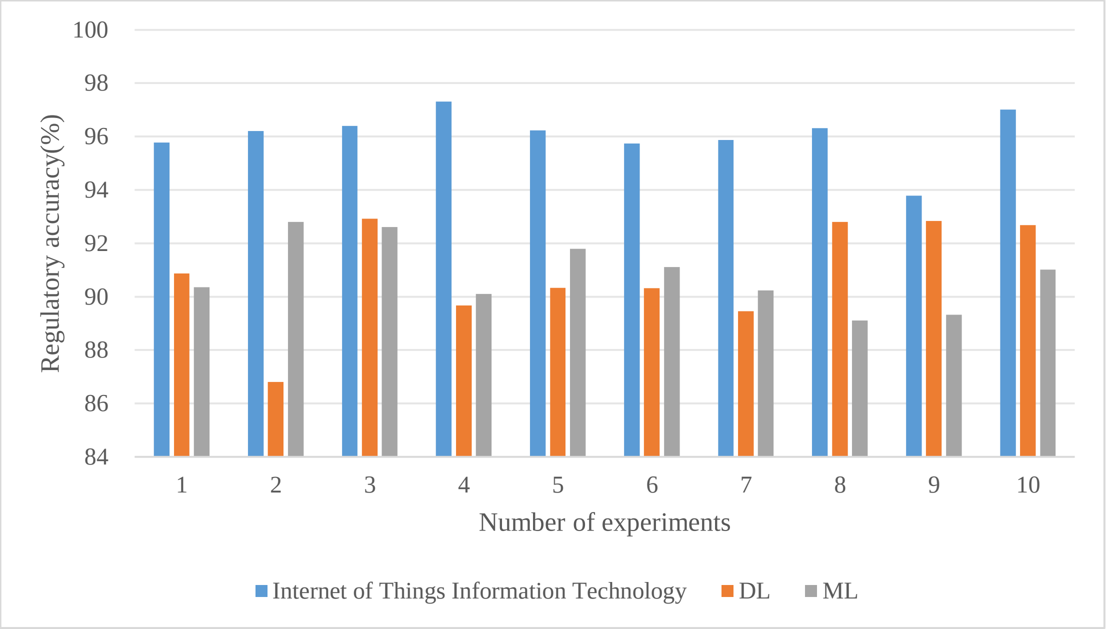

Figure 9: Accuracy of Different Research Methods on Computer NIS Data Supervision

As shown in Figure 9, the method studied in this article is much more accurate than other methods for the surveillance of computer NIS data than other methods. Among them, the regulatory accuracy of the methods studied in this paper is higher than 93. 77%, while those of DL and ML are below 92. 93% and 92. 81%, respectively. Meanwhile, when 10 experiments were conducted, the mean regulatory accuracy of the method studied in this paper was 96. 06%, which is 5. 19% and 5. 22% higher than the regulatory precision based on DL and ML, respectively.

6. Results of the discussion and ethics

(1) Results and Discussion

With the rapid development of the IoT technology, people's life and work have been closely linked with the computer network. However, with the popularity of the IoT, the problem of computer NIS is becoming increasingly prominent. This study aims to explore the surveillance and protection strategies for computer NIS under Iot IT. The security of IoT devices is one of the key factors affecting the security of computer network information. Due to the huge number of IoT devices and the complex connection between devices, the security risks are greatly increased. In addition, privacy protection during data processing and transmission is also an important issue. In the environment of big data and cloud computing, how to ensure that personal information is not leaked or abused is an urgent problem to be solved. To address these problems, we propose some regulatory and protection strategies. First, for device security, stricter device authentication and encryption technology are recommended to reduce the risk of devices being attacked. Secondly, for privacy protection in data processing and transmission, data anonymity and encryption technology can be adopted to ensure the security of personal data. However, the implementation of these strategies requires a comprehensive consideration of multiple aspects, including technology, economy, and law. Technically, we need to constantly innovate and develop more efficient and secure protection technologies. Economically, significant resources are needed to implement these technologies. Legally, relevant laws and regulations need to be formulated and improved to protect personal privacy and data security. In short, the computer NIS under the IoT IT is a complex and important problem. Only through the comprehensive use of various strategies and technologies can this problem be effectively solved to protect people's privacy and data security.

The potential impact on the industry can improve operational efficiency: The large-scale deployment of IoT devices will enable enterprises to access operational data in real time, thus optimizing operational processes and improving operational efficiency. Promoting the Digital Transformation: The IoT is one of the key technologies in the digital transformation. Through the IoT IT, enterprises can realize the transformation from the traditional mode to the digital mode. With the increase of iot devices, so is the demand for data processing and analysis. IoT devices can realize remote monitoring and control of equipment, in order to improve the automation level of production and improve production efficiency. It can improve service quality. By monitoring the operation status of the equipment in real time, equipment faults can be found and solved in time to improve service quality. Reduce operating costs. By optimizing operating processes and reducing equipment failures, enterprises can reduce operating costs and improve economic benefits.

(2) Ethics and privacy

Of course, it is an important consideration to study the ethical implications of computer NIS supervision and protection strategies under the IoT IT. With the popularity of the IoT technology, the privacy issue has become an issue that cannot be ignored. Ethical considerations are crucial in the study of the supervision and protection strategy of computer NIS under the IoT IT. Especially in research involving data security and privacy issues, we must always maintain respect for personal privacy and rights and interests. In the process of collecting and processing data from iot devices, we must strictly comply with privacy regulations to ensure the anonymity and security of personal data. The data shall not be used for purposes other than for research purposes without the consent of the user. During the course of the study, we need to clearly explain to the participants the purpose of the study, the data collection and processing methods, and the security measures of the data. Ensure that participants are fully aware of the study content and possible risks and participate. When conducting the study, we must follow relevant ethical guidelines such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulations). These guidelines provide guidance and specification for data security and privacy protection. In conclusion, this study will strictly adhere to ethical guidelines and ensure that the privacy rights and interests of participants and users are fully respected and protected while pursuing scientific progress. We will take the necessary technical and management measures to ensure the security and privacy of the data and to prevent data abuse and unauthorized access.

7. Conclusions

The supervision and protection of NIS is an inevitable requirement of today's social development, and it is also an important manifestation of the development of modern IT. Therefore, improving NS management has become an indispensable link in current enterprise security work. IoT IT is applied to NS management, which can monitor and locate the network. By using its information transmission function to analyze and process data such as user behavior, many drawbacks of traditional work methods are effectively solved, which realizes information sharing and security protection. Based on the problems of network vulnerabilities, external attacks, and system instability in the current software security system, this document analyzed traditional defense measures affecting NIS and focused on the concept and characteristics of IoT technology. Combined with the actual needs, the NS management and control system based on IoT technology was proposed. The feasibility and effectiveness of the protection system in the actual operation process were verified through experiments, which improved people's attention to NS issues and promoted the further healthy and orderly development of the NS industry.

Although some achievements have been made in the research of computer NIS supervision and protection strategy under the IoT IT, there are still some shortcomings. First, there may be methodological limitations. The current study relies mainly on theoretical analysis and simulation experiments and lacks data support from practical applications and field investigations. Therefore, the reliability and applicability of the study findings may be limited. Second, with the rapid development of the IoT technology, new threats and security risks are also constantly emerging. However, existing regulatory and protection strategies may not fully respond to these new threats and risks and need to be constantly updated and refined.

As a new computing mode, edge computing transfers the ability of data processing and analysis from the central server to the edge of the device, which can better meet the needs of the IoT. As IoT devices become increasingly integrated into people's lives, the privacy protection issue is becoming increasingly prominent. Future research will focus more on how to achieve effective data utilization while protecting user privacy.

References

[1] Chen J X. (2018). Analysis of computer network information security and protection under big data. Information Technology and Informatization, 68 (7): 1-15.

[2] Zhao M, Wang X Z. (2018). Design and implementation of network information security system based on CA technology. Journal of Science of Teachers' College and University, 58 (13): 1-7.

[3] Kansal L, Baqasah A M. (2022). Implementation of network information security monitoring system based on adaptive deep detection. Journal of Physics Conference Series, 31 (1): 454-465.

[4] Deb R, Roy S. (2021). A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets. Expert Systems with Applications, 183 (9): 1-17.

[5] Yin C. (2021). Application of Virtual Private Network Technology in University Network Information Security. Journal of Physics Conference Series, 1915 (4): 42-71.

[6] Wang Z, Zheng X. (2021). Application of internet of things information security in the informationization of sports training and education. Journal of Intelligent and Fuzzy Systems, 9 (4): 1-7.

[7] Yao Y, Tong X. (2019). Dynamically Reconfigurable Encryption and Decryption System Design for the Internet of Things Information Security. Sensors, 19 (1): 143-160.

[8] Li M, Botchey F E. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7 (3): 65-72.

[9] Yhl A, Shuang Z. (2020). Information security and storage of Internet of Things based on block chains. Future Generation Computer Systems, 10 (6): 296-303.

[10] Liang N. (2020). Security Transmission and Storage of Internet of Things Information Based on Blockchain. IOP Conference Series: Materials Science and Engineering, 750 (1): 159-164.

[11] Geng Q, Tang X, Wang L. (2019). Discussing the Influencing Factors of Information Security from the Perspective of Organizational Management. Chinese Journal of Health Informatics and Management, 19 (2): 116-137.

[12] Wang X, Lei W, Jia R. (2018). An Empirical Study on the Influencing Factors of the Security Behavior in Personal Information in Social Networks. Library and Information Service, 40 (2): 34-47.

[13] Fang S H, Peng X Y. (2029). IoT information record based on blockchain technology secure storage. Natural Science Edition, 30 (1): 117-138.

[14] Gao Y, Hasegawa H, Yamaguchi Y. (2022). Malware Detection Using Gradient Boosting Decision Trees with Customized Log Loss Function. Aerospace science and technology, 121 (2): 45-50.

[15] Farhan A K, Ali R S. (2017). Secure location map and encryption key based on intelligence search algorithm in encryption and steganography to data protection. 2019. Acta Physica Sinica, 66 (23): 690-698.