ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

Network Security and Privacy Security in the IoT Environment

Haijun Xu

Shenzhen Zheyang Technology co., LTD, Shenzhen, 518000, Guangdong, China
navyxu-cn@qq.com

Abstract: *The Internet of things is the second major revolution based on the Internet. It realizes the purpose of connecting things and promotes the development of economy and society. In order to ensure the security of the Internet of things environment, network security and privacy security become the primary problem to be solved. Based on the above background, the purpose of this paper is to study the analysis of network security and privacy security in the Internet of things environment. In order to describe the implicit information among the situation elements in the index system intuitively, this paper proposes a network security and privacy security situation assessment method based on PSO-MCELman, and a network security and privacy security situation prediction method based on PSO-MCELman according to the timing characteristics of situation prediction data. When each method completes the situation prediction training, the PSO-MCELman neural network proposed in this paper The least number of network iterations is 23, which is 22, 14 and 5 times less than traditional Elman, GA-Elman and PSO-Elman neural networks. Through the prediction of network security and privacy security situation, users can be more aware of the importance of Internet of things security and privacy security, and hope to provide some help for the solution of Internet of things security and user privacy security.*

Keywords: *IoT Security, Privacy Protection, Convolutional Neural Network, Elman Neural Network*

1. Introduction

In recent years, with the development of economy and society, information and communication technology has also continued to progress at an unprecedented rate [1]. In particular, various smart terminals and wireless communication technologies represented by smart phones are rapidly entering our lives [2]. In this big environment, the Internet of Things technology came into being [3-4]. While the Internet of Things technology has facilitated our lives, it also has many challenges. Any information system will face a variety of security issues, and the Internet of Things system is no exception [5]. Due to the open nature of the Internet of Things, it is more vulnerable to various security threats [6-7]. In addition, since the Internet of Things technology is still in its infancy, there are still many problems, especially security issues that need to be resolved [8]. If its security problems cannot be solved, the promotion of Internet of Things technology will face great resistance. Because no one wants to use a system without security [9].

As the development and extension of the Internet, the Internet of Things technology will be widely used in various industries [10]. The essence of the Internet of Things technology is to effectively integrate the latest information and communication technologies, collect signals through various sensing devices, and pass the collected signals to the central processor through various communication methods (wired or wireless) for centralized processing and control [11]. In order to achieve the effective integration of information acquisition, processing and control [12]. Increase the potential utilization of various resources, and thus increase the labor force of staff. However, since the Internet of Things system needs to connect a large number of sensing devices and items to the system [13]. And most of the information of these sensing devices or items is transmitted wirelessly. Criminals may use this information transmitted wirelessly to obtain improper benefits. Therefore, the security problem of the Internet of Things system is an urgent problem to be solved [14]. In addition, although the Internet of Things is built on the existing Internet, there are many mature traditional Internet-based security solutions that can be borrowed or used. However, after all, the Internet of Things system has its particularity, so we cannot directly use the security solutions in the traditional Internet to completely solve the problems in the Internet of Things [15].

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

Abstract social media enables people to share information across a vast network of people without having to spend a lot of money and time required by print and electronic media. Mobile-based social media applications have dramatically changed the perspective of information sharing. However, with the emergence of such applications on an unprecedented scale, the privacy of information will be harmed to a greater extent if defaults cannot be mitigated sufficiently. As healthcare applications are also being developed for mobile devices so that they can also benefit from the power of social media, the issue of cybersecurity privacy for such sensitive applications becomes critical. Leah discussed the architecture of a typical mobile medical application in which a custom privacy level is defined for individuals participating in the system. It then details how to make communication across social networks more secure and private in multi-cloud environments, especially for medical applications [16]. In the context of cybersecurity and cloud or big data development, data security classification is becoming a real issue in most organizations today. Nir tried to come up with a way to help manage data classification. They will explain the problems behind data classification from a security perspective. They will show some of the constraints behind the concept of information. They proposed a three-step approach and focused on the first step, the risk assessment matrix. This academic work was supported by a large-scale pragmatism experiment by a worldwide company [17]. Anand reviewed the current game theory methods for network security and privacy issues, and classified their applications into two categories, security and privacy. To illustrate the application of game theory in cyberspace security and privacy, they chose three main applications: cyber physical security, communication security, and privacy. They introduced the game model, characteristics and solutions of the selected works, and described their advantages and limitations from the design of the defense mechanism to their implementation. They also identified some new trends and topics for future research. This survey not only shows how to use game theory to deal with security and privacy issues, but also encourages researchers to use game theory to fully understand the security and privacy issues and possible solutions in cyberspace [18]. The proliferation of smart, connected, and inherently unsafe devices is changing the security paradigm. While the transformation of IoT technology will require a clear legal framework, alternative approaches will also need to be developed. Rolf explored changes in the legal cybersecurity environment in the context of the Internet of Things. It discusses selected applicable international regulations and alternative approaches to address security issues in the Internet of Things [19]. The Internet of Things is a network system composed of many wired or wireless smart sensors and applications. Therefore, the security and management of the Internet of Things security system becomes particularly important. The research work of IoT security management includes five parts. Luanne first pointed out the concept and background of the Internet of Things. Then, the security requirements of the Internet of Things were discussed in depth. Then, a hierarchical security management architecture is proposed. The paper details how the architecture can be used for security management of the Internet of Things. Finally, the results of implementing the proposed security function architecture in the IoT environment to obtain efficient and powerful security are summarized [20].

This paper proposes a network security and privacy security situation assessment method based on Inception-CNN. Aiming at the time series characteristics of situation prediction data, this paper proposes a network security and privacy security situation prediction method based on PSO-MCELman. When each method completes the situation During prediction training, the PSO-MCElman neural network proposed in this paper has the least number of iterations, which is 23, which is 22, 14, and 5 times less than the traditional Elman, GA-Elman, and PSO-Elman neural networks, respectively. By predicting the situation of network security and privacy security, users can be made more aware of the importance of IoT security and privacy security.

2. Proposed Method

2.1. Internet of Things Technology System

4 key technologies in the Internet of Things: sensor technology (to sense things), RFID technology (to mark things), nanotechnology (to shrink things), and smart technology (to think about things) . The wide application of the Internet of Things has made the Internet of Things technology show different application requirements and technical forms in different industries. With reference to the basic concepts of the Internet of Things, combined with the key technologies of the Internet of Things, the key technologies involved in the Internet of Things are analyzed and sorted, and the Internet of things technology system model will be obtained, as shown in Figure 1. In the illustrated technology system, it includes four technology systems, which mainly cover the technologies of perception and

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

identification, computer network and information and communication technology, computing and service technology, and management and support technology.

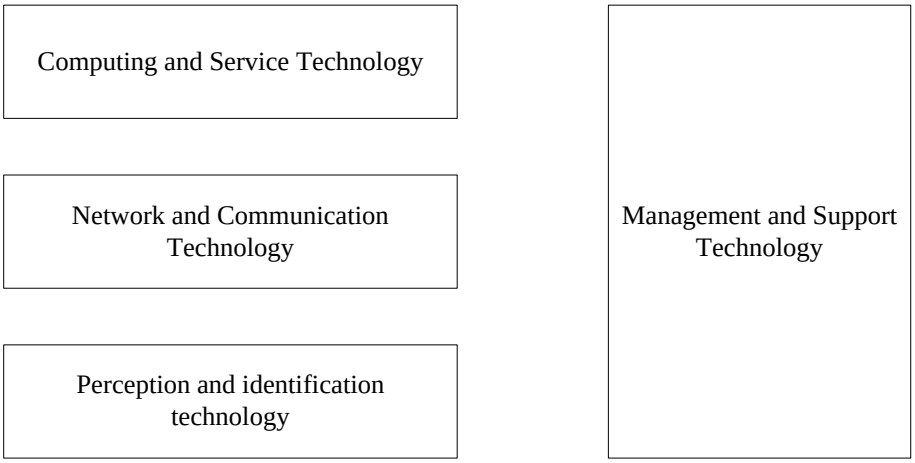

Figure 1: Internet of things technology system

(1) Perception and identification system

Among the Internet of Things technologies that are generally familiar to people, perception and identification technology is a relatively key technology.This technology is mainly used to collect some data in the real physical world, so as to achieve people's perception, judgment and recognition of the real world. This technology currently includes many parts with a lot of technical maturity: for example, sensor technology, radio frequency identification technology, and two-dimensional code technology.

1) Perceptual technology. The Internet of Things is a multiple, self-organized wireless network system, which is composed of many sensor nodes deployed in the monitoring area. In the area covered by the network, each sensor node can perceive each other's information, and can process the relevant information it has detected, collected, and then sent the information processing result to the time observer. . The current development of the Internet of Things technology has strong advantages, which is directly related to its large-scale deployment of terminal equipment.Therefore, some terminal equipment will naturally become the object of further research, such as wireless sensor network equipment and together. Matching adapters, and network gateways.

It is generally believed that the sensing technology is actually using some sensing technology equipment and some multi-hop self-organizing sensor networks to sense each other's sensor nodes and collect, detect and process the information that the sensors can sense. However, the technical equipment of the sensor has very high requirements for basic technology and comprehensive technology. It depends on sensitive materials, sensitive mechanisms, process equipment, and measurement technology. At present, an important bottleneck in the development of the industrialization of IoT-related technologies is that when sensors detect objects, their measurement types, measurement accuracy, information reliability, result stability, power consumption, and application costs have not yet reached Standards needed for large-scale applications.

Identification technology. Recognition of the physical world is the basis for achieving comprehensive perception. It mainly includes object recognition, location recognition and geographic recognition. Radio frequency identification is the foundation of the Internet of Things identification technology. The system shown in Figure 2 is a typical RFID system. It mainly consists of electronic tags and readers and information processing systems.

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

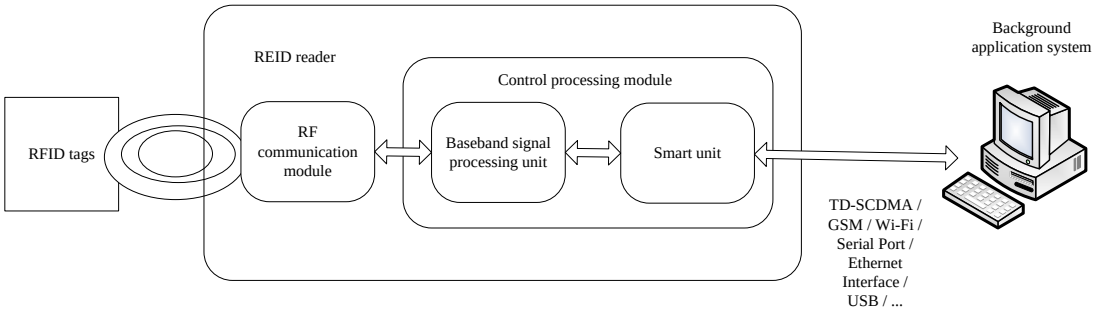

Figure 2: Composition of the REID system

For recognition technology, if you want to achieve that all objects can be directly interconnected, the most direct and effective way is to give each object you want to predict an identity, which can be achieved by assigning different IDs, but, for some special things, we must consider not only its common characteristics, but also its special needs.For example, in terms of the security of the Internet of Things, in addition to the common security issues of ordinary networks, we must also consider its special characteristics. Side: the security and privacy of information. At present, the hot research issues to promote the development of RHD technology are: anonymous identification technology and the structural design of identification, and the mapping mechanism of identification.

According to the different application requirements of the identification technology, the status of the letter to be solved will also have a different order. The first situation to be dealt with is the global identification of objects. After different objects are identified, the standardization of this system is also needed It also integrates and complies with some current sensor technologies and identification methods, and prepares for compatible technologies for future identification schemes.

(2) Network and communication technology

The reason why communication information can be accurately transmitted is that the most basic information transmission equipment supporting this service technology is a computer network. To achieve the efficient transmission of information, sensor equipment must be applied to the widely existing network function field.

1) Access and networking technology. Technologies such as ubiquitous access and backbone transmission are key network technologies for the Internet of Things. A good basic condition for the development of the Internet of Things is a next-generation network with IPv6 technology as its core. After the large-scale application of the peripheral network represented by the sensor network, it will still have access problems with the backbone network. Network technology includes not only the sensor network but also the backbone network. Information collaboration between them is needed, all of which will face challenging problems in the future. Therefore, further research is needed on wireless networks (fixed), mobile Internet networks, self-organizing network technologies, autonomous computing, and networking technologies.

2) Communication and frequency management technology. In the future real world, the research focus of the Internet of Things should be wireless, short-range information and communication technologies, but it is still necessary to comprehensively consider limited and wireless information and communication technologies. Because its network terminals generally use the ISM (Industrial Scientific and Medical) frequency band for communication (2.4GHz ISM frequency band, license-free, universal worldwide), because this frequency band contains many information network communication equipment and existing information Transmission equipment, the spectrum utilization space of each device will be very limited, so it will restrict the large-scale practical application of the Internet of Things. Therefore, if different IoT services can run at the same time in the same space, it is necessary to improve the effective utilization of spectrum resources in order to achieve interoperability and integration between various networks.

(3) Computing and service technology

The fast and efficient processing of a large amount of perceived information in the Internet of Things is the core supporting technology, and its value is ultimately reflected in the two aspects of service and application.

1) Computing technology. After the Internet of Things develops its applications on a large scale, the

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

key support for the application of information computing and information processing technology instructors. After a large amount of sensory information is collected, a series of intelligent information processing is required to solve various problems of the Internet of Things technology. Among them, the core of information computing technology is distributed shared storage resources.

2) Service technology. For future service forms and different applications, we must find out the core technical support that supports the development of the Internet of Things in applications, and develop applications for different needs, and how to make a conventional service architecture.

(4) Management and support technology

With the continuous expansion of the application direction of the Internet of Things, the service issues that have arisen are also increasing. When asked about the key technologies to ensure its management and support, the following aspects must be analyzed.

1) Measurement analysis. Testability is the basic problem in network research, and measurement is the basic method to solve the problem of network visibility. Therefore, we need to study key technologies for efficient measurement and analysis of the Internet of Things, and establish service-oriented IoT measurement mechanisms and methods to cope with increasing network complexity and emerging new services.

2) Network management. There is a sharp contradiction between the natural characteristics of the "autonomy, proliferation, and diversity" inherent in the Internet of Things and the basic requirements of network operation and management.Therefore, we need to create a new Internet of Things management model and study new key technologies of the Internet of Things. Ensure that the network system can run normally and efficiently.

3) Security and privacy protection technology. Since most applications of the Internet of Things will involve personal privacy or institutional privacy, it must have strict security and controllable technologies. The identification code (ID) of any tag can be scanned at will remotely, and the tag can automatically and indiscriminately respond to the reader's instructions, and then transmit the stored information content to the reader. This has led to security and privacy protection issues, which is one of the key technologies for the security of the Internet of Things.

2.2. Internet of Things Security Technology

The degree of protection of IoT network security and privacy security determines the breadth and decisiveness of IoT applications. Now that the development of the Internet of Things has slowly penetrated into various fields, the security of the Internet of Things is also involved in various aspects. Therefore, the security guarantee technology of the Internet of Things has become more and more intensive.

(1) Key system is the foundation of the Internet of Things security technology

The key system includes asymmetric and symmetric systems, one is to distribute and manage the key system through the IoT key center, and the other is to distribute management of the key system through different network centers, and different network structures correspond The keys for communication between different network nodes are negotiated and managed. The security strength of the secret key produced by the secret key algorithm guarantees confidentiality during data transmission. It is possible to reduce the insecurity in the data transmission process by shortening the key cycle, and to avoid illegal activities.

(2) Security processing of data privacy information

Every step of the information transmission process of the Internet of Things is inseparable from the security protection of private information. By ensuring that the data information is not tampered and stolen during collection and transmission under a reliable network security environment. In particular, location services in IoT applications are the basic services of the Internet of Things.Some mobile phone positioning, electronic maps, and wireless sensor network privacy information queries require secure processing.Currently, the Internet of Things's security technologies include space encryption, space-time Anonymity and location camouflage.

(3) Guarantee of routing security protocol

Internet of Things applications span a variety of different types of platforms, and each platform has its own different routing protocols and algorithms, such as mobile communication protocols, IP address

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

routing protocols, and sensor network routing protocols. It is precisely because of these multi-platform different protocols that solving the routing security of multi-network convergence is the top priority, and try to prevent false routing and forwarding vulnerabilities. So far, more effective routing technologies include data-centric hierarchical routing and geographical routing based on location routing.

(4) Authentication access technology

In the use of the Internet of Things, it is necessary to verify the authenticity of the identity of the users of the Internet of Things by authenticating the users of the Internet of Things and exchange session keys with each other. This is based on timeliness and confidentiality, including access technology for message authentication, which confirms the reliability of the other party by sending information to the other party. The authentication and access technology of the Internet of Things only needs the combination of public key authentication technology, random key pre-distribution technology and other auxiliary authentication technologies to perform authentication and access control on Internet of Things users.

(5) Fault tolerance technology

When someone maliciously invades, the fault tolerance of the network is needed to prevent the network from crashing caused by malicious invasion, which improves the anti-interference of the network. In order to ensure that link failures occur in the operating environment of the Internet of Things, nodes can continue to communicate normally in the event of loss of nodes and sudden conditions in harsh environments, and error-free data transmission is achieved. Fault tolerance mechanism to solve.

The problem that sensor nodes are easily manipulated by the physical network cannot be avoided by sensor networks. Therefore, other technologies must be used to improve the security performance of sensor networks. If the identity between the nodes can be authenticated before communication, in order to make it impossible or difficult for an attacker to deduce the key information of other nodes from the node information obtained from the manipulated node, a new key needs to be designed negotiate a plan. In addition, the security performance of the node itself can be improved by measures such as authenticating the legitimacy of the node software.

3. Experiments

3.1. Experimental Background

Based on the inductive analysis of the research status of situation assessment and prediction at home and abroad, this article uses neural network models to evaluate and predict network security and privacy situations in the IoT environment.First, in conjunction with the existing network security situation indicator system, according to The network information risk assessment standard selects relatively important factor indicators from multiple levels and dimensions to build an indicator system, and at the same time quantifies the underlying indicators according to relevant mathematical formulas. Then, based on the established index system, a new method of network security situation assessment based on Inception-CNN is proposed, and a related situation assessment model is constructed.The inception module is combined with traditional convolutional neural networks, and filtering is introduced. The idea is to use high-lift filtering to amplify the characteristics of sub-situations in different dimensions and increase the sensitivity of the evaluation model to different sub-situations, making it more operable and practical.

3.2. Experimental Data Collection

This article obtained the complete CIC-IDS2017 data set by consulting the data.The data set was made by CIC and up to 55GB.It is a complete update of the CIC-IDS2012 data set and has many advantages over other data sets: First, Provide PCAPS capture files under real environment. In the past, many data sets used security simulation attacks instead of real network attack experiments, but the PCAPS file provided by the CIC-IDS2017 data set completely and detailedly records the network status of each period for in-depth analysis. Second, more common and newer cyber attacks are used in the attack experiments, which are in line with the current trend of network environment changes. Third, provide the corresponding CSV file. This file contains rich information such as timestamp, source address, destination address, source port, destination port, protocol, and attack type, which is

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

convenient for situation research. Fourth, add a variety of common network user behaviors. This data set adds user behaviors such as based on HTTP, HTTPS, FTP, SSH, and email, which are closer to the real network usage environment. Therefore, the CIC-IDS2017 dataset overcomes the shortcomings of previous datasets well, and is more adapted to the current real network environment and attack modes.

The CIC-IDS2017 data set records all network data for five working days a week. It has a complete network configuration and the network topology includes multiple host devices, firewalls, switches, and routers. In the experimental environment, the attack network exists outside the victim network system, and the victim network system contains 12 different hosts. The specific composition of the victim network system and attack network system is shown in Table 1.

Table 1: Network equipment composition

Host category	Host system	IP
Secure host	Fire	205.174.165.80
	DNS+DC Server	192.168.10.3
Attack host	Kali	205.174.165.73
	Win	205.174.165.69\205.174.165.70\205.174.165.71
Victim host	Web server 16 Pubic	192.168.10.50\205.174.165.68
	Ubuntu server 12 Public	192.168.10.51\205.174.165.66
	Ubuntu 14.4,32B	192.168.10.19
	Ubuntu 16.4,32B	192.168.10.16
	Win7 Pro,64B	192.168.10.9
	Win 8.1,64B	192.168.10.5
	Win Vista,64B	192.168.10.8
	Win10,pro 32B	192.168.10.14
	Win10,64B	192.168.10.15
	Mac	192.168.10.25

The CIC-IDS2017 data set has the characteristics of long recording time, large amount of data, and complicated storage form, so it needs to be processed many times before it can be converted into the used data form. In the data processing stage, the CIC-IDS2017 dataset is first divided into 240 time slices, which is more than double the number of KDD-CUP datasets commonly used in previous experiments to ensure the reliability of the experiment. Then, through effective data mining techniques and suitable data processing tools, effective information is mined from 240 time slices, relevant situational factors are obtained, and the underlying situational index values are calculated according to the quantitative formula.Finally, manual annotation is performed to make samples to adapt to the assessment. Input and output with predictive model.

3.3. Experimental Sample Production

In the sample production of network security and privacy security in this paper, first, the elements of network security and privacy security obtained by mining technology and analysis software are quantified by formula 1 and formula 2 to obtain the underlying index values required for the experiment. Then, according to the network situation assessment system constructed in Chapter 3, the underlying indicator values obtained are arranged, and the indicator values are fragmented according to the set time slice. Part of the input data is randomly extracted after fragmentation.

$$Y = \frac{\sum_{j=1}^{N}\sum_{i=1}^{k} 10^{P_{ji}} Q_j C_{ji}}{K}$$
$$I_j = \begin{cases} 1.0 & \text{confidential} \\ 0.7 & \text{important} \\ 0.4 & \text{ordinary} \end{cases} \tag{1}$$
$$Q_j = \frac{I_j}{\sum_{j=1}^{N} I_j}$$

Among them, Y represents the severity of the attack, N is the total number of hosts, K is the number of types of attacks, K is the total number of all attacks detected in a certain period of time, Cji is the number of times that the j-th host was attacked by i, and Pji is the j-th The attack level factor when the host is under the i-th attack.This element can be obtained by scoring the attack damage.Qj represents the importance of the j-th host.Qj can be measured by the importance score of the information

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

contained in the host and normalized deal with.

$$N = \sum_{i=1}^{L} \sum_{j=1}^{K} A_h^{ij} A_w^{ij} Con_h^{ij} Con_w^{ij} + \sum_{i=1}^{L} \sum_{j=1}^{P} B_h^{ij} B_w^{ij} Pool_h^{ij} Pool_w^{ij} \quad (2)$$

Among them, L is the number of layers of Inception, K and P are the number of convolution kernels and pooling kernels of the first layer of the Inception module, and Aijh and Aijw are the new convolution kernels of the i-th layer after the convolution operation. The height and width of the feature map, Bijh and Bijw are the height and width of the new feature map after the pooling operation of the j-th pooling kernel in the i-th layer, and Conijh and Conijw are the heights of the j-th convolution kernel in the i-th layer. And width, Poolijh and Poolijw are the height and width of the j-th pooling kernel of the i-th layer.

4. Discussion

4.1. Situational Evaluation Experiment Analysis

(1) Elman evaluation experiment analysis

In this paper, the obtained situation values are used to form a prediction sample set. In the prediction sample set, a total of 192 samples are selected as training samples in the first four days, and 48 samples on the last day are used as test samplesis shown in Table 1. .

Table 2: Forecast model input and output data

Sample number	Input data	Output Data
1	0.93,0.92,0.84,0.82,0.78,0.75	0.74
2	0.93,0.84,0.82,0.78,0.75,0.74	0.82
3	0.84,0.82,0.78,0.75,0.74,0.82	0.90
4	0.82,0.78,0.75,0.74,0.82,0.90	0.76
5	0.78,0.75,0.74,0.82,0.90,0.76	0.80

This paper compares the traditional Elman feedback neural network model with two feedforward neural network models of BP and RBF. The prediction results of some test samples are shown in Figure 3 below.

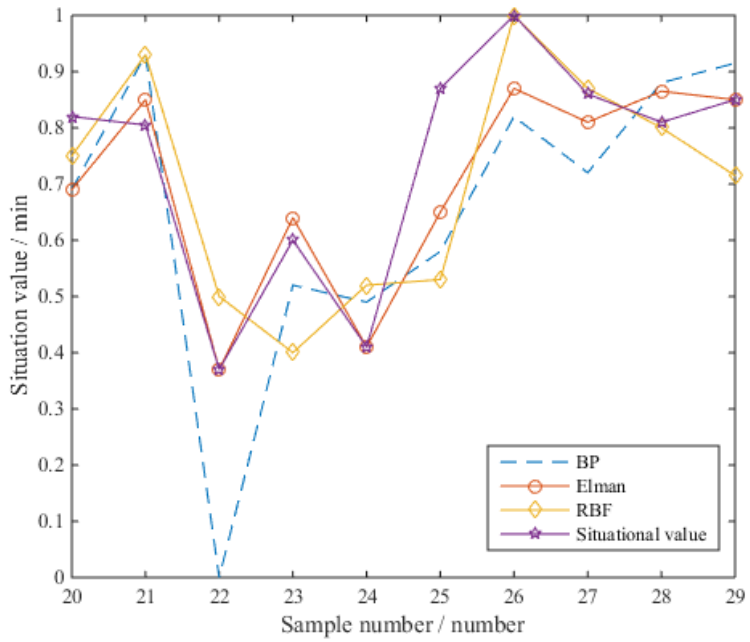

Figure 3: Elman, RBF, and BP situation prediction results

It can be seen from the figure that in the situation prediction, the fitting speed and degree of fitting of the ELMAN neural network are relatively good. According to prediction sample 20, it can be known that the error control ability of RBF in the initial stage is stronger than that of BP and Elman neural

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

networks. The predicted trend is opposite to the real-time trend. The ELman network's prediction accuracy is more accurate than BP and RBF, and the response speed is relatively fast.Therefore, according to the characteristics of time-series samples in situation prediction, an ELMAN neural network with feedback capability is selected. The network is more scientific and effective.

(2) Convolutional neural network and situation analysis

This article compares the trained improved convolutional neural network with the commonly used situation assessment method SVM and the unimproved convolutional neural network for situation assessment performance experiments. 15 test samples were input into the evaluation model for situation prediction, and the degree of deviation between the evaluation results obtained from the situation evaluation methods using SVM and CNN was relatively high, and the evaluation results curve and situation true value of Inception-CNN used in this paper The curve fits more closely. The absolute error of each algorithm's situation assessment is shown in Figure 4. It can be seen from the figure that the difference between the evaluation result of each test sample and the real situation value is relatively small.

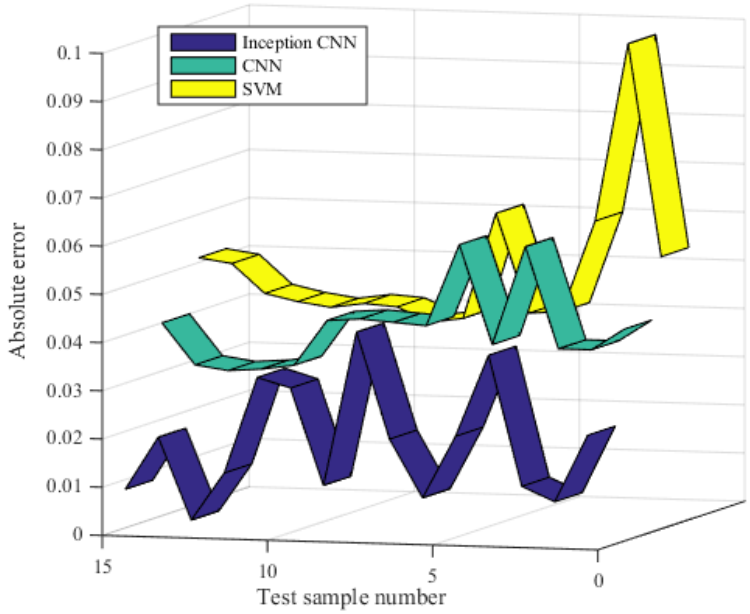

Figure 4: Graph of Absolute Error Fluctuations in Situation Assessment

This article refers to the cyber network awareness materials of the MS-ISAC (Multi-State Information Sharing and Analysis Center) and the basic security index of the National Internet Emergency Response Center Network Security. Moderate, Poor and Dangerous, as shown in Table 3.

Table 3: Situation value safety level table

Security Level	excellent	good	mid	bad	danger
Situation value / min	[0-0.2]	(0.2-0.4]	(0.4-0.75]	(0.75-0.9]	(0.9-1]

4.2. PSO-MC Elman and Elman Prediction Experimental Analysis

(1) PSO-MCElman situation prediction analysis

After comparative experiments, the test samples were input into the situation prediction model based on the PSO-MCElman situation prediction model proposed in this paper. Similarly, the traditional Elman neural network, Elman neural network optimized by genetic algorithm (GA-Elman), and Elman neural network optimized by optimized particle swarm algorithm (PSO-Elman) were used to perform situation prediction on 48 test samples.Among them, The absolute value of the situation prediction error of each method for each test sample is shown in Figure 5.

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

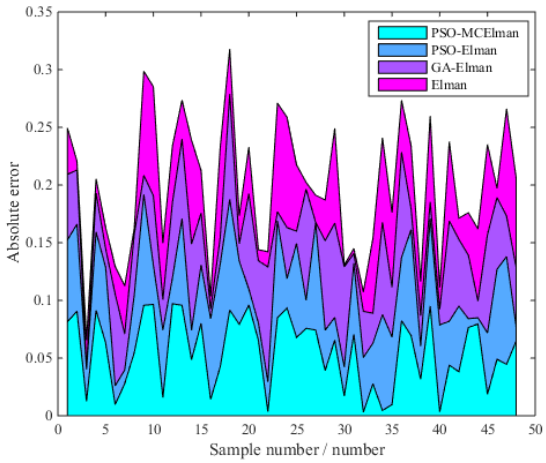

Figure 5: Graph of Absolute Error Fluctuations in Situation Forecast

Analysis and analysis of Figure 5 found that the Elman neural network and GA-Elman neural network have relatively large prediction errors for most samples, while the PSO-MCElman neural network has relatively small situational prediction errors and has better robustness. And the amplitude of the absolute value curve of the improved Elman neural network used in this paper is relatively mild, the error fluctuation range is smaller and more stable, and the defect that the Elman neural network is easily trapped in local minimum values is improved, and the prediction accuracy is better than that of ordinary optimization. Elman neural network significantly improves the situation prediction effect.

(2) Comparative experimental analysis of Elman neural network

This paper selects Gray Neural Network (GNN) and Wavelet Neural Network (WNN), which are commonly used to solve time series prediction problems and have good prediction effects on nonlinear and time-varying data, and the improved Elman neural network Network for comparative experiments. The situation prediction fitting situation is shown in Figure 6.

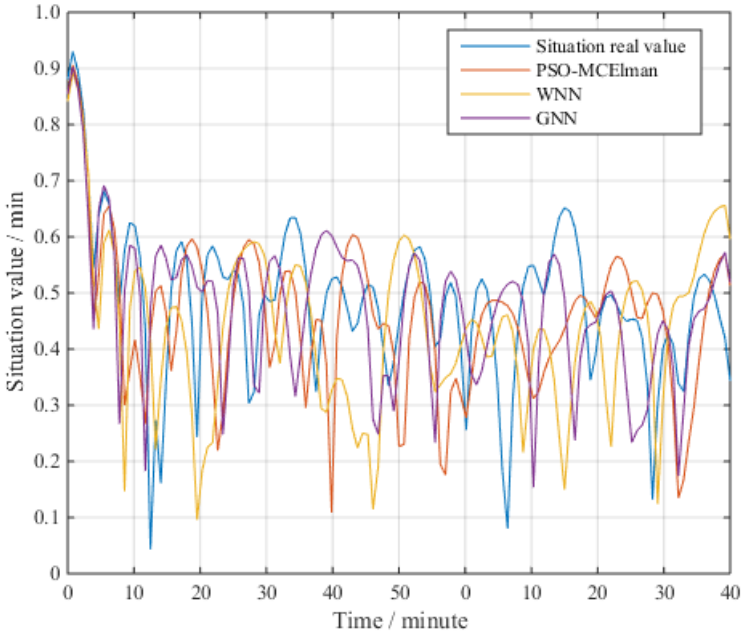

Figure 6: PSO-MCElman, WNN, GNN situation prediction fit

It can be seen from Figure 6 that the wavelet neural network and gray neural network have relatively large errors in the prediction results of most test samples. The prediction results of the situation prediction method in this paper have a relatively small deviation from the true values, and the overall simulation of the true values of the network security situation The degree of integration is better

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

than the other two situation prediction methods. The error accuracy index of PSO-MCElman prediction model is smaller than that of wavelet neural network and gray neural network, especially in the mean square error, which indicates that the optimization algorithm in this paper has better accuracy. Therefore, when predicting the network security situation, the PSO-MCElman neural network has better generalization ability and stability, while making the network security situation prediction more accurate, reliable, and effective.

As the latest development of information and communication technology, the Internet of Things technology is increasingly widely used in all aspects of our lives. The Internet of Things mainly uses smart devices with various functions (such as various sensors, communication devices, smart appliances) to connect by wired or wireless means. Through the communication and coordination between various devices, new application paradigms or new functions are generated. Although the Internet of Things technology has strong application potential, it still faces many problems. Among them, system security and user privacy protection are one of the important issues that the Internet of Things technology must solve.

5. Conclusions

The problems of information security, network security, and data security in the development of the Internet of Things are more prominent. The research on the corresponding key security technologies is related to the cost and complexity. The development and research of security technologies are directly proportional to the investment. Although the Internet of Things technology has strong application potential, it still faces many problems. Among them, system security and user privacy protection are one of the important issues that the Internet of Things technology must solve. Based on the neural network, this paper proposes a network security and privacy security situation assessment method based on an improved convolutional neural network and a network security and privacy security situation prediction method based on an improved dynamic regression neural network. The construction of the evaluation and prediction model was discussed.

This paper proposes a network security and privacy security situation assessment method based on Inception-CNN and constructs a corresponding evaluation model. In this paper, convolutional neural networks in deep networks are introduced into situation assessment.By combining traditional CNN with optimized Inception module, the situation details and global features are reduced, the amount of calculation is reduced, the calculation speed of the evaluation model is accelerated, and The two major tasks of deep excavation of situational characteristics and accurate analysis of overall situation. A network security and privacy security situation prediction method based on PSO-MCElman is proposed and a corresponding prediction model is constructed. When using Elman neural network for situation prediction, first improve the traditional Elman neural network structure, construct a memory layer and feed back the output data to the input layer to make up for the short-term memory defects of the receiving layer, while adding external feedback, and forming an internal and external cycle with the receiving layer Feedback, forming a dynamic system of internal and external loop feedback. Then build a selection layer, and tap the periodic changes of the situation time series.

At present, many researchers are focusing on the research of Internet of Things security technology, and new research results are constantly appearing. However, after all, the Internet of Things technology is still developing, and there are still many new security issues that need to be continuously researched and explored. In the Internet of Things security solution, this article believes that more in-depth research is needed in the following aspects: wireless communication security; Internet of Things privacy protection issues; security management issues; Internet of Things security standardization issues. Therefore, a key issue for the research and development of the Internet of Things has surfaced, namely how to design a secure and effective privacy protection mechanism.

References

[1] Christian Esposito, Alfredo De Santis, Genny Tortora. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?[J]. IEEE Cloud Computing, 2018, 5(1):31-37.
[2] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis. IoT Middleware: A Survey on Issues and Enabling Technologies[J]. IEEE Internet of Things Journal, 2017, 4(1):1-20.
[3] Elisa Bertino, Kim-Kwang Raymond Choo, Dimitrios Georgakopolous. Internet of Things (IoT): Smart and Secure Service Delivery[J]. Acm Transactions on Internet Technology, 2016, 16(4):1-7.

ISSN 2706-6827 Vol. 3, Issue 8: 5-16, DOI: 10.25236/IJFS.2021.030802

[4] Rachad Atat, Lingjia Liu, Jonathan Ashdown. A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems[J]. IEEE Internet of Things Journal, 2017, 5(1):295-309.
[5] Tan Soo Fun, Azman Samsudin. Attribute Based Encryption—A Data Centric Approach for Securing Internet of Things (IoT)[J]. Advanced Science Letters, 2017, 23(5):4219-4223.
[6] Mohammed Moness, Ahmed Mahmoud Moustafa. A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy[J]. IEEE Internet of Things Journal, 2015, 3(2):134-145.
[7] Barbara L Filkins, Ju Young Kim, Bruce Roberts. Privacy and security in the era of digital health: What should translational researchers know and do about it?[J]. American Journal of Translational Research, 2016, 8(3):1560-1580.
[8] Xabier Larrucea, Annie Combelles, John Favaro. Software Engineering for the Internet of Things[J]. IEEE Software, 2017, 34(1):24-28.
[9] S.McKenna, D. Staheli, C. Fulcher. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns[J]. Computer Graphics Forum, 2016, 35(3):281-290.
[10] Carlos Lopez, Arman Sargolzaei, Hugo Santana. Smart Grid Cyber Security: An Overview of Threats and Countermeasures[J]. Journal of Power & Energy Engineering, 2015, 9(7):632-647.
[11] Chao Lin, Debiao He, Neeraj Kumar. Security and Privacy for the Internet of Drones: Challenges and Solutions[J]. IEEE Communications Magazine, 2018, 56(1):64-69.
[12] Guobin Xu, Wei Yu, Zhijiang Chen. A cloud computing based system for cyber security management[J]. Parallel Algorithms & Applications, 2015, 30(1):29-45.
[13] Nir Kshetri. India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership[J]. IEEE Security & Privacy Magazine, 2015, 13(3):16-23.
[14] Orlando Arias, Jacob Wurm, Khoa Hoang. Privacy and Security in Internet of Things and Wearable Devices[J]. IEEE Transactions on Multi-Scale Computing Systems, 2017, 1(2):99-109.
[15] Anil Gurung, M.K. Raja. Online privacy and security concerns of consumers[J]. Information & Computer Security, 2016, 24(4):348-371.
[16] Leah Zhang-Kennedy, Sonia Chiasson, Robert Biddle. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cyber Security[J]. International Journal of Human–computer Interaction, 2016, 32(3):215-257.
[17] Nir Kshetri. India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership[J]. IEEE Security & Privacy Magazine, 2015, 13(3):16-23.
[18] Anand Shah, Shishir Dahake, Sri Hari Haran J. Valuing data security and privacy using cyber insurance[J]. ACM SIGCAS Computers and Society, 2015, 45(1):38-41.
[19] Rolf H. Weber, Evelyne Studer. Cybersecurity in the Internet of Things: Legal aspects[J]. Computer Law & Security Review the International Journal of Technology Law & Practice, 2016, 32(5):715-728.
[20] Luanne Billingsley, Shawn A. McKee. Cybersecurity in the Clinical Setting: Nurses' Role in the Expanding "Internet of Things"[J]. Journal of Continuing Education in Nursing, 2016, 47(8):347-349.