International Journal of Digital Crime and Forensics
Volume 15 • Issue 1

Assurance of Network Communication Information Security Based on Cyber-Physical Fusion and Deep Learning

Shi Cheng, Nantong University, China
https://orcid.org/0000-0002-0597-9823
Yan Qu, Nantong University, China
Chuyue Wang, Nantong University, China
Jie Wan, Nantong University, China*
https://orcid.org/0000-0002-7826-0422

ABSTRACT

The internet brings high efficiency and convenience to society; however, the issue of information security in network communication has significantly affected every aspect of the society. How to ensure the security of this network communication information has become an important research topic. This paper proposes a diagnosis and prediction method based on cyber-physical fusion and deep learning, such as LSTM and CNN, to diagnose and predict network security in a complex network environment. The experiment results showed that the accuracy of network security diagnosis of the LSTM method in the training set was approximately 80%/ After the CNN training process, it has the highest accuracy rate of 95% on the test data set. This paper analysed the nature of network security problems from the perspective of cyber-physical fusion. CNN-based method to diagnose network security can obtain results with a higher accuracy rate so that technicians can better take measures to protect network security.

KEYWORDS

Convolutional Neural Network, Cyber-Physical Fusion, Deep Learning, Information Security

1. INTRODUCTION

Physical fusion of information and deep learning are rapidly developing technologies in recent years, and they have a wide application prospect in network communication information security. Information physical fusion can combine physical signal with information processing technology to improve the reliability and security of data transmission. Deep learning has powerful data processing and analysis capabilities, which can monitor and predict the data in network communication in real time and

DOI: 10.4018/IJDCF.332858
*Corresponding Author

improve the security of the network. Data in network communication is usually sequential data that arrives in chronological order, such as network traffic and log records. LSTM can effectively capture long-term dependencies in sequence, model and predict sequence data. In the field of information security, LSTM can be used to detect abnormal network behavior, intrusion detection and password cracking. CNN is widely used in the field of image processing, but its excellent feature extraction ability can also be used in network communication information security. Through convolutional operation, CNN can extract local and spatial features in data, which are often important information in network communication data, such as packet header information in network traffic and characters on the login page. CNN can also be combined with other network level information for classification and identification, such as the use of convolutional layer and full connection layer for spam filtering, malicious URL detection and other tasks.

With continuous research on fifth-generation mobile communication networks, the number of various terminals and the demand for services are exploding, and the operation of wireless networks is facing many challenges. The traditional manual management method is no longer suitable for this network structure. Therefore, timely detection and diagnosis of network faults through intelligent algorithms under the premise of ensuring system capacity has become one of the focuses of current network operators. Given that the improvement of user experience is very important for network service providers, effective solutions are needed in the field of network security diagnostics, which would surely be a research topic for future network security maintenance. The innovation of this paper is that it proposes a deep learning method for cyber-physical fusion and elaborates and compares the LSTM and CNN methods in detail. The use of a reputation mechanism to protect network security is proposed.

Although many scholars have conducted in-depth research on LSTM and CNN methods and there are many application areas for network security assurance, the variation patterns of network fault prediction accuracy under different quantities have not been explored. However, this article found through experiments that as the number of data records increases, the accuracy on the training set gradually improves, the stability improves, and the accuracy on the test set significantly improves. However, when the historical data were recorded at 400, there was almost no improvement in performance.

2. RELATED WORK

Today, with the popularization and development of network technology, an increasing number of industries rely on computer networks to complete daily business, and the establishment of network communication information security is becoming increasingly important. Joshi C found that online information is one of the university's most important assets and must be protected from security breaches. He analyzed the specific evolution of security threats in the university network and proposed an information security framework for the university network environment in response to these problems (Joshi & Singh, 2017). Dang-Pham D believed that employees in modern organizations can build their own security awareness by participating in the organization's social network. Social network analysis methods provided a wide range of analytical capabilities that contribute to the development of this safe workplace (Dang-Pham et al.,2017). According to Chen J, heterogeneous networks can enhance the functionality of mobile communication technology because mobile communication is so open, that information security is also put at risk. He gave a brief introduction to heterogeneous networks and used security rate analysis to examine the physical layer security performance of heterogeneous networks in an effort to increase the security of mobile communication (Chen et al.,2020). Yang X N proposed that in view of the challenges faced by national cyberspace, people should start from the current state of cyberspace. He proposed the tripartite theory of cyberspace and the corresponding strategies and research architecture and then discussed the characteristics and security requirements of these networks (Yang et al.,2018). Shang W discovered that ambiguous

elements frequently have an impact on the assessment of the industrial control system's information security risk. He suggested using the attack tree model to analyse the risk to information security (Shang et al.,2019). Scholars have mentioned that although the Internet has brought about earth shaking changes and many conveniences to people, the problem of network information security is becoming increasingly serious. Therefore, people should find ways to ensure the security of network communication information. However, they did not explain how security was guaranteed.

Deep learning techniques have delivered cutting-edge outcomes in several fields by using multiple processing layers to create hierarchical representations of input. Zhang Q S found that although deep neural networks show excellent performance in different roles, interpretability has always been a challenge for deep neural networks. High interpretability can help people breakdown some of the barriers in deep learning (Zhang & Zhu, 2018). Tom Y found that in the natural language processing (NLP) environment, different design models and methods have been proposed. He explored and developed important models and methods related to deep learning, which were used in many natural language processing roles (Xue et al.,2021). Zhu X X believed that machine learning techniques were becoming more important but not at the heart of the shift to a data-intensive scientific paradigm. Deep learning has proven to be a major breakthrough and an extremely powerful tool in many fields to analyse the challenges of using deep learning to analyse Earth's remote survey data (Zhu et a;.,2018). Deep learning, in He L's opinion, is a promising strategy because its multilayered structure is also suitable for edge computing environments. To enhance the functionality of advanced IoT teaching apps through edge computing, he incorporated deep learning into the environment (Li et al., 2018). Network security is a key element in the computer industry. To raise the bar for computer network security to a new level, emphasis must be placed on the implementation of virtual network technologies. In light of this, Qi K examined how virtual network technology was used for computer network security and offered some recommendations for the future (H. Zhang et al., 2019). Scholars believed that deep learning has been widely used in the Internet of Things and can play a huge role, especially in the aspect of network security protection. Deep learning has been welcomed by many people. However, scholars have not conducted concrete experiments to prove that their proposed method is effective.

The core idea is the combination of LSTM and CNN and explores whether both methods can predict future security situations, but the accuracy of the two methods is not consistent. At the same time, this article compares the differences in accuracy and false alarm rates between the model studied in this article and the CNN model. To verify the high accuracy of the CNN method, simulation experiments were conducted in this paper, and it was found that the CNN method not only has high accuracy but also has a high recall rate. This article also proposed the impact of reputation mechanisms on network security. Through experiments, it was found that the probability of being attacked by malicious resources is lower when there is a reputation mechanism than when there is no reputation mechanism.

3. NETWORK SECURITY DIAGNOSIS AND PREDICTION BASED ON DEEP LEARNING

In recent years, the network has penetrated into all fields and aspects of society, especially the development of the Internet, which has triggered a revolution in social lifestyle, and human beings have begun to enter the network society. However, with the rapid development of the Internet, shared computer network resources are becoming increasingly abundant, and the accompanying information security issues are also becoming increasingly prominent. The serious damage caused by computer cybercrime in national security, commercial security and personal security is increasingly evident (Young et al.,2018). Hackers, viruses, loopholes and other problems emerge in an endless stream, and the computer network is seriously threatened from all aspects. The network information security architecture is shown in Figure 1:

As shown in Figure 1, to facilitate management and maintenance, it realizes so-called automatic networking and plug-and-play, which requires free access rights and self-discovery/self-installation of nodes. These requirements are exactly what cybersecurity needs to protect (Han et al., 2018).

3.1 Diagnosis and Prediction Based on LSTM Neural Network

A variation of an RNN is an LSTM network. Due to gradient vanishing, RNN can only have short-term memory. Through sophisticated gate control, the LSTM network integrates short-term memory with long-term memory, partially resolving the vanishing gradient issue. Each element of deep learning is called a "neuron". Neurons are connected to each other, and the learning process is the process of changing the power of neurons. In this change, each layer is adapted to the characteristics of the neuron network, so the network composed of deep learning is a multilevel neuron network (Haenssle et al.,2018).

The network structure is usually represented by many different functions, in which case a function can be used to describe this process, such as Formula 1:

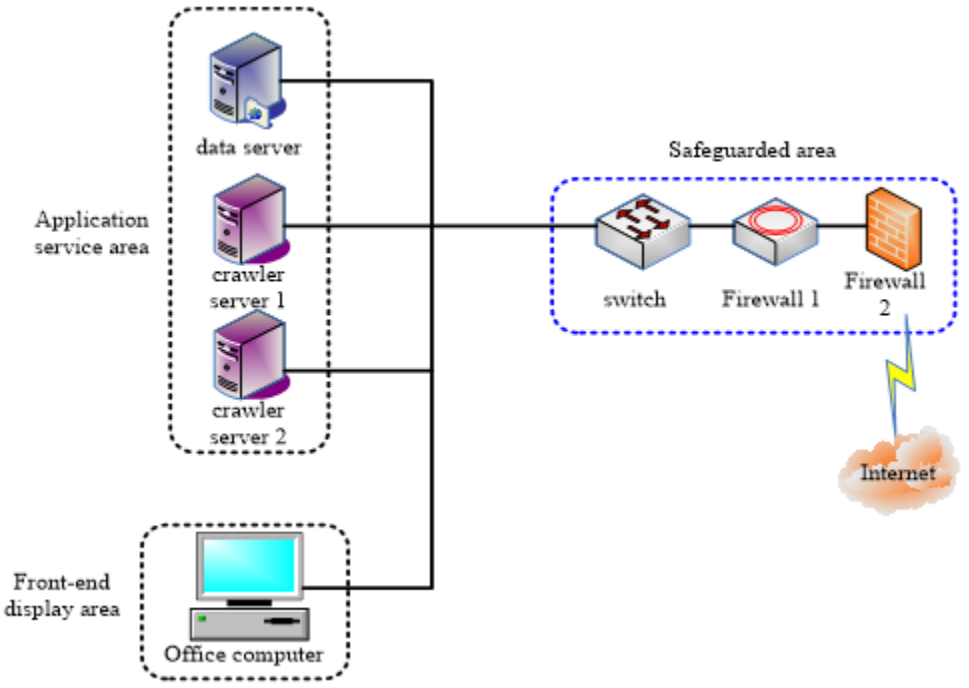
$$f\left(a\right) = f^{(3)}\left(f^{(2)}f^{(1)}\left(a\right)\right) \tag{1}$$

The function f is a description for a certain network layer.

How to use the existing network environment parameters to effectively predict the probability of network node and link failure in a certain period of time in the future has become an important challenge in current network virtualization research (F. Chen & Jahanshahi, 2018).

In theory, the structure of a general neural network can solve the problem of information loss caused by parameter selection and distance, but in practice, it cannot achieve the desired effect

Figure 1. Network information security architecture



(Grassmann et al.,2018). LSTM can overcome the shortcomings of recurrent neural networks and achieve excellent results in many tasks(Zhong, B., & Cheng, S., 2022). LSTM adds a memory storage structure to the original recurrent neural network structure, as shown in Figure 2:

As shown in Figure 2, the output unit gate can affect the information of other storage structures (Kemker et al., 2018). Moreover, the forget unit gate can adjust the self-circulating connection state of the memory storage unit and remember or forget the previous network unit state information based on the training error.

The forward update of the LSTM neural network at each time step is explained below. According to the structure of the neuron, the activation vector of the input gate is Formula 2:

$$i\left(t\right)=\sigma\left(W_{ai}a\left(t\right)+W_{hi}h\left(t-1\right)+W_{ci}s\left(t-1\right)\right) \tag{2}$$

W_{ai} is the transfer weight between neuron connections. $a\left(t\right)$ is the input vector of the network, $h\left(t-1\right)$ is the output vector of the external neuron at the previous time point, and $\left(t-1\right)$ is the neuron cell state at the previous time point. The state value of the memory storage structure is updated according to Formula 3:

$$b_{g}\left(t\right)=\tanh\left(W_{ac}a\left(t\right)+W_{hc}h\left(t-1\right)\right) \tag{3}$$

At time t, a historical data set of length n can be obtained. In the formula, W_{ac} is the input parameter matrix, and W_{hc} represents the length of the associated data for fault prediction.

$$A\left(n\right)=\left\{A\left(t-n+1\right),A\left(t-n+2\right),...,A\left(t-1\right),A\left(t\right)\right\} \tag{4}$$

In this paper, the time of the data feature refers to the network parameter statistics at a certain time point, and the time on the data label refers to the fault statistics in the time period. The network fault diagnosis model based on LSTM is shown in Figure 3:

Figure 2. LSTM structure diagram

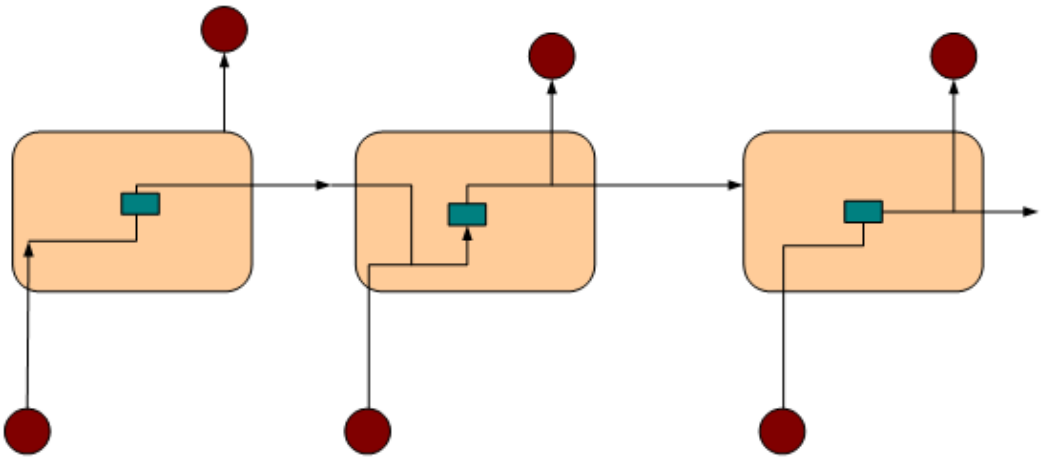
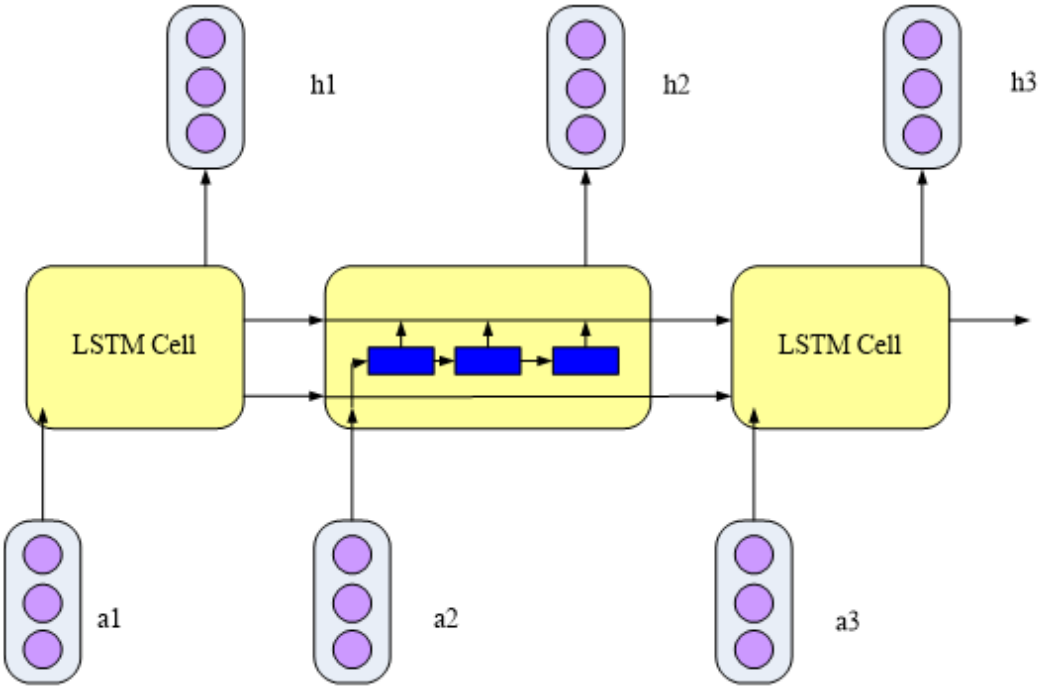


Figure 3. LSTM-based network fault diagnosis model



As shown in Figure 3, the output of the first layer of LSTM neurons is transmitted to the next layer of LSTM neuron memory, and it is also transmitted to itself and the same layer of neuron memory blocks (Lu et al.,2020).

In this paper, softmax is selected as the activation function of the fully connected layer. The form of the softmax function is shown in Formula 5:

$$\sigma\left(z\right)_j = \frac{e^{z_j}}{\sum_{k=1}^{k} e^{zk}} \tag{5}$$

Activation functions are used in deep learning to build networks that address nonlinear problems. The ability of the deep network would be enhanced only after the activation function with nonlinearity is used.

3.2 Heterogeneous Wireless Network Fault Diagnosis Based on a Convolutional Neural Network

Regression analysis of the data is performed, which is an important step to test the effect of the network security detection algorithm. In the process of network information security detection and implementation, it must first understand the use of gradient optimization during processing. The gradient-based optimization strategy is the one that is most frequently employed in deep learning. The goal of this training procedure is to reduce the loss function such that network security detection is accurate. In this paper, a convolutional neural network (CNN)-based two-stage fault diagnosis system is proposed. The neurons in each layer of a convolutional neural network are arranged in three dimensions: width, height, and depth, which are in contrast to conventional neural networks. Because

convolution is a two-dimensional template, the width and height are simple to comprehend. Instead of the depth of the entire network, convolutional neural networks define depth as the third dimension of the active data volume. The number of layers in the network is referred to as the network's overall depth, as shown in Figure 4:

The monitoring stage is the initial stage, as depicted in Figure 4. The monitoring application would then perform time series pattern analysis on the collected network data, match the fault characteristics in the network database, and analyse the acquired network data based on a minimal number of network characteristic factors. The approach suggested in this study enhances the time sequence of the original method, which can forecast network faults better than the conventional monitoring stage.

To ensure the generalization ability of the network security detection algorithm, a large data set is required at this time, and $E_{a,b\sim pdata}$ represents the data generation distribution, which is Formula 6:

$$J\left(\theta\right)=E_{a,b\sim pdata}L\left(a,b,\theta\right)=\frac{1}{m}\sum_{i=1}^{m}L\left(a^{(i)},b^{(i)},\theta\right) \tag{6}$$

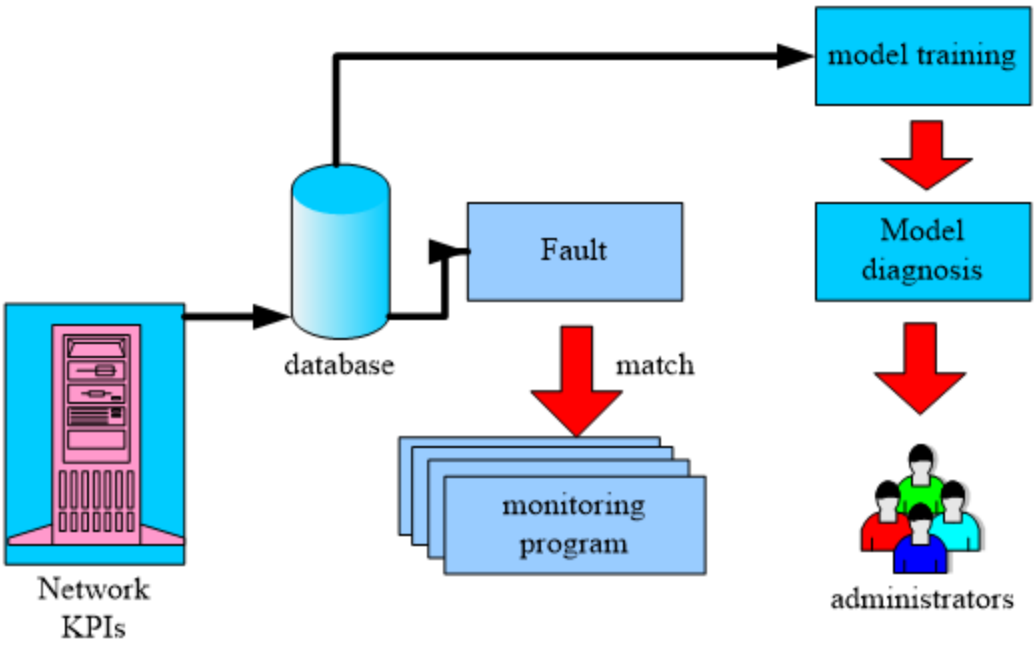
L is the loss function for each sample:

$$L\left(a,b,\theta\right)=-\log p\left(b\left|a;\theta\right.\right) \tag{7}$$

For these additive loss functions, gradient descent needs to be computed:

$$\Delta_{\theta}J\left(\theta\right)=\frac{1}{m}\sum_{i=1}^{m}L\left(a^{(i)},b^{(i)},\theta\right) \tag{8}$$

Figure 4. Two-stage fault Diagnosis scheme



The gradient estimate is expressed here as Formula 9:

$$g = \frac{1}{m}\sum_{i=1}^{m'} L\left(a^{(i)}, b^{(i)}, \theta\right) \tag{9}$$

After a small number of samples, gradient descent can be estimated:

$$\theta \leftarrow \theta - \in g \tag{10}$$

$\in$ is the learning rate. Since deep learning is developed based on machine learning, people should first understand the general method of building machine learning. If people take the simplest linear regression algorithm as an example, that is, a data set consisting of a and b components, the loss function is Formula 11:

$$J\left(w,b\right) = -E_{a,b\sim pdata} \log p_{\mathrm{mod}\,el}\left(b\left|a\right.\right) \tag{11}$$

The loss function usually consists of several lines, and an estimate of the maximum probability can be obtained by minimizing the loss function:

$$J\left(w,b\right) = \lambda\left\|\left\|w\right\|\right\|_2^2 - E_{a,b\sim pdata} \log p_{\mathrm{mod}\,el}\left(b\left|a\right.\right) \tag{12}$$

Most loss functions no longer have optimal closed solutions, which requires choosing an iterative numerical optimization process, most commonly gradient descent.

3.3 Security Task Assignment Based on Cyber-Physical Fusion and Deep Learning

In this paper, the reputation mechanism is used to measure the probability of a node obtaining a task, that is, the higher the reputation value is, the higher the probability of obtaining a task. Reputation is mainly measured by the historical experience of the node performing tasks in the past time, that is, the reliability of its future tasks is predicted by its past task performance behavior.

The reputation of each unit depends on its ability to perform its functions and the state of its network security. Therefore, this paper defines the reputation value of a node based on the functional safety degree λ_f and the network safety degree λ_c. Assuming that the reference starting time for calculating the reputation value is t_0, then the reputation value of unit node i at time t is Formula 13:

$$r_i^{t_0\to t} = \alpha\lambda_f^{t_0\to t} + \beta\lambda_c^{t_0\to t} \tag{13}$$

The two functions $\lambda_c^{t_0\to t}$ and $\lambda_f^{t_0\to t}$ represent the cumulative functional safety and network safety of unit i from time t_0 to t, respectively. α and β are two parameters representing the relative importance of the two parts, $\alpha+\beta=1$. For simplicity, the reference starting time of the reputation value can be ignored, and the current reputation value of sensor or actuator node i can be directly recorded as r_i.

Assuming that the controller of an existing cluster is P, the reputation value of the cluster at time t can be defined as Formula 14:

$$R_P = \sigma \bullet \sum_i w_i r_i^{t_0 \to t} + \omega \bullet \lambda_c + \partial \lambda_f \tag{14}$$

w_i represents the weight of sensor or actuator unit i in the cluster. λ_c and λ_f stand for controller functional safety and network safety, respectively.

To achieve safe task assignment, the probability of the task obtaining reliable required capability resources during execution should be improved. Therefore, a secure allocation algorithm should be based on the reputation of the node and the capabilities it possesses. Task assignment is divided into two stages: cluster assignment and assignment of sensors and actuator units within the cluster.

Assuming that the set of capability resources required by task t is C_t and the set of capability resources owned by the controller's own cluster reported by the human-computer interaction agent is C_p, then the system would assign task t to the following controller as Formula 15:

$$Final - P = \arg\max \left(\mu \cdot \frac{1}{\left| C_t - C_p \right| + 1} + v \cdot R_p \right) \tag{15}$$

In the formula, μ and v are the indicators used to balance the controller's ability resource satisfaction degree and the importance of reputation value, $\mu + v = 1$. If the importance of capability resources is emphasized when allocating resources, then μ can be set to a higher value. If the importance of safety is emphasized, v can be set to a higher value.

Assuming that the set of capability resources required by task t is C_t and the set of capability resources owned by unit i through its own cluster reported by the communication agent is C_i, then the controller assigns task t to the following units (denoted as $Final - i$ units):

$$Final - i = \arg\max \left(\mu \cdot \frac{1}{\left| C_t - C_i \right| + 1} + v \cdot r_i \right) \tag{16}$$

Due to the existence of malicious agents, the task may be assigned to one or more malicious agents and thus cannot be executed successfully. The clustering control system needs to assign tasks to security agents as much as possible, and once the above situation is detected, it needs to reallocate resources. It takes considerable time to reassign tasks, so the effect of the reputation mechanism proposed in this paper can also be reflected from the time of task execution in a malicious environment.

The following sections analyse the execution time of tasks with and without the reputation mechanism. When the credit mechanism is not used, the task would randomly obtain the resources it needs from the agent. After adopting the reputation mechanism, the task only acquires resources with high reputation in the system, thus effectively avoiding being assigned to malicious resources.

Assume that the total number of tasks to be executed by a system is n; the number of resources required to execute a task is r; the number of resources owned by each cluster is o; and the total number of resources of the system is g. The number of resources that are hacked and become malicious resources is h. The probability of being assigned to a malicious resource is P_h. The calculation formula of the probability P_h allocated to malicious resources under the no-reputation mechanism is as follows:

$$P_h = 1 - \frac{P_{g-h}^{nr}}{P_g^{nr}} \tag{17}$$

P_{g-h}^{nr} is a permutation that finds all the resources required by n tasks from the unattacked resources. P_g^{nr} is a permutation of finding all resources required by n tasks from all resources. $\frac{P_{g-h}^{nr}}{P_g^{nr}}$ is the probability that the resources allocated by n tasks are completely safe resources. For easier calculation, after simplification, it obtains:

$$P_h = 1 - \frac{P_{g-nr}^{h}}{P_g^{h}} \tag{18}$$

The storage of reputation value has always been a core issue of reputation mechanisms. According to the characteristics of the cluster control system, the reputation storage mechanism is designed in this paper: the operation management personnel store the reputation of each cluster. Each controller stores the reputation of the sensors and actuator units in the cluster. Therefore, the sensor and actuator unit can also select the sensor and actuator unit with high reputation value in the cluster to cooperate in the process of executing the task.

4. NETWORK SECURITY ASSURANCE EXPERIMENT BASED ON DEEP LEARNING

The mobile network in this simulation scenario consists of five macro base stations, each of which spans a hexagonal cell with a radius of approximately 600 meters. A wireless network, a carrier network, and a core network—all of which are composed of 2/3/4/5G networks—make up the fundamental structure of mobile communication networks. Users are randomly placed in their respective cells, and there are 139 users in the macro base station, which has several low-energy nodes deployed in densely populated locations. In the low power base station, there are 305 customers. The details are displayed in Table 1:

As shown in Table 1, the occurrence times of these faults are preset, which is convenient for manually generating training data labels. In the test data set, the time when the fault occurs is also set in a prespecified way. After the fault occurs, the network enters the abnormal state; when the fault occurs, the network enters the normal operation state, and the parameters of the network buffer state in the normal operation state are not recorded.

4.1 Experiment on the Accuracy of Network Fault Prediction

The accuracy of the training and testing sets corresponding to the sample size of the LSTM method when the number of historical data records is 400 is shown in Figure 5:

As seen in Figure 5(a), the accuracy of the training is very unsteady because the network state data that were acquired when the historical data record was 200 cannot accurately capture the change trend of the network state. Although the accuracy on the training set is fairly high, as seen from (b), the performance on the test set is subpar. The accuracy rate on the training set gradually rises with more data records, the stability improves, and the accuracy rate on the test set rises dramatically. However, the speed barely improved when the number of historical data records was 400.

Table 1. Network simulation parameters

Simulation Parameters	Macro Base Station	Low Power Base Station
Number of base stations	5	5
number of users	139	305
Transmission power	45 dBm	45 dBm
shadow fading standard deviation	6 dB 1.1	8 dB 1.2
Antenna gain	13 dBi 1.3	6 dBi 1.4
operating mode	LTE 5 MHz FDD 1.5	LTE 20 MHz FDD(Default Channel Index) 1.6
Receive sensitivity	-105 dBm(Default) 1.7	-102 dBm 1.8

Next, the network security diagnosis time and accuracy of the CNN are simulated, as shown in Table 2.

As shown in Table 2, with the increase in historical records, the time used by the CNN to predict every 100 historical data points also shows an increasing trend. After the deep learning network is trained, the network parameters are determined, so the calculation is simple and the time consumption is relatively small. Since this paper proposes that in the abnormal symptom diagnosis stage, the similarity algorithm is only compared with the limited fault data records. This filters out many normal data samples, and the number of requests transmitted to the CNN model is greatly reduced, which is superior to the LSTM model in the timeliness of diagnosis. If the detection delay is relatively low, the diagnostic method has good diagnostic performance and can take countermeasures in a short time after the fault occurs. If the detection delay is relatively large, it may bring a large performance loss to the system.

When taking a different amount of historical data as the prediction input each time, the comparison of the fault recall rate of different algorithms is shown in Figure 6:

As shown in Figure 6(a), although the recall rate of CNN is higher than that of LSTM, the difference between the two methods is not large. From Figure (b), it can be found that the recall of CNN is not only higher than that of LSTM but also the gap is getting bigger and bigger.

When there is a local correlation in the data, the convolution operation of CNN can effectively capture the local features. For example, in image classification, the spatial relationship between pixels is very important, and the convolution layer of CNN can extract the features of local regions. In contrast, LSTM is more suitable for long-term dependencies in serial data, and CNN is more suitable for data with strong local correlation.

4.2 Experiments of Reputation Machine System on Communication Network Security

Under a certain total amount of resources (in simulation experiments, assuming a total of 100 resources), regardless of whether the security resources in the system are sufficient, as long as malicious resources exist, the task of controlling the system may be assigned to malicious resources. With the increase in the number of malicious resources in the system, the probability of allocating malicious resources increases rapidly. To verify the importance of the reputation mechanism to network security, this paper simulates the relationship between the probability of tasks assigned to malicious resources and the number of tasks and malicious resources through MATLAB simulation, as shown in Figure 7.

Figure 5. LSTM accuracy under different numbers of records: (a) LSTM accuracy in the training set, (b) LSTM accuracy in the test set

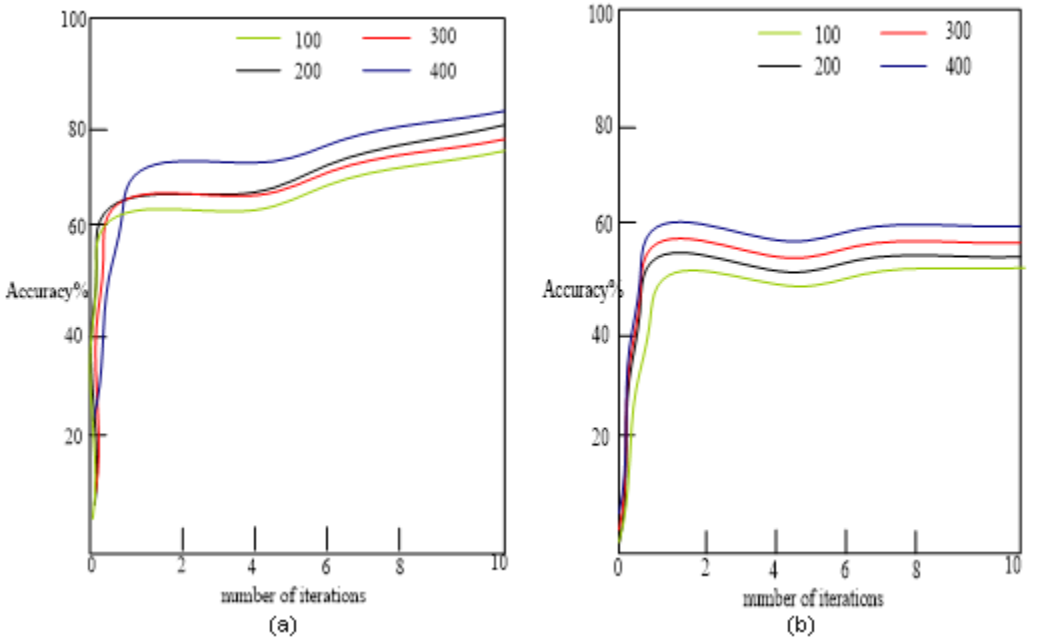


Table 2. Network security diagnosis time and accuracy of CNN

Number of Data	Time/s	Accuracy
100	0.03s	89%
200	0.05s	90%
300	0.07s	91%
400	0.08s	92%
500	0.12s	93%
600	0.15s	95%

As shown in Figure 7 (a), it was found that in the absence of a reputation mechanism, when the malicious resource is 20, the task begins to be attacked, and the probability increases. When the reputation mechanism is found from Figure (b), when the malicious resource is greater than a certain value, that is, when the security resource is insufficient, the malicious resource begins to play a role, and the probability of task assignment to the malicious resource begins to increase. When the security resources are insufficient, there are obvious differences in the probability of task assignment to malicious resources

4.3 Prediction Performance Test of CNN

In recent years, with the development of information globalization and the popularization of network applications, people have become increasingly dependent on the internet. Computer networks have become indispensable in people's work, study and life. On the other hand, the number of intrusion security incidents is also rapidly increasing. The network attacks from 2014 to 2019 are shown in Table 3.

Figure 6. Recall rates for both methods: (a) recall rates in the training set and (b) recall rates in the test set

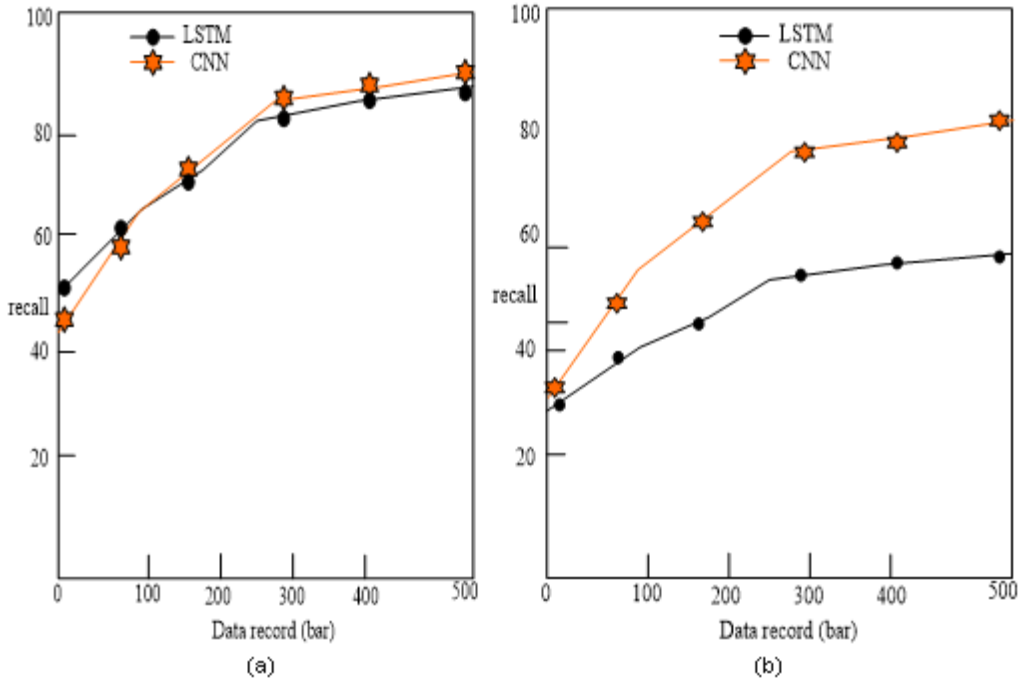
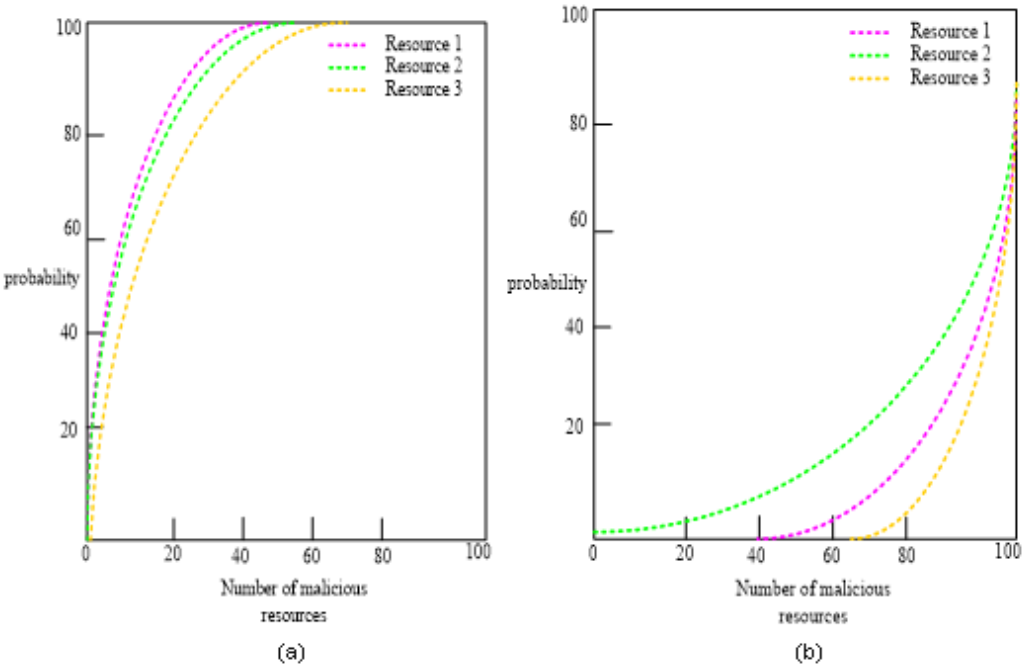


Figure 7. Impact of reputation mechanism on information security: (a) attack probability of malicious resources without a reputation mechanism, (b) attack probability of malicious resources with a reputation mechanism



As shown in Table 3, common network communication information security problems include network vulnerabilities, viruses, external attacks and so on. At the same time, the destruction of information systems and illegal intrusion activities are still increasing, and the network threat continues to spread at an alarming rate, which brings huge economic losses to people's production and life. The current network security has aroused widespread concern both inside and outside the industry.

Deep learning can recognize dangers to the present network environment in real time and comprehend the current status of the complete network operation. This forecasts future security trends and gives network security administrators a solid foundation on which to base timely and correct security decisions. In the process of training the CNN, the relationship between the number of training iterations and the accuracy of the model when the training reaches a steady state is shown in Figure 8:

As shown in Figure 8, the prediction results of the platform for the next moment of the system environment are as follows: the probability of developing in a safe state is between 0.5 and 7, and the probability of developing in a dangerous state is between 0.3 and 0.5. The platform can make a clear trend prediction for the future security situation of the system environment, that is, the probability of tending toward safety and tending toward danger are comparable. According to this rule, security administrators can make real-time judgments based on network security trends and take defensive measures in advance.

CNN realizes parameter sharing through convolution operation, that is, different regions share the same weight, thus reducing the number of parameters of the model and increasing the training efficiency of the model. This is very important for processing data such as large-scale images. However, the LSTM model has a large number of parameters, and the processing of large-scale data sets may be time-consuming.

To validate the method proposed in this article, KDD cup99 was used for training and ultimately tested. The model in this article is implemented using the Python language, and its framework is TensorFlow. There are a total of 5 types of attacks, namely, Normal, Dos, Probe, R2L, and U2R. The following article would measure the performance of the model from two perspectives: accuracy and false alarm rate, as shown in Table 4 and Table 5:

From Table 6, it can be clearly seen that compared with the other two methods, the method proposed in this paper has a higher accuracy and a significantly higher false alarm rate. This also indicates that the use of parallel mechanisms greatly improves the network attack detection ability.

5. CONCLUSION

With the development of computer technology, the amount of various data has increased dramatically. How to transmit a large amount of data stably, quickly and safely has become a current research topic. Network communication information security is also an urgent problem that must be solved. To better judge and predict the trend of network communication information security, this paper conducted

Table 3. Cyber attacks from 2014 to 2019

Years	network Vulnerability	Virus	Outside Attack
2014	39%	42%	46%
2015	45%	46%	51%
2016	49%	48%	54%
2017	54%	53%	57%
2018	58%	55%	63%
2019	60%	62%	66%

Figure 8. Relationship between the number of training iterations and CNN accuracy

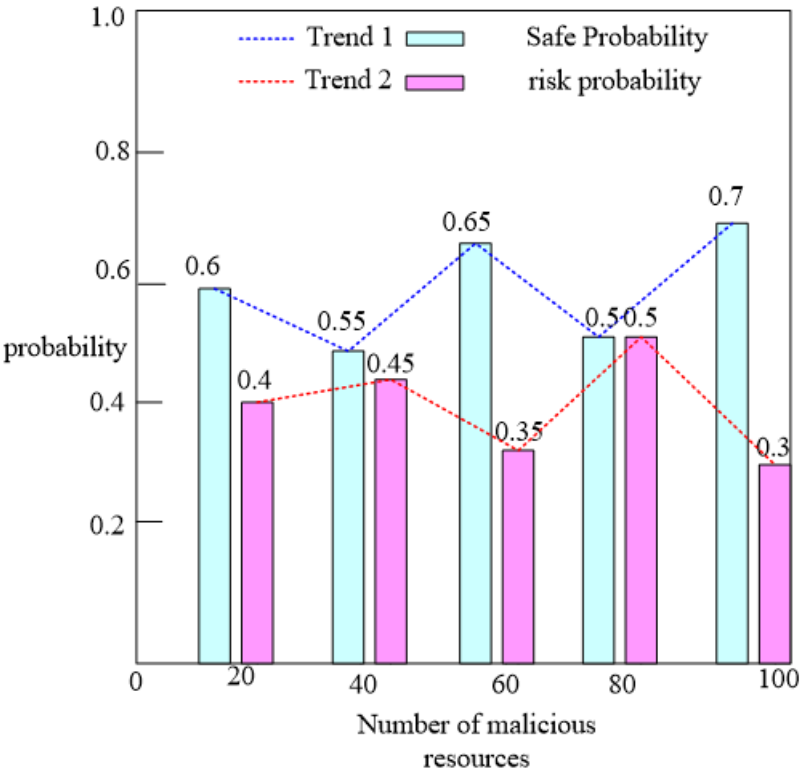


Table 4. Training set categories and corresponding proportions

Types	Normal	Dos	Probe	R2L	U2R
Proportion of total data (%)	8000	1000	2500	1600	100
1.1	60.6	7.6	18.9	12.1	0.8

Table 5. Test set categories and corresponding proportions

Types	Normal	Dos	Probe	R2L	U2R
Proportion of total data (%)	7000	2000	2000	2100	100
1.1	53	15.2	15.2	15.8	0.8

a detailed analysis of cyber-physical fusion and deep learning and proposed the LSTM method and CNN method to diagnose and predict network information security. Both methods can predict the security situation in future periods, but the accuracy rates of the two methods are not consistent. This paper also proposed the effect of the reputation mechanism on network security. Through experiments, it is found that the probability of being attacked by malicious resources is lower when there is a reputation mechanism than when there is no reputation mechanism. However, this paper also had some shortcomings, and the utilization rate of the experimental simulation environment resources

Table 6. Comparison results of the two methods

Model	Types	Accuracy (%)	False Alarm Rate (%)
The method in the paper	Normal	98.8	0.6
	Dos	96.1	2.6
	Probe	95.9	3.8
	R2L	92.8	2.4
	U2R	95.8	1.3
CNN model	Normal	95.8	2.6
	Dos	96.3	2.6
	Probe	95.4	2.9
	R2L	94.5	2.8
	U2R	95.8	0.9

proposed in this paper was still insufficient. Due to the limitation of experimental hardware resources, this paper can only realize communication between the single board and the computer, so the smooth communication of the Gigabit network should be ensured in future work.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

FUNDING STATEMENT

This work is supported by National Natural Science Foundation of China, under Grant 62002179 within NanTong University China.

REFERENCES

Chen, F., & Jahanshahi, M. R. N. B.-C. N. N. (2018). Deep Learning-Based Crack Detection Using Convolutional Neural Network and Naïve Bayes Data Fusion. *IEEE Transactions on Industrial Electronics*, *65*(5), 4392–4400. doi:10.1109/TIE.2017.2764844

Chen, J. M., Zhao, F., & Xing, H. (2020). Research on Security of Mobile Communication Information Transmission Based on Heterogeneous Network. *International Journal of Network Security*, *22*, 145–149.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security*, *68*, 1–15. doi:10.1016/j.cose.2017.03.010

Grassmann, F., Mengelkamp, J., Brandl, C., Harsch, S., Zimmermann, M., Linkohr, B., Peters, A., Heid, I. M., Palm, C., & Weber, B. H. F. (2018). A Deep Learning Algorithm for Prediction of Age-Related Eye Disease Study Severity Scale for Age-Related Macular Degeneration from Color Fundus Photography. *Ophthalmology*, *125*(9), 1410–1420. doi:10.1016/j.ophtha.2018.02.037 PMID:29653860

Haenssle, H. A., Fink, C., Schneiderbauer, R., Toberer, F., Buhl, T., Blum, A., Kalloo, A., Hassen, A. B. H., Thomas, L., Enk, A., Uhlmann, L., Alt, C., Arenberger, P., Bakos, R. M., Baltzer, A., Bertlich, I., Blum, A., Bokor-Billmann, T., & Bowling, J. (2018). Man against machine: Diagnostic performance of a deep learning convolutional neural network for dermoscopic melanoma recognition in comparison to 58 dermatologists. *Annals of Oncology : Official Journal of the European Society for Medical Oncology*, *29*(8), 1836–1842. doi:10.1093/annonc/mdy166 PMID:29846502

Han, J., Zhang, D., Cheng, G., Liu, N., & Xu, D. (2018). Advanced Deep-Learning Techniques for Salient and Category-Specific Object Detection: A Survey. *IEEE Signal Processing Magazine*, *35*(1), 84–100. doi:10.1109/MSP.2017.2749125

Joshi, C., & Singh, U. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, 128–137. doi:10.1016/j.jisa.2017.06.006

Kemker, R., Salvaggio, C., & Kanan, C. (2018). Algorithms for semantic segmentation of multispectral remote sensing imagery using deep learning. *ISPRS Journal of Photogrammetry and Remote Sensing*, *145*, 60–77. doi:10.1016/j.isprsjprs.2018.04.014

Li, H., Jia, X., & Dong, M. (2018). Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing. *IEEE Network*, *32*(1), 96–101. doi:10.1109/MNET.2018.1700202

Lu, J., Liu, X., Zhang, S., & Chang, Y. (2020). Research and Analysis of Electromagnetic Trojan Detection Based on Deep Learning. *Security and Communication Networks*, *2020*, 1–13. doi:10.1155/2020/6641844

Shang, W., Gong, T., Chen, C., Hou, J., & Zeng, P. (2019). Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees. *Security and Communication Networks*, *2019*, 1–11. doi:10.1155/2019/3574675

Xue, X., Wu, X., Zhang, J., Zhang, L., Zhu, H., & Mao, G. (2021). Aggregating Heterogeneous Sensor Ontologies with Fuzzy Debate Mechanism. *Security and Communication Networks*, *2021*, 1–12. doi:10.1155/2021/2878684

Yang, X., Wang, W., Xu, X., Pang, G., & Zhang, C. (2018). Research on the Construction of a Novel Cyberspace Security Ecosystem. *Engineering (Beijing)*, *4*(1), 47–52. doi:10.1016/j.eng.2018.01.003

Young, T., Hazarika, D., Poria, S., & Cambria, E. (2018). Recent Trends in Deep Learning Based Natural Language Processing [Review Article]. *IEEE Computational Intelligence Magazine*, *13*(3), 55–75. doi:10.1109/MCI.2018.2840738

Zhang, H., Guo, Y., & Li, T. (2019). Multifeature Named Entity Recognition in Information Security Based on Adversarial Learning. *Security and Communication Networks*, *2019*, 1–9. doi:10.1155/2019/3038586

Zhang, Q., & Zhu, S. (2018). Visual interpretability for deep learning: A survey. *Frontiers of Informaion Technology & Electronic Engineering*, *19*(1), 27–39. doi:10.1631/FITEE.1700808

Zhong, B., & Cheng, S. (2022). A fast encryption method of social network privacy data based on blockchain. *International Journal of Web Based Communities*, *18*(3-4), 345–356. doi:10.1504/IJWBC.2022.125502

Zhu, X. X., Tuia, D., Mou, L., Xia, G., Zhang, L., Xu, F., & Fraundorfer, F. (2017). Deep Learning in Remote Sensing: A Comprehensive Review and List of Resources. *IEEE Geoscience and Remote Sensing Magazine*, *5*(4), 8–36. doi:10.1109/MGRS.2017.2762307

Qu Yan is a postgraduate student at Nantong University. His main research interests are information security and signal processing.

Chuyue Wang are currently works in Nantong University China.

Jie Wan is currently works as a Lecturer in Nantong university China since 2015. her main research topics are the Internet of Things, Deep Learning and Human activity recognition. Dr, Wan compete her PhD from the University College Dublin, Ireland in 2015.