Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7182989, 17 pages
https://doi.org/10.1155/2022/7182989

Research Article

Industrial Internet of Things Anti-Intrusion Detection System by Neural Network in the Context of Internet of Things for Privacy Law Security Protection

Di Teng

Department of Law, Harbin Finance University, Harbin 150000, China

Correspondence should be addressed to Di Teng; 2009035@hrbfu.edu.cn

Received 2 April 2022; Revised 12 May 2022; Accepted 13 May 2022; Published 6 June 2022

Academic Editor: Mu-Yen Chen

Today, the Industrial Internet of Things (IIoT) and network technology are highly developed, and network data breaches occur every year. Therefore, an anti-intrusion detection system has been established to improve the privacy law security protection of IIoT. In the adversarial network, the security performance requirements and structural system of the Internet of Things have high-strength requirements. The network system must adopt a system with strong stability and a low data loss rate. After comparing a large number of network structures, the initial network technology in deep learning is adopted. The Convolutional Neural Network (CNN) technology for handwritten character recognition optimizes and upgrades the LeNet-5 network, and the new LeNet-7 is built. Additionally, three network technologies are combined, and an IIoT anti-intrusion detection system is constructed. The performance of the system is tested and verified. The model has high data accuracy, detection rate, and low false-positive rate. The model's generality on high-performance data is validated and compared with privacy-aware task offloading methods, achieving the best performance. Therefore, the system can be applied to the data privacy law security protection of IIoT.

1. Introduction

Due to the rapid development of the Internet of Things (IoT) and 5th-Generation Mobile Network (5G) technologies, the data generated by network users across the country have gathered into a vast network, and it has penetrated any corner of work and life. This significantly improves the convenience and work efficiency of people's lives. Renewable energy has become one of the main resources to help the world protect the environment from pollution and provide people with new energy [1]. Because of the rapid development of the IoT, each section of data in the network contains private data such as the user's personal information and location information, the enterprise's business secrets, and the state secrets of the government. In recent years, data breaches have occurred frequently. For example, in 2010, diplomatic mails from the United States were leaked through WikiLeaks [2]. In 2016, the LinkedIn network platform spread to nearly 500 million users [3]. The economic losses caused by data breaches averaged 3.6 million U.S. dollars each year, according to the report released by IBM in 2020 [4]. The news all show that today's networks face serious security threats, and network attacks occasionally occur, especially in the field of the Industrial Internet of Things (IIoT). It is precisely because of the increased occurring IoT security issues that some scholars have emphasized the need to pay attention to the privacy protection of network data and the accountability of data leakage [5]. In recent years, many professionals have researched the security issues of IIoT. Hui et al. used the N-shift encryption scheme and Lyapunov stability theory to establish a chaotic secure communication scheme to solve the security risks in data transmission [6]. Wei proposed a MAGAN model that is less affected by the data loss rate than the baseline comparison model. It shows better results than traditional processing methods [7]. Sharmeen et al. concluded that IIoT working environment is complex, malicious programs increase, and it is not easy to be found, and attacks from criminals are

the main reasons for IIoT security threats [8]. Therefore, ensuring the integrity, privacy, effectiveness, controllability, and antiattack of data in IIoT is the main work of current IIoT security technology research. And strengthening confidentiality measures, user authentication technology, and anti-intrusion detection technology are specific research projects. In the *Global Industrial Internet of Things Network Security Report*, anti-intrusion detection technology ranks third among current IIoT security protection measures [9], which shows that IIoT anti-intrusion measures can improve IoT security protection performance from the source. Balakrishnan et al. argued that since IoT involves many different entities and different applications, the vulnerability to unauthorized access is much higher. Today's cyberattacks facing communication networks are very powerful and very worrying [10]. Wei et al. proved that mobile smart terminals had become prominent targets of cyberattackers. Security vulnerabilities and privacy leaks seriously restrict the application development of IoT [11]. The IoT vulnerability situation is getting worse by the day. Therefore, the anti-intrusion technology of IIoT is studied. Bovenzi et al. [12] studied the hierarchical hybrid intrusion detection method in the IoT scenario and proposed a two-stage hierarchical network intrusion detection method. Their novel lightweight solution based on multimodal deep autoencoders performs anomaly detection. In addition to the performance advantages, the proposed system is suitable for distributed and privacy-preserving deployments. Additionally, the system limits the necessity of retraining, in line with the high efficiency and flexibility required for IoT scenarios.

This study will comprehensively analyze the initial network and IIoT anti-intrusion detection methods in deep learning and optimize them for the LeNet-5 network. Section 1 introduces and explains the background of the IIoT and mobile network technology. Section 2 carries out the performance test of the Internet of Things security protection system by introducing the Internet of Things mobile smart devices, combined with the structural analysis of the information technology industry. Section 3 tests the performance of the anti-intrusion detection model by using an improved Convolutional Neural Network (CNN). Section 4 draws experimental conclusions through the inductive arrangement and systematic summary of the data results, analysis, and discussion. The innovation is that the initial network and CNN are combined in deep learning to establish an anti-intrusion detection model. Deep neural networks are built to enhance the representational power of the model. The network successfully uses the ReLU activation function as the activation layer of the cellular neural network, which alleviates the gradient disappearance problem of the sigmoid activation function, and the convergence speed is faster. Smaller convolution kernels and smaller sliding strides are used. Compared with ordinary neural networks, the initial network has only two convolution kernel sizes. Therefore, the network can be further deepened. Furthermore, multiple small convolution kernels are introduced to reduce the total network parameters. Simple average pooling is used instead of fully connected layers as the output of the convolution operation. Characteristic patterns may appear in different locations in the image.

2. Methods

2.1. IIoT

2.1.1. The Concept of IIoT. IIoT is the abbreviation for the combination of IoT and industrial manufacturing to improve the efficiency of industrial automation products. IIoT can perceive the system, has the advantages of reliable transmission and processing intelligence, and is commonly used in transportation, power grids, factories, and environmental monitoring. There are generally four implementation stages [13–16]

For the first stage, intelligent control is shown in Figure 1. This node combines sensors, wireless sensor networks, and other modules through intelligent sensing to achieve industry data collection and control equipment

In Figure 1, communication technologies such as local networks or the Internet are used to connect sensors, controllers, machines, people, things, to form the connection between people and things and things and things and realize informatization, remote management control, and intelligent network. The IoT is an extension of the Internet. It includes the Internet and all resources on the Internet and is compatible with all applications on the Internet. But all elements in IoT (all devices, resources, communications, etc.) are personalized and privatized. For the second stage, the comprehensive exchange is shown in Figure 2. IIoT uses sensors and other modules to collect data and integrates information technology and features through communication technologies such as the Internet, mobile networks, wide area networks, or radio and transmits the data in real time and quickly.

In Figure 2, the communication protocol is the language of the networked world. But the industrial network world is often not as open and unified as the Internet, due to industries, application scenarios, network topology, and mutual games between major industrial enterprises and countries. With the advent of emerging concepts such as the Industrial Internet, traditional industrial protocols are underdeveloped in terms of security and future-proofing. Industrial control security has become an important part of national infrastructure security. IoT technology is the integration of the Internet and the idea of intelligent data analysis. The construction of an integrated system where hardware entities and software entities are placed is very important [17]. The deep application of the third stage is shown in Figure 3. Cloud computing, big data, and other platforms are used for modeling, analysis, and optimization to develop multisource heterogeneous data and find valuable information at a high speed and accuracy through data mining, data storage, and other technologies.

In Figure 3, the technological revolution is at some stage before the digital industrial revolution is truly revolutionized. After the invention of new technologies, industry professionals find their own internal technology gaps and choose new technologies that are suitable for them. Then,

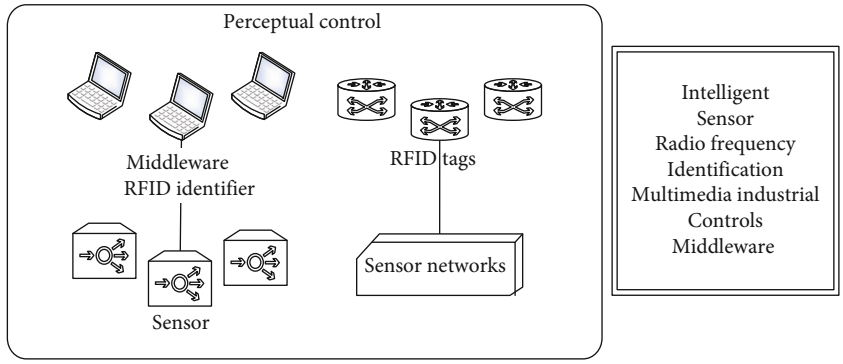

Figure 1: IIoT intelligent control stage.

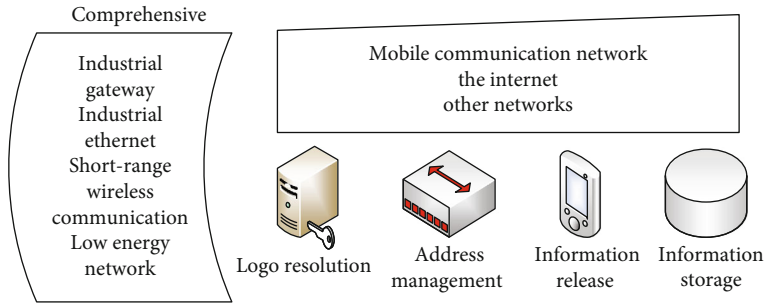

Figure 2: IIoT full communication stage.

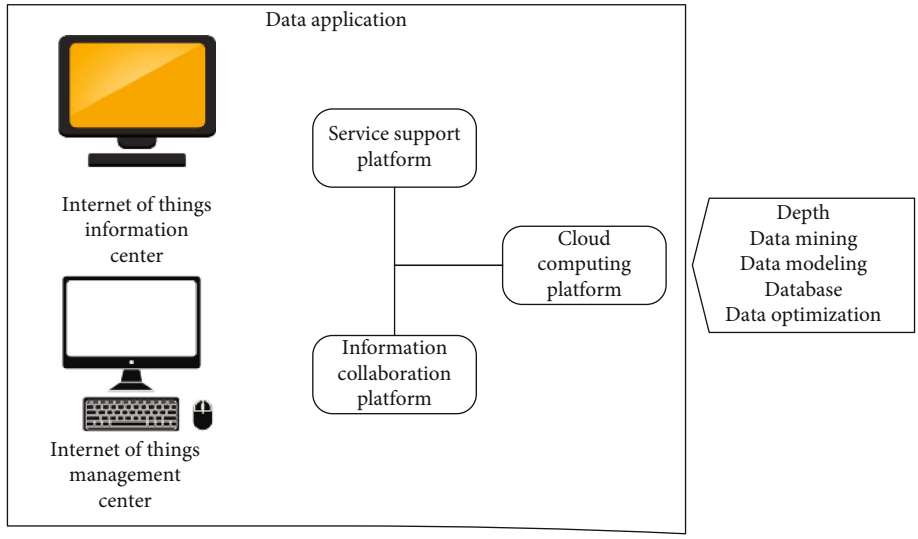

Figure 3: Deep application stage of IIoT.

the technology is further configured for each industry. However, technology generally remains the same. Different industries have different application scenarios, resulting in different requirements. Replacing the kernel of the network (i.e., the search machine) by spiral search and bubble net search can improve the accuracy and reduce the execution time to achieve the goal achieved by the retrieval function [18]. For the fourth stage, service innovation is shown in Figure 4. Through intelligent equipment, platform integration, and other technologies, it can provide users with innovative services, including smart logistics and competent medical care, and establish a new ecological model of IIoT in all aspects to improve service levels.

In Figure 4, the innovation stage of the IIoT is divided into three stages. Step 1 is cognitive innovation. The cognition of the Industrial Internet has gradually evolved and made breakthroughs, extending from the interconnection of equipment to the interconnection of people, machines, and things and then to the comprehensive link of all elements, the entire industrial chain, and the entire value chain.

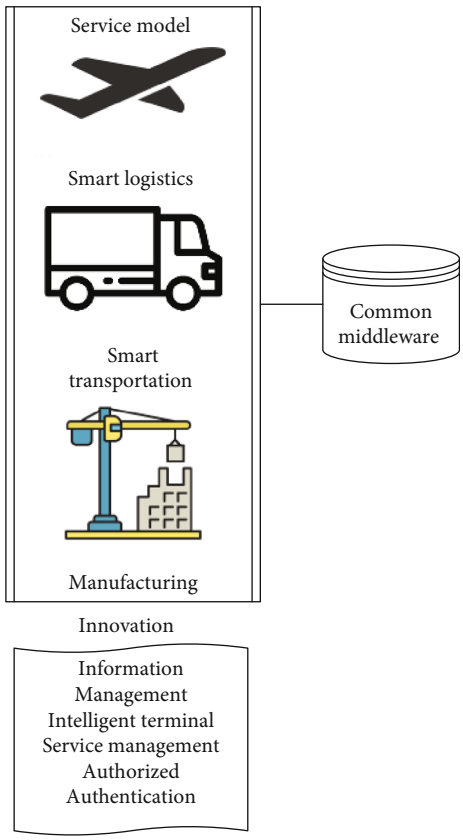

Figure 4: IIoT innovative service stage.

The Industrial Internet is an important cornerstone of the fourth industrial revolution. It is the deep integration of a new generation of network information technology and manufacturing. It can form a new industrial manufacturing and service system and promote the high-quality development of the real economy represented by advanced manufacturing.

Step 2 is idea innovation. The development law and mechanism of the Industrial Internet should be correctly grasped. The Industrial Internet is not a simple copy of the consumer Internet in the field of production, but a comprehensive expansion and leap of information network technology from virtual to physical, from life to production. This is not the connection extension of the consumer Internet from people to things, but the complete creation of a networked and intelligently upgraded infrastructure that expands from manufacturing to various industrial fields.

Step 3 is pattern innovation. The world today is going through a new round of major development, transformation, and adjustment, and the economic and social development of various countries is increasingly linked. Open cooperation is a realistic requirement to promote the stable recovery of the world economy. The development of the Industrial Internet is not limited to one country and one place. It must provide new impetus for the global economy to get out of the recession cycle in the process of "bringing in" and "going out." The development of the IIoT is not just to catch up and improve the development level of the country but also to provide an important breakthrough for global network governance to break the monopoly deadlock and move towards multiparty cogovernance based on new elements, new fields, and new forms.

2.1.2. The Structure of IIoT. Starting from the system and automation control, IIoT can be divided into four structures, comprehensive perception, network transmission, intelligent processing, and integrated application, as shown in Figure 5 [19–22].

In Figure 5, the key technologies of IIoT mainly include comprehensive perception, information transmission, intelligent processing, and information feedback. Comprehensive perception refers to the collection and acquisition of information on objects anytime and anywhere by using modern information collection and collection techniques. Information transmission is the reliable exchange and sharing of information anytime and anywhere through various communication networks and the Internet. Intelligent processing is to analyze and process the collected massive data and information, improve the insight into the industrial production environment and market, and realize intelligent decision-making and control. Information feedback means that the processed information is communicated to each production link in the form of program instructions to optimize the production structure and complete the production plan. In comprehensive perception, data collection equipment includes instruments and sensors. Its primary function is to realize the exchange of IIoT information. The most used control device is the Programmable Logic Controller (PLC). Its role is to issue commands to the control device. Field equipment includes complex collection equipment responsible for collecting on-site process data to achieve accurate control and management.

In network transmission, data transmission is a collection of multiple communication networks. Its function is to connect the network of various devices on-site, is a bridge between data collection and postprocessing, and integrates multiple connection methods such as 5G, Bluetooth, and Wi-Fi. In IIoT, a variety of connection technologies must be used to ensure the connection of many sensors and processors.

Intelligent processing includes communicator, manager and historical data server, remote control, and other equipment. Generally, cloud computing is used as a platform for large-scale data processing to ensure data security. Comprehensive application is a service based on practical application. It provides personalized assistance to users through information control, authentication, authorization, etc., and it is necessary to ensure the safe access and privacy protection of users.

2.2. Current Status of IIoT Security Testing. At present, the safety protection system used in actual production is subject to design constraints, causing the problem of incomplete analysis of the system's learning of data characteristics. It mainly exists in the following categories [23]:

Unable to extract the characteristics of multiple data: IIoT is more advanced than the current security protection

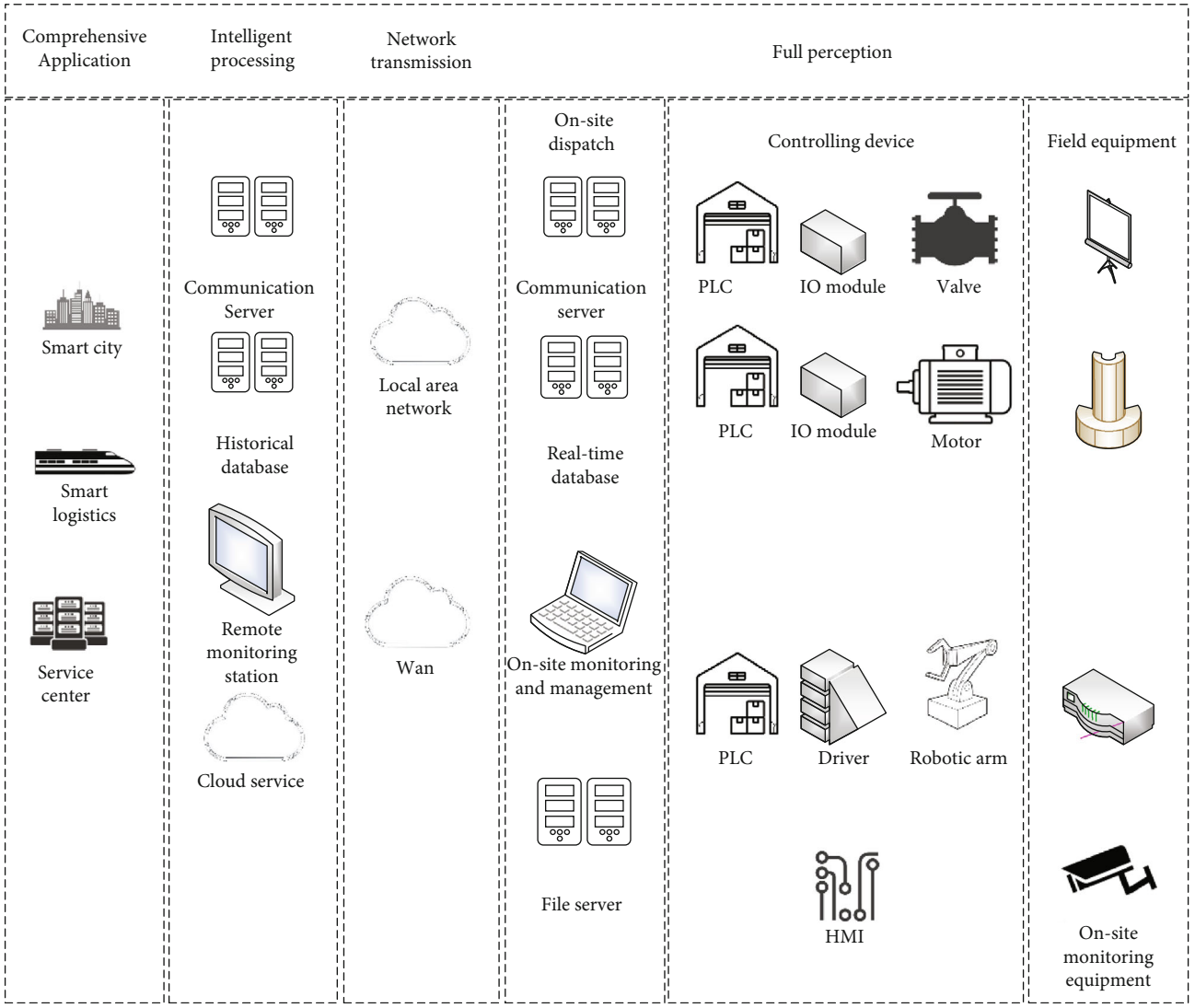

Figure 5: Four structures of IIoT.

system. Various new types of intrusion methods continue to appear. There is endless emergence of old protection systems that cannot process new high-latitude data and cannot extract the characteristics of the data, resulting in excessive energy consumption and inability to complete the work.

Detection accuracy is low: when computing many multidimensional data features, various calculation equations and parameters will be used, which requires high model processing performance. The current detection system cannot use these equations to cause the problem of low detection accuracy.

High false alarm rate: in the actual IIoT production process, there will be a variety of data exchanges involving multiple device communications. Due to loopholes in the traditional detection system, regular data access is judged as an intrusion, causing the device to fail to receive data usually.

What is designed here is an IIoT-IDS. According to the security requirements of IIoT [24], the detection system needs to have the following functions, as shown in Table 1.

The deeper integration of key elements of IIoT will boost traditional industries to develop faster, create better value, and improve productivity and production efficiency. There are also two sides to the deep application of IIoT. While it improves industrial efficiency and promotes the development of social processes, the security risks caused by the complexity and uncertainty of the network will affect the location of network value.

2.3. IDS

2.3.1. Basic Concepts. In James P. Anderson's Computer Security Monitoring and Surveillance in 1980, the concept of anti-intrusion detection was first proposed [25]. In 1986, Peter Neumann and Dorothy Denning established the real-time model of IDS [26]. They applied this model to computer security defense work for the first time. The IDS is essentially a network security management system, and its function diagram is shown in Figure 6. The working principle is to collect and analyze data information in the network

Table 1: Functional requirements of the detection system.

Functional requirements	Describe
Stability	Because the IIoT keeps running for a long time and almost does not allow the system to restart or rest, it is necessary to ensure the long-term operation of the system.
High precision	Distinguishing between targeted intrusions and regular user access requires a high degree of identification.
Timeliness	In the long-term work, it is necessary to ensure the accuracy of the data, no packet loss phenomenon can occur, and intrusion behavior can be detected in time.
Versatility	Because IIoT work types are divided into multiple systems, they need to be highly adaptable and easy to deploy.

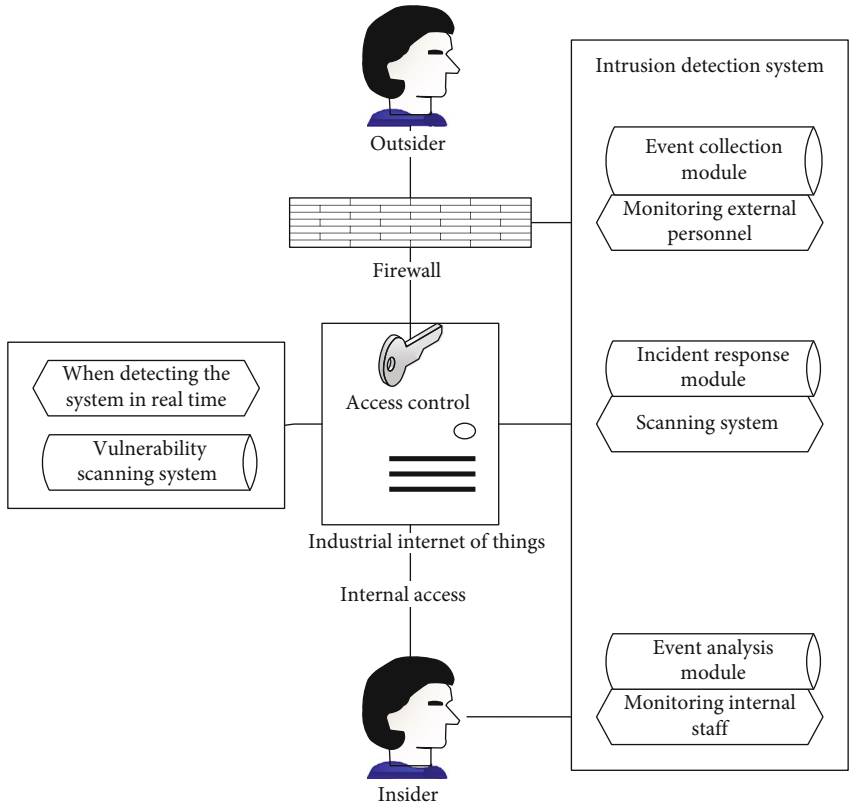

Figure 6: Schematic diagram of the role of IDS.

to extract offensive details and behaviors to determine whether the data has intrusions. Unauthorized or abnormal access behavior in the network is judged [27].

In Figure 6, since the system cannot be completely prevented from being attacked or intruded, the intrusion detection system becomes a system that can detect attacks or intrusions in time and provide valuable security alerts to security managers. As the actual harm of intrusion events is increasing, people pay more and more attention to intrusion detection systems. Intrusion detection system has become an important link in the network security architecture. The IDS can effectively judge abnormal network phenomena and protect the system, equipment, and machinery. The IDS extends the firewall, which usually includes the behavior subject, resource objects, audit records, behavior files, abnormal records, and processing rules [28]. The general detection process is shown in Figure 7.

In Figure 7, the first steps of professional business process management include process design, analysis, and optimization. Design includes documenting the actual state of existing processes. The relevant knowledge held by the employees of the process is collected and integrated, which not only improves the transparency of the process but also allows for a more in-depth analysis of the process. Structured and process-organizational models can reflect the complexity of business operations and simplify them into manageable terms. The IDS needs to identify abnormal behaviors accurately and efficiently. When designing the structure, it must have all the mentioned functions. Therefore, referring to the general process of the IDS, the basic flow of the IIoT-IDS is shown in Figure 8.

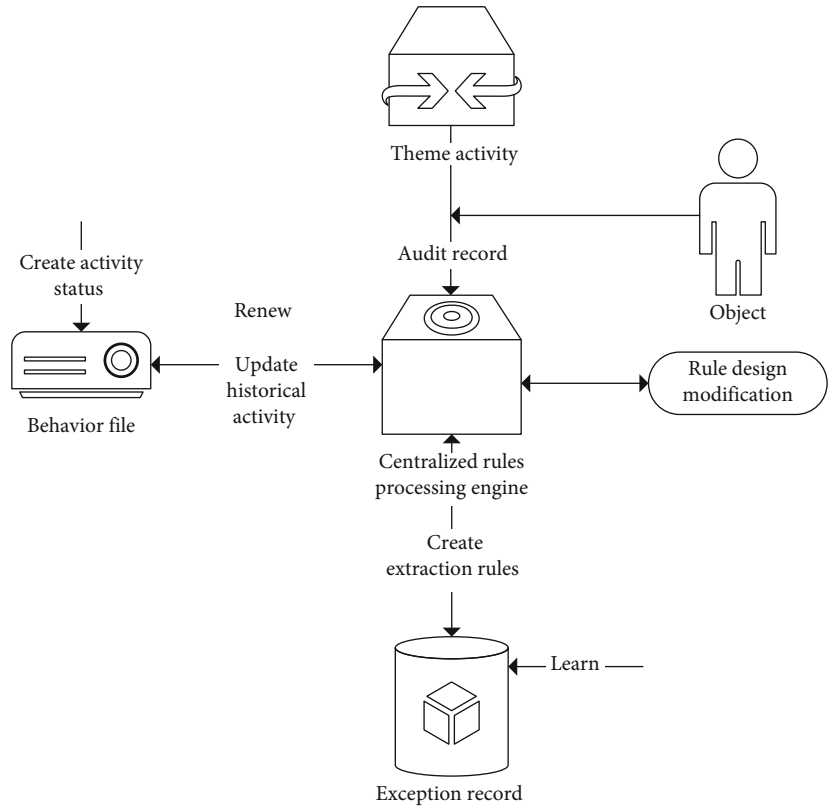

Figure 7: General IDS process.

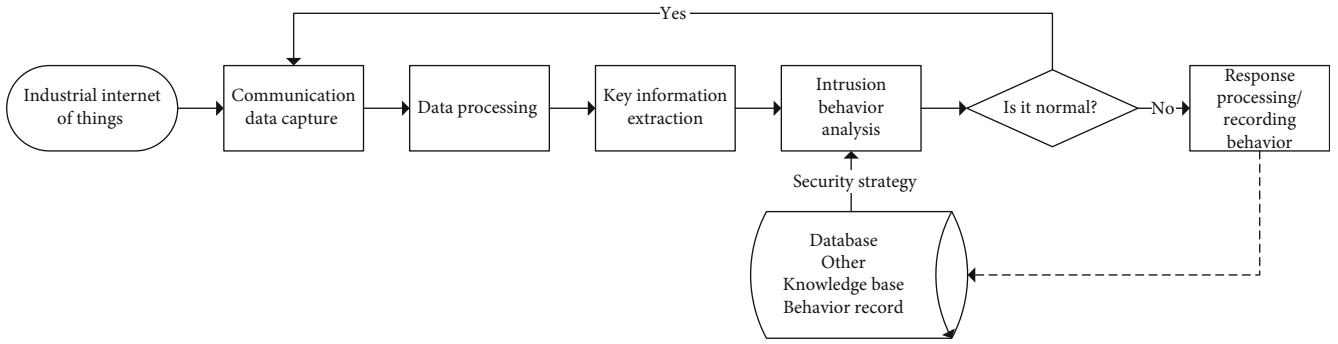

Figure 8: The basic flow of IDS.

In Figure 8, this stage is the core stage of the entire intrusion detection system. The purpose of the system is to detect anomalies or to detect system vulnerabilities or application bugs for intrusion. According to the purpose of the system, it can be divided into abnormal behavior and misuse detection. The report and response phase responds to the judgments made in the previous phase. If it is judged that an intrusion has occurred, the system will take corresponding response measures or notify the management personnel that an intrusion has occurred so that measures can be taken. Recently, people's requirements for intrusion detection and response are increasing, especially for their tracking functions.

2.3.2. IDS Category. According to the data source to classify [29], the standard classification method is the object and detection technology. The general classification is shown in Figure 9. In addition, it can be divided into the centralized type and distributed type according to the model system. The operational mode of the tool can be divided into connection and offline types.

According to the classification of detection technology [30], the IDS can be divided into three types: anomaly detection, misuse detection, and hybrid detection. The principle of anomaly check is to determine whether it is an intrusion by the proportion of network users' daily behaviors and operations to system resources. The working principle of misuse detection is to establish a database through the recorded intrusion behavior. When an access behavior occurs, it is compared with the intrusion behavior recorded in the database to judge the intrusion behavior. Traditional anomaly detection can identify attacks from unknown users.

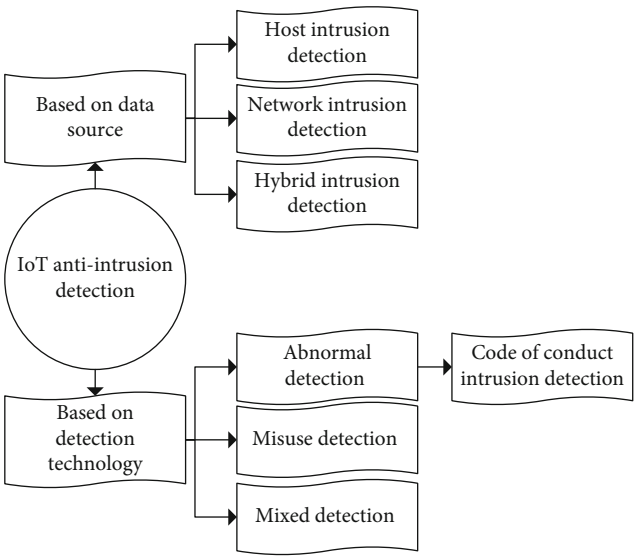

Figure 9: Classification of IDS.

In actual applications, false positives occur from time to time. The detection rate of misuse detection is high, and the false-negative rate is also high. Therefore, a hybrid detection is produced after the two are comprehensively optimized. The frame is shown in Figure 10.

In Figure 10, intrusion detection technology is a technology designed and configured to ensure the security of computer systems that can timely detect and report unauthorized or abnormal phenomena in the system. It is a technology used to detect violations of security policies in computer network technology. In addition to firewalls and antivirus systems, intrusion detection technology has become an effective way to resist hacker attacks and has become the third wave of network security. IDS is primarily used to monitor and analyze user and system activity, identify activity patterns that reflect known attacks, and alert relevant individuals. For abnormal behavior patterns, IDS performs statistical analysis in the form of reports.

2.3.3. Anti-Intrusion Detection Method. In the IIoT-IDS, each connection point instance is taken as a point in the feature space, and the training set T is given as follows:

$$T = \{(X_i, y_i), \cdots, (X_n, y_n)\} \in R^N \times \{-1, 1\}^N. \quad (1)$$

N is the number of connection points of the input space network, (X_i, y_i) is the output feature vector, and the binary variable $y \in \{-1, 1\}$. The hyperplane is defined as shown in the following equation:

$$\omega^T x + b = 0. \quad (2)$$

ω is the hyperplane weight, and b is the bias value. The classification decision function can be obtained through ω and b, as shown in the following equation:

$$f(x) = \text{sign}\left(\omega^T x + b\right). \quad (3)$$

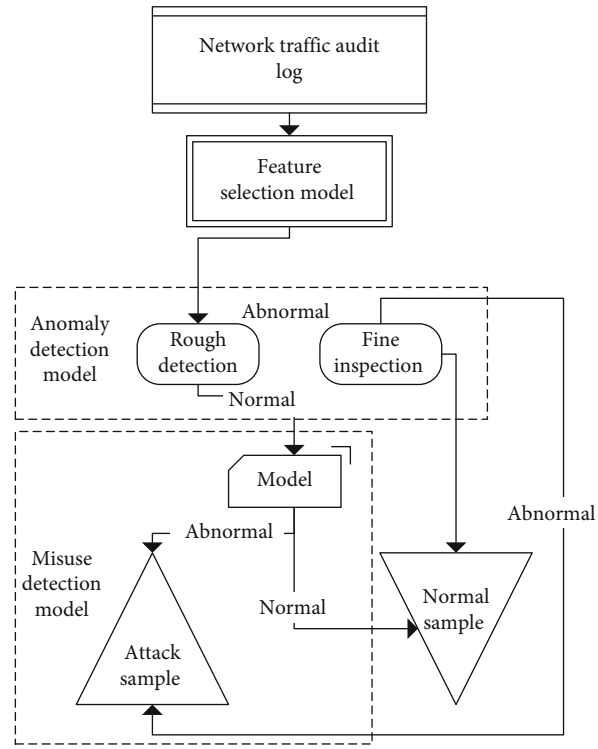

Figure 10: Hybrid anti-intrusion detection structure.

The objective function of the linearly separable constrained optimization problem is shown in the following equation:

$$\begin{aligned} &\min_{\omega,b} \frac{1}{2}\|\omega\|^2 \\ &\text{s.t.} y_i\left(\omega^T x_i + b\right) \geq 1, \quad i = 1, \cdots, N \end{aligned} \quad (4)$$

Lagrange multiplier is introduced, as shown in the following equation [31]:

$$\alpha = (\alpha_1, \cdots, \alpha_n), \quad \alpha \geq 0, i = 1, \cdots, N. \quad (5)$$

Therefore, Equation (6) is obtained:

$$\mathrm{L}(\omega, b, \alpha) = \frac{1}{2}\|\omega\|^2 + \sum_{i=1}^{N} \alpha_i - \sum_{i=1}^{N} \alpha_i y_i\left(\omega^T x_i + b\right). \quad (6)$$

Equation (6) is minimized, and Equation (7) is obtained:

$$\max_{\alpha} \min_{\omega,b} L(\omega, b, \alpha). \quad (7)$$

Therefore, it is necessary to find the minimum value of $\omega, \mathbf{b}$ in L and the maximum value of α, which can further transform the problem of solving the convex quadratic

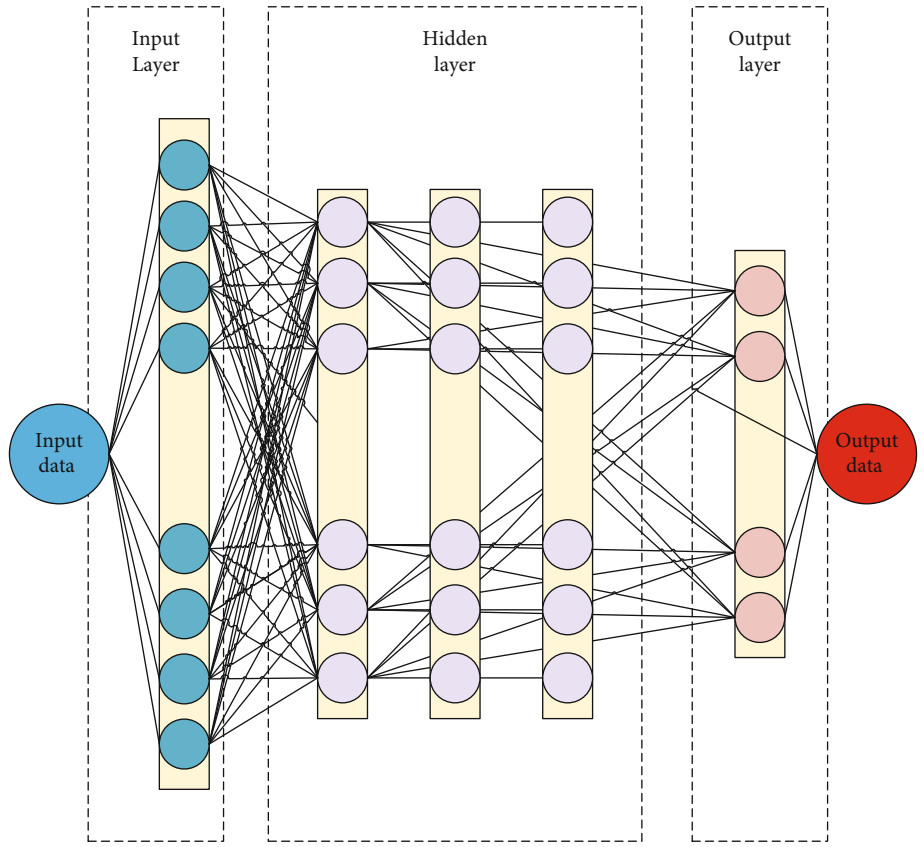

Figure 11: Multilevel structure of the neural network.

programming of the support vector machine (SVM) into a dual problem, such as shown in Equations (8) and (9):

$$\max_{\alpha} \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{i=1}^{N} \alpha_i \alpha_j y_i y_j x_i^T x_j \tag{8}$$

$$\text{s.t.} \sum_{i=1}^{N} \alpha_i y_i = 0, \quad \alpha \geq 0, i = 1, \cdots, N \tag{9}$$

Solving again can get the value of the Lagrange multiplier α_i . Turn to find the optimal hyperplane ω, b. Finally, the hyperplane and the classification decision function are obtained. These are the current mainstream algorithms for solving.

2.3.4. Arrangement of Anti-Intrusion Detection Algorithms Combined with Artificial Neural Networks. The Artificial Neural Network (ANN) is a processing algorithm proposed by research experts inspired by neural signals in human nerves. It can be explained by multilevel sensors [32], and the basic model is shown in Figure 11.

The increase in the number of hidden layers can reduce network error and improve accuracy. Still, it also complicates the network, thereby increasing the training time of the network and the tendency of "overfitting." The design of a neural network should give priority to a 3-layer network. Increasing the number of hidden layer nodes to obtain lower errors makes the training effect easier to achieve than increasing the number of hidden layers. A neural network model without hidden layers is a linear or nonlinear regression. Therefore, the network model without hidden layers is included in the regression analysis. The technology is so mature that it is unnecessary to discuss it in neural network theory. Choosing the number of hidden layer nodes in a neural network is significant. It has a great impact on the performance of the established neural network model and is the direct cause of "overfitting" during training. At present, there is no scientific and universal determination method in theory. The calculation formulas proposed in most literature to determine the number of hidden layer nodes are aimed at arbitrarily many training samples and for the most unfavorable situation. It is difficult to satisfy in general engineering practice and should not be used. The neural network comprises an input layer, a hidden layer, and an output layer. When using an ANN as an IDS, assume that the connection data X of the input network is a $\mathbf{m} \times n$ -dimensional classification sample. Then, the neurons of the input layer are as shown in the following equation:

$$X = \{X_1, X_2, \cdots, X_n\}, \quad X_i \in \{0, 1\}. \tag{10}$$

The hidden layer analyzes whether the input data is an intrusion, and the output layer is responsible for making decisions. For the input neuron X, it is mapped to the hidden layer, as shown in the following equation:

$$H = \{H_1, H_2, \cdots, H_n\}, \quad H_i \in \{0.1\}. \tag{11}$$

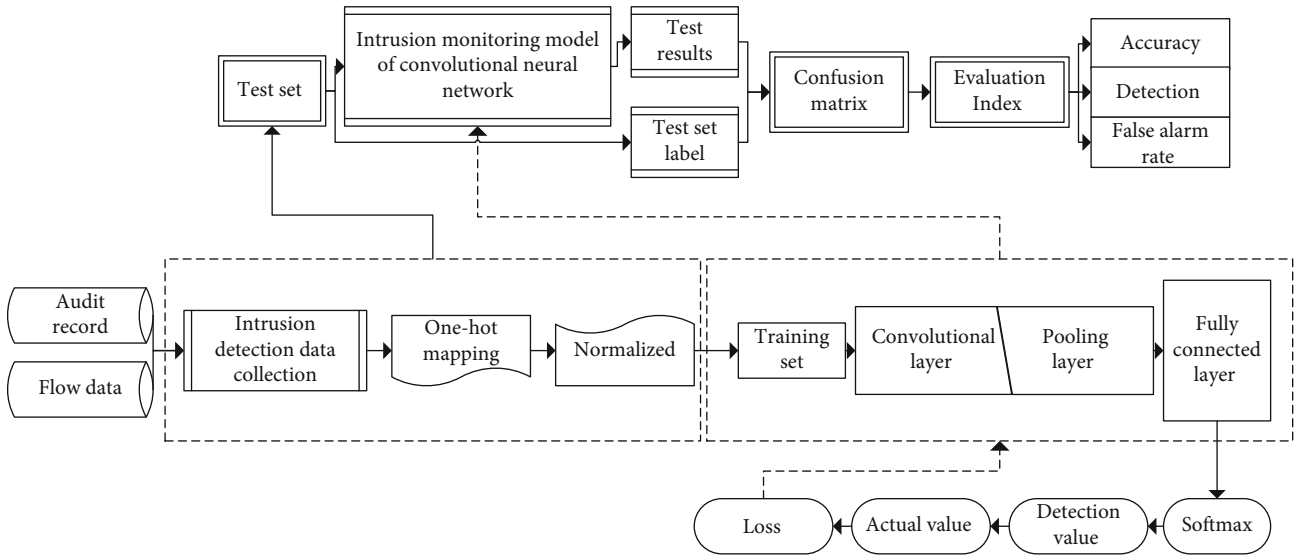

Figure 12: CNN-IIoT anti-intrusion detection model structure.

The output result is as shown in the following equation:

$$H = \sigma(f(x)) = \sigma(W * X_i + b_i). \tag{12}$$

Use the output result of the hidden layer as the input to map to the output layer, as shown in the following equation:

$$Y = \sigma(g(H)) = \sigma\left(W^T * H_i + b_i\right). \tag{13}$$

σ is the nonlinear activation function mapping [33]. An ANN is a representative method of artificial intelligence (AI) in deep learning. Since it was proposed, it has been applied to different scenarios, and many new structures have evolved. Deep learning can efficiently handle high-latitude nonlinear problems and is widely used in many fields. The anti-intrusion detection is a multiclassification problem, and the neural network structure in deep learning is used for research.

2.4. IIoT-IDS by LeNet-5CNN

2.4.1. Basic Structure. In IIoT, devices are always connected to the Internet. Therefore, security protection should be established in IIoT. The autonomy of deep learning is used. The constructed IIoT-IDS model structure is shown in Figure 12, which is used to identify intrusion data.

In Figure 12, intrusion detection is accomplished by performing tasks: (1)monitor and analyze user and system activities; (2) audit system structures and weaknesses; (3) identify patterns of activity that reflect known attacks and alert relevant individuals; (4) statistical analysis of abnormal behavior patterns; (5) evaluate the integrity of important systems and data files; and (6) audit trail management of operating systems, and identify user behaviors that violate security policies.

2.4.2. IIoT Anti-Intrusion Model by LeNet-5. CNN was first proposed in 1990. In 1998, Lecun established a LeNet-5 model for handwritten digit recognition [34], one of CNN's earliest representative models. It contains one input layer, one output layer, two convolutional layers, two pooling layers, and one fully connected layer. The convolutional and pooling layers can be changed to change the structure of the entire network.

Although the LeNet5 network is small, it contains the basic modules of deep learning: convolutional layers, pooling layers, and fully connected layers. This is the basis for other deep learning models. The input image is subjected to the first convolution operation (using six convolution kernels of size $5 * 5$) to obtain 6 C1 feature maps (6 feature maps of size $28 * 28$, $32 - 5 + 1 = 28$). The size of the convolution kernel is $5 * 5$, and there is a total of $6 * (5 * 5 + 1) = 156$ parameters. Among them, +1 means that grain has a bias. For the convolutional layer C1, each pixel in C1 is connected to $5 * 5$ pixels in the input image and one tendency. So there are $156 * 28 * 28 = 122304$ connections in total. There are 122304 connections, but only 156 parameters need to be learned, mainly through weight sharing. The most used LeNet-5 currently has a 7-layer structure, as shown in Figure 13.

Among them, the convolutional layer is the core component of CNN, and there are two primary responsibilities. One uses several convolution kernels to extract data features, and the other uses activation functions to process data results. The input data of the convolution layer comes from the pooling layer, and the obtained data is subjected to the convolution operation. The result is obtained through the corresponding activation function [35]. The process is shown in Equations (14) and (15):

$$x_i^l = f\left(h_j^l\right), \tag{14}$$

$$h_j^l = \sum_{i \in M_j} h_j^{l-1} \otimes W_{ij}^l + b_j^l. \tag{15}$$

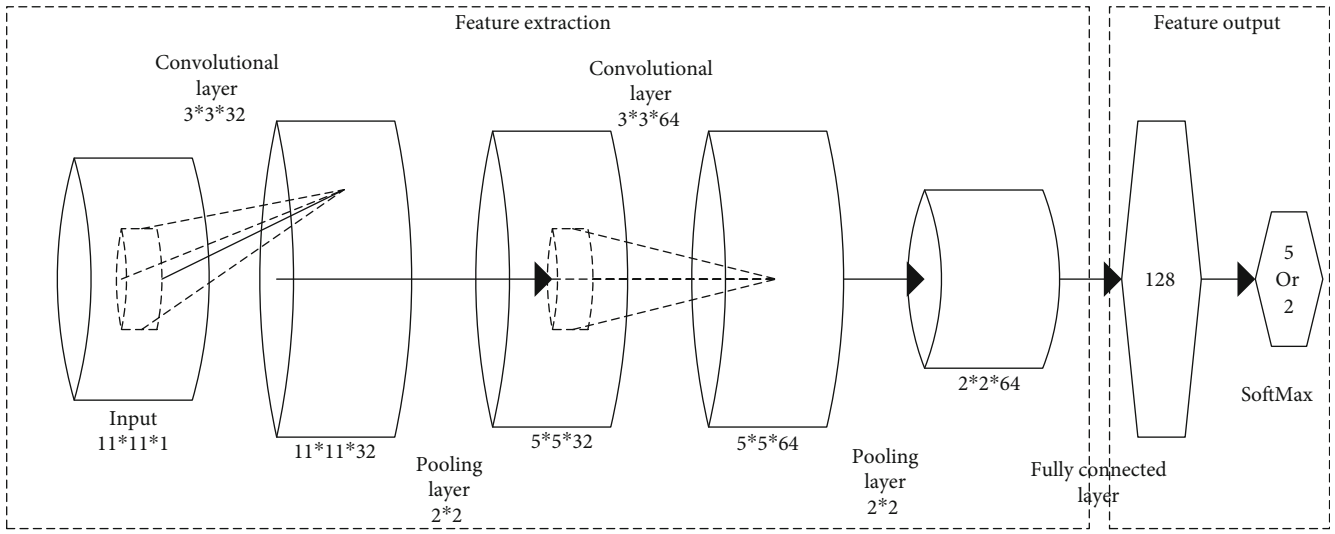

Figure 13: The basic structure of LeNet-5 networks.

h_j^l is the activation output of the jth nerve in the lth layer, h_j^{l-1} represents the ith two-dimensional output matrix of the $l-1$ layer, W_{ij}^l is the convolution kernel, $\otimes$ is the convolution operation, and b_j^l is the bias value.

After the convolution calculation, the dimensionality of the data is still very high. A pooling operation is needed. The data output by the convolution is sampled and compressed to reduce the feature dimensionality, as shown in the following equation:

$$h_j^l = \beta_j^l \text{upsample}\left(x_i^{l-1}\right) + b_j^l. \tag{16}$$

x_i^{l-1} is the output feature of the upper layer, β_j^l is the pooling coefficient, and upsample is the pooling function.

The fully connected layer changes the pooled two-dimensional data features into one-dimensional data features, like multilayer sensors, such as Equations (17) and (18):

$$x_j^l = f\left(h_j^l\right), \tag{17}$$

$$h_j^l = \sum_{i \in M_j} x_i^{l-1} * W_{ij}^l + b_j^l. \tag{18}$$

CNN is divided into two stages for training. One is forward propagation, and the other is reverse fine-tuning. The overall training process is shown in Figure 14.

The main steps and content are shown in Table 2.

This part is aimed at protecting data and preventing breaches in the network. Any exploitation of malware can cause a lot of damage to the company. Safely maintaining a network is the goal of all system administrators. Here, there are several important open source network intrusion detection tools. In today's world, data breaches, threats, attacks, and intrusions are becoming very sophisticated. Cybercriminals and hackers have come up with new ways to gain access to business and home networks, making a multilayered approach to cybersecurity an urgent need. Therefore, the intrusion detection system is the most important tool used to defend the network from the high-tech attacks that occur on a daily basis. IDSs are network security tools used to detect exploits against targeted applications or computers. It is considered a high-end network device or software application that assists network or system administrators to monitor various malicious activities or threats in the network or system. A security information and event management system is used to report any unusual activity to administrators.

In Figure 14, the convolutional network is essentially an input-to-output mapping. It can learn a large number of mapping relationships between input and output without any precise mathematical expression between input and output. As long as the convolutional network is trained with known patterns, the network has input and output pairs. Convolutional networks perform supervised training, so their sample set consists of pairs of input vectors and ideal output vectors. All of these vector pairs should be derived from the actual "running" results of the system that the network is about to simulate. They can be collected from the actual operating system. Before starting training, all weights should be initialized with some different small random numbers. "Small random numbers" can be used to ensure that the network does not saturate due to too large weights, resulting in training failure. "Different" can be used to ensure that the network can learn properly. In fact, if the weight matrix is initialized with the same number, the network cannot learn.

2.4.3. Improved LeNet-5 Model. The traditional activation functions are saturated nonlinear, sigmoid, and tanh. A saturated nonlinear function will take longer to converge than a nonsaturated nonlinear function ReLU model. For large datasets, a faster learning process means more time savings.

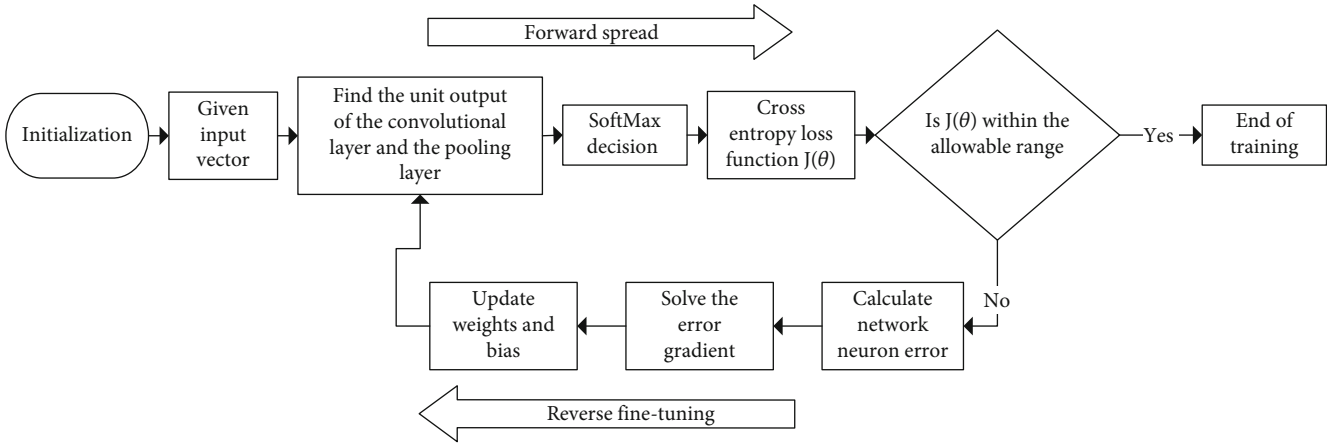

Figure 14: The training process of CNN.

Table 2: Training process steps.

Step number	Step content
Step 1	Initialize network weights
Step 2	Input data through convolutional layer, sampling layer, and fully connected layer to get the output value
Step 3	Use the crossentropy function to compare the error between the output value and the target value
Step 4	If the error is greater than the actual value, input the error into the network and calculate the total error
Step 5	Update according to the error; repeat the second item

In addition, ReLU also introduces a certain sparsity. In the category of feature representation, the data has a certain sparsity. Some of the data is redundant. This sparsity can be simulated to preserve the characteristics of the data in a maximum approximation manner by introducing ReLU. In addition, the data collected by the LeNet-5 network also has the shortcomings of too light fitting degree and single response mode. Standard LeNet-5 networks are flawed. When convolutional layers are used for data feature extraction, and pooling layers are used for dimensionality reduction, data features become sparse. The data processing by the two-layer convolutional layer of the LeNet-5 network model will cause incomplete data extraction. The characteristic information of the data will be lost when the subsequent pooling layer of the convolutional layer processes the data.

The feature information of anti-intrusion detection data is unevenly distributed. The feature attributes of some data have a more significant impact on the recognition of detection results during network model processing. Part of the attribute feature information contains a small amount of data, which will cause the phenomenon that the data feature has nothing to do with intrusion behavior. When processing these data in the convolutional and pooling layers, it will cause a waste of redundant resources, which will interfere with the detection of intrusion behavior. In LeNet-5's anti-intrusion detection, the input data is different from the original image data because the convolutional layer and the pooling layer are alternately used. One-dimensional data mapping will become blurred after two-dimensional space, making the entire model unable to describe the characteristic behavior accurately, and the model's anti-intrusion performance is not ideal. Therefore, the traditional LeNet-5 [36] model will be optimized. The two convolutional layers are subjected to a pooling operation, and suitable parameters are used to extract the abnormal features of the data fully. The optimized model is the LeNet-7 model, and the structure is shown in Figure 15. There are four convolutional layers in the improved LeNet-7 network, two pooling layers, and one fully connected layer.

In Figure 15, as the depth of the network increases, the accuracy of the network should increase synchronously, and the overfitting problem needs to be paid attention to. But one problem with increasing network depth is that these added layers signal parameter updates. The gradient is propagated from the back to the front. After increasing the depth of the network, the gradient of the earlier layers will be very small, which means that the learning of these layers is basically stagnant. This is the vanishing gradient problem. The second problem with deep networks is training. When the network is deeper means the parameter space is larger and the optimization problem becomes harder. Therefore, simply increasing the network depth leads to higher training errors. Although the deep network converges, the network begins to degenerate; that is, increasing the number of network layers leads to greater errors.

2.5. IIoT-IDS by Inception-CNN. The improved LeNet-7 is improved compared to LeNet-5, but it is not enough to process the complex data in IIoT. The Inception network in the field of deep learning combined with CNN is used; the IIoT-IDS is established.

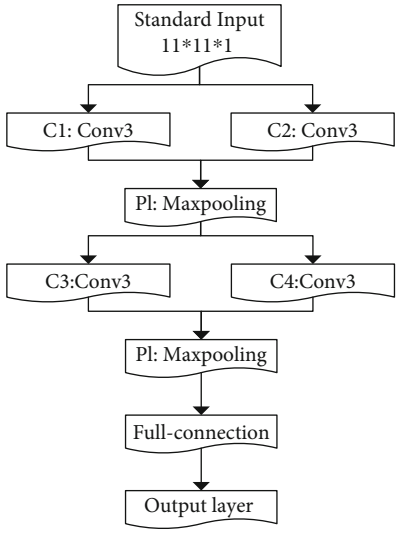

Figure 15: Improved LeNet-7 model structure diagram.

2.5.1. Inception Network. To specifically solve the severe high-energy problem caused by the parameter hierarchy in the neural network, people have proposed deep learning combined with the CNN Inception network [37].

There are currently 4 Inception networks, of which Inception V4 can be combined with residual connections to build a deeper Inception-ResNet network. The Inception network can sparse the network structure and produce dense data. Multiple channels and multiple levels can be set in the network, and various convolution kernels and pooling can be used to operate. The basic structure of Inception is shown in Figure 16.

In order to increase the nonlinear model and reduce the parameter settings, the Inception model is expanded. The calculation amount of the model is increased, its structure is modified, the amount of convolution parameters is reduced, and the network nonlinearity is appropriately deepened. Combining different channels can extract more data features.

2.5.2. The Detection Method of Inception-CNN. The modified pooling method can scale and move data features undistorted. And it can reduce the load on the network. Therefore, an adaptive pooling algorithm is proposed. It can assign pooling weights to the dynamic elements of different pooling cores and more comprehensively express data characteristics, as shown in Equations (19) and (20):

$$S_{ij} = \mu_{ij} \max_{i=1,j=1}^{c} \left(F_{ij}\right) + b, \tag{19}$$

$$\mu_{ij} = \frac{2}{c^2\left(1 + e^{-\left(F_{ij}/F_{\text{sum}}\right)\sigma^2}\right)}. \tag{20}$$

μ_{ij} is the pooling factor, F_{sum} is the total element of the pooling core, and σ is the standard deviation. This algorithm can overcome the limitation of maximum pooling and obtain more accurate feature information.

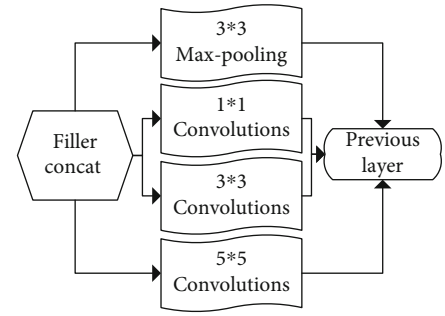

Figure 16: The basic structure of Inception.

2.5.3. IIoT-IDS Solution by Inception-CNN. Integrating the detection method of Inception and the improved LeNet-7 network, the model flow chart of the built Inception-CNN IIoT-IDS and the training structure of the model are shown in Figure 17.

Data preprocessing: the data used here comes from the MNIST dataset, and the mobile network data in the dataset is screened. Then, the information is normalized. Because the dimensionality of the original data is high, it must be reduced. Data with greater influence on the result is selected, and no influence data is removed. After that, the abnormal data part is adaptively manipulated. The detection algorithm flow of this model is shown in Table 3.

Model training: the data obtained by preprocessing is converted into a two-dimensional format to adapt it to the CNN format. Extract rich and diverse characteristics of intrusion behavior; adjust parameters until convergence.

Data output: after completing the training, use the test set to evaluate the model's performance. If it meets the requirements, stop training. Otherwise, repeat the above steps to check the accuracy of the model.

2.5.4. The Limitations of the Anti-Intrusion Detection Algorithm of the Inception-CNN Network. At present, IDS technology is still regarded as a state that has not been fully completed. From a technological point of view, the technology does have some shortcomings and distances. People expect the functionality that IDS brings, but there are still bottlenecks that cannot be fully overcome in current commercial IDS suites. The amount of information generated by IDS is excessive, but the skills and ability to effectively filter, sift, and correlate data are lacking. Although IDS can bring various advantages, it should be emphasized here that the establishment of IDS is not foolproof for enterprises to strengthen information security. Before enterprises have mature basic concepts and processing procedures for information security, they will face more difficulties when building an IDS. IDS detects attack events based on the characteristic data of intrusion attacks rather than the way of using behavior. Therefore, intrusion detection is limited to predefined system events. In addition, the management console cannot effectively manage an unlimited number of monitoring devices, nor does it support intercorrelation of data from multiple different information sources. Currently, most of the data-related returns provided by IDS are based

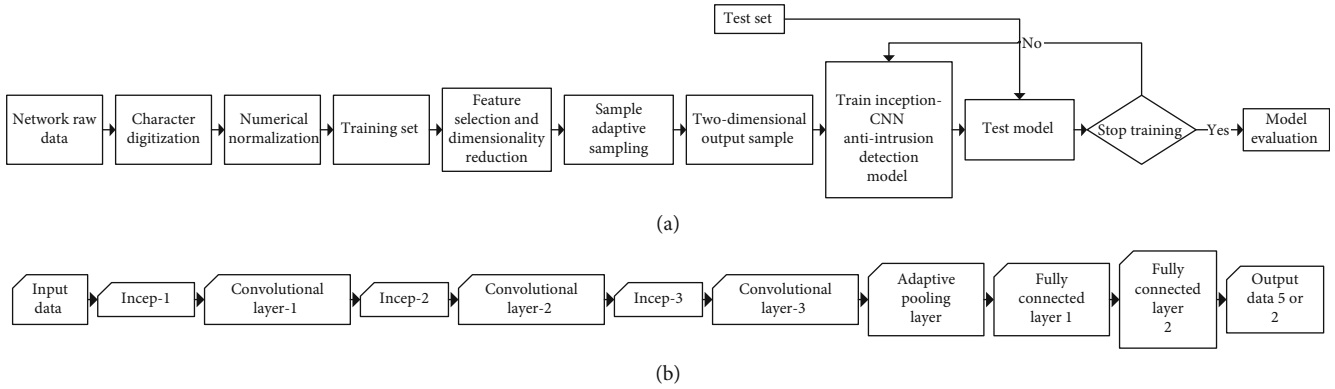

Figure 17: Inception-CNN IIoT-IDS structure diagram. (a) Shows the detection flow chart of the entire system. (b) Shows the model training structure diagram.

Table 3: The process of the anti-intrusion detection algorithm of Inception-CNN.

Number	Content
1	Lookup packet netDevice = pcap_lookupdev(errbuf)
2	Create capture criteria p = pcap_open_live(netDevice, 3000, 1, 440, errbuf)
3	Set filter conditions pcap_compile(p, &fcode, filter_ string, 0, netmask)
4	Enter loop condition while((ptr = (char ∗)(pcap_next(p, &hdr))) = NULL)
5	Format the captured data eth = (struct libnet_ethernet_ hdr ∗)ptr
6	Close the capture standard and initialize the signal processing function pcap_close if(eth->ether_type = ntohs(ETHERTYPE_ARP))
7	End

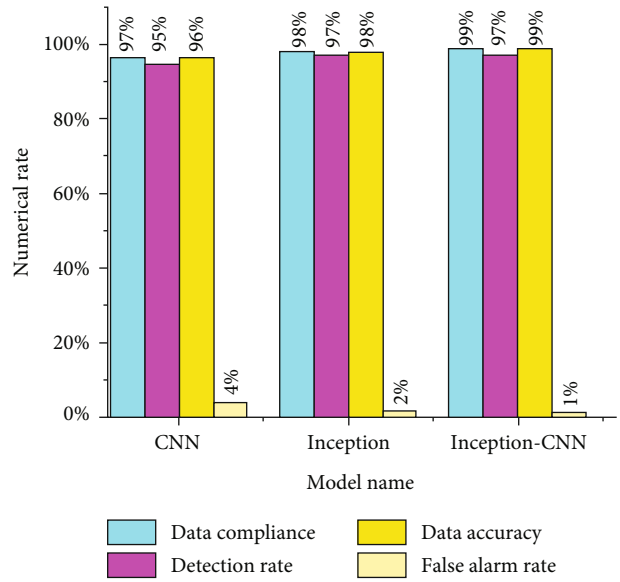

Figure 18: Comparison of the performance values of the three networks.

on predesigned templates. Such reward schemes are helpful, but limited.

3. Results

3.1. Inception-CNN IIoT Anti-Intrusion Detection Model Performance Test. The three performances of a single CNN, a traditional Inception network, and an improved Inception-CNN network are tested, and the performance of the three models is compared. This proves the applicability of the established Inception-CNN model, and the result is shown in Figure 18.

In Figure 11, the data accuracy rate of the improved Inception-CNN model is 99%, the detection rate is 97%, the data accuracy rate is 99%, and the data false alarm rate is only 1%. This shows that its performance is entirely beyond the other two traditional models. This model has a high autonomous learning ability and can adapt to network data monitoring in a complex environment. Network security requires the management of a multilayered system. The goal of cybersecurity is to protect the integrity of core assets, minimize possible losses, maximize return on investment, and ensure business continuity. The occurrence of network intrusion has increased people's management of network security. This can help users establish a dynamic defense-in-depth system and grasp network security as a whole and is also the development direction of network security.

3.2. Inception-CNN IIoT Anti-Intrusion Detection Model Performance Change Trend. After the improvement, the Inception-CNN model is better than the traditional two monitoring models. It is necessary to analyze the accuracy of the data and the trend of the loss value to determine whether the model's high performance is accidental. The test and training set are analyzed uniformly, and the result is shown in Figure 19.

In Figure 19, the data accuracy of the improved Inception-CNN model and the training set test set can maintain a gradual upward trend and finally stabilize. At the beginning of the test, the loss value of the data is more significant than one in the training set of the test set. As the experiment progresses, the loss value gradually decreases,

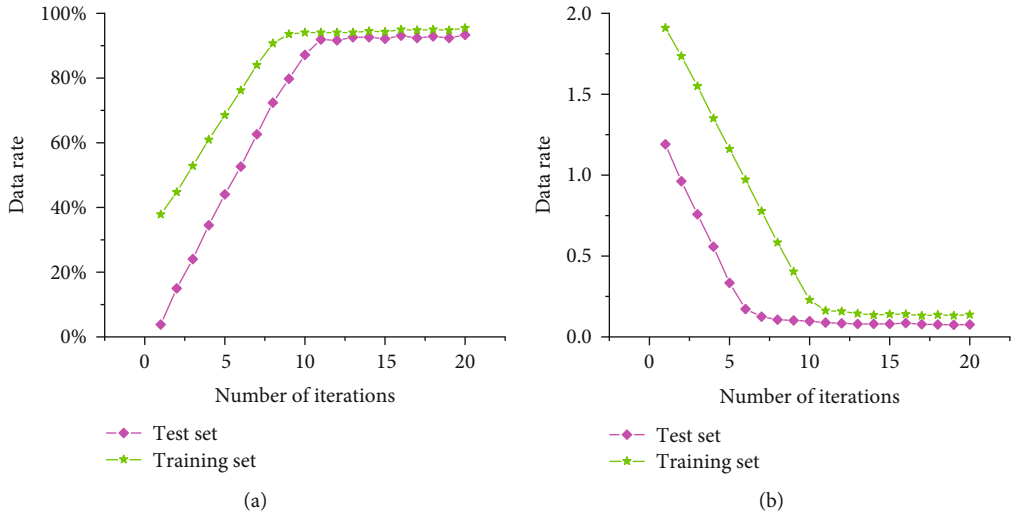

Figure 19: Inception-CNN model accuracy and loss value change trend. (a) Shows the accuracy change curve of the training set test set. (b) Shows the loss value change curve of the training set test set.

Table 4: Comparison of research methods.

Method comparison	Lenet-7	A privacy-aware task offloading method
Main technology used	Neural networks	Cloud computing
Preprocessing technology	Neural network pooling layer	Gan training
Type of data	Network intrusion data	Network intrusion data
Evaluation measures	Detection accuracy and loss values	Benchmark performance experiments
Advantage	High detection accuracy and small loss value	Low network load
Shortcoming	Unable to detect in a complex network environment	Vulnerable to leaks when targeting multiple targets

approaches 0, and remains stable. These two result curves show that the improved Inception-CNN model has good stability, and the high accuracy and high precision are not due to accidental factors. Therefore, the model can be applied to the actual IIoT-IDS. The network environment is also becoming more and more complex. Various complex devices need to be constantly upgraded and patched, which makes the work of network administrators continue to increase. The negligence of network administrators may cause major security risks. Therefore, the intrusion detection system has become a new hot spot in the security market, not only attracting more and more attention but also beginning to play its key role in various environments.

4. Discussion

Starting with the security of the IIoT, the requirements for security performance are learned from the literature. The structure system of IIoT is introduced, and the corresponding security protection technology is analyzed. The IDS of IIoT is built based on the Inception network and the convolutional neural LeNet-5 network in deep learning. The LeNet-5 network is modified according to actual requirements. A new LeNet-7 network structure is constructed. IDS has the advantages of high accuracy, high data accuracy, high detection, and low false-positive rate. This kind of system has high detection accuracy for single intrusion behavior of simple data. However, the established LeNet-7 detection network system has insufficient detection ability for larger databases. Secondly, the detection performance in a specific complex network environment will be affected by various objective factors, which will lead to the degradation of the detection performance. Xu et al. developed a privacy-aware task offloading method. Firstly, the strength Pareto evolutionary algorithm is well studied and improved to obtain offloading strategies that synergistically improve training performance and privacy protection [38]. A comparison of the method with the method used is shown in Table 4.

Then, the most balanced offloading policy is trained. Finally, systematic experiments show that the method achieves the best performance among other representative benchmark methods. The new network technology proposes a privacy protection model, which can demonstrate the security of using the technology, the importance of privacy protection, and the necessity of using new technologies for privacy protection research.

5. Conclusion

With the development of information technology and industrial technology, IIoT takes up an increasing proportion of

manufacturing, which provides excellent convenience for industrial control and inspection. However, the hidden dangers of IIoT that threaten private data and security have also increased. In recent years, network data breaches have emerged one after another. The design of security and anti-intrusion systems for IIoT has also become the endpoint of research. Starting from the safety of IIoT, the security performance requirements are learned from the literature. The structural system of IIoT is introduced. The corresponding security protection technology is analyzed. By the Inception network and the convolutional neural LeNet-5 network in the field of deep learning, an IDS for IIoT has been established. According to actual requirements, the LeNet-5 network is improved, and the new LeNet-7 network structure is built. Integrating Inception, LeNet-5, and LeNet-7 technologies, the Inception-CNN IIoT IDS is established, and its performance is tested. Experimental results show that this model has the advantages of high accuracy, high data accuracy, high detection, and low false alarm rate. Therefore, this model can be used in IIoT data privacy protection work. However, the research here is only tested in a single network environment, not used in large-scale industrial processes, nor has the model been validated multiple times in a more complex, multi-interaction network environment. In addition, Nascita et al. [39] conducted research on AI techniques for mobile traffic classification by understanding and improving multimodal deep learning architectures. AI-based techniques investigate trustworthiness and interpretability, and the behavior of state-of-the-art multimodal deep learning traffic classifiers is explained and improved. The research has important reference value for the reform of network traffic patterns. However, this study is not very representative. Afterwards, the performance of the built model in the actual IIoT will be verified.

Data Availability

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest

The author declares that there is no conflict of interest.

References

[1] S. Al-Janabi, A. F. Alkaim, and Z. Adel, "An innovative synthesis of deep learning techniques (DCapsNet & DCOM) for generation electrical renewable energy from wind energy," *Soft Computing*, vol. 24, no. 14, pp. 10943–10962, 2020.

[2] A. Hallsby, "Psychoanalysis against WikiLeaks: resisting the demand for transparency," *Review of Communication*, vol. 20, no. 1, pp. 69–86, 2020.

[3] S. Al-Janabi and A. F. Alkaim, "A nifty collaborative analysis to predicting a novel tool (DRFLLS) for missing values estimation," *Soft Computing*, vol. 24, no. 1, pp. 555–569, 2020.

[4] C. Makridis and B. Dean, "Measuring the economic effects of data breaches on firm outcomes: challenges and opportunities," *Journal of Economic and Social Measurement*, vol. 43, no. 1-2, pp. 59–83, 2018.

[5] D. Khubalkar, "Data protection and privacy in cyberspace-national and international perspective," *Psychology and Education Journal*, vol. 57, no. 9, pp. 5243–5246, 2020.

[6] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial internet of things," *China Communications*, vol. 17, no. 1, pp. 73–88, 2020.

[7] H. W. Wei, "MAGAN: a masked autoencoder generative adversarial network for processing missing IoT sequence data," *Pattern Recognition Letters*, vol. 138, pp. 211–216, 2020.

[8] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE Access*, vol. 6, pp. 15941–15957, 2018.

[9] T. D. Diwan, "An experimental analysis of security vulnerabilities in industrial internet of things services," *Information Technology in Industry*, vol. 9, no. 3, pp. 592–598, 2020.

[10] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet of Things*, vol. 14, article 100112, 2021.

[11] F. Wei, P. Vijayakumar, N. Kumar, R. Zhang, and Q. Cheng, "Privacy-preserving implicit authentication protocol using cosine similarity for Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5599–5606, 2021.

[12] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persicoand, and A. Pescapé, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–7, New York, 2020.

[13] M. Hadipour, J. F. Derakhshandeh, and M. A. Shiran, "An experimental setup of multi-intelligent control system (MICS) of water management using the Internet of Things (IoT)," *ISA Transactions*, vol. 96, pp. 309–326, 2020.

[14] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers & Electrical Engineering*, vol. 81, article 106522, 2020.

[15] H. Naeem, F. Ullah, M. R. Naeem et al., "Malware detection in industrial internet of things based on hybrid image visualization and deep learning model," *Ad Hoc Networks*, vol. 105, article 102154, 2020.

[16] W. Chen, "Intelligent manufacturing production line data monitoring system for industrial internet of things," *Computer Communications*, vol. 151, pp. 31–41, 2020.

[17] S. Al-Janabi, A. Alkaim, E. Al-Janabi, A. Aljeboree, and M. Mustafa, "Intelligent forecaster of concentrations ($PM_{2.5}$, PM_{10}, NO_2, CO, O_3, SO_2) caused air pollution (IFCsAP)," *Neural Computing and Applications*, vol. 33, no. 21, pp. 14199–14229, 2021.

[18] S. Al-Janabi and A. Alkaim, "A novel optimization algorithm (Lion-AYAD) to find optimal DNA protein synthesis," *Egyptian Informatics Journal*, vol. 12, 2022.

[19] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[20] D. Zhang, C. C. Chan, and G. Y. Zhou, "Enabling industrial internet of things (IIoT) towards an emerging smart energy system," *Global Energy Interconnection*, vol. 1, no. 1, pp. 39–47, 2018.

[21] X. Huang, "Intelligent remote monitoring and manufacturing system of production line based on industrial Internet of Things," *Computer Communications*, vol. 150, pp. 421–428, 2020.

[22] S. Al-Janabi, A. Patel, H. Fatlawi, K. Kalajdzic, and I. Al Shourbaji, "Empirical rapid and accurate prediction model for data mining tasks in cloud computing environments," in *2014 international congress on technology, communication and knowledge (ICTCK)*, pp. 1–8, Mashhad, 2014.

[23] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[24] K. A. Abuhasel and M. A. Khan, "A secure Industrial Internet of Things (IIoT) framework for resource management in smart manufacturing," *IEEE Access*, vol. 8, pp. 117354–117364, 2020.

[25] S. Hussin, A. Alguttar, K. Alashik, and R. Yildirim, "An observation of intrusion detection techniques in cyber physical systems," *Avrupa Bilim ve Teknoloji Dergisi*, vol. 34, pp. 277–284, 2020.

[26] M. A. Mahdi and S. Al_Janabi, "A novel software to improve healthcare base on predictive analytics and mobile services for cloud data centers," in *Big Data and Networks Technologies. BDNT 2019*, Y. Farhaoui, Ed., vol. 81 of Lecture Notes in Networks and Systems, pp. 320–339, Springer, Cham, 2019.

[27] P. Wang, M. Zhou, and Z. Ding, "A two-layer IP hopping-based moving target defense approach to enhancing the security of mobile ad-hoc networks," *Sensors*, vol. 21, no. 7, p. 2355, 2021.

[28] S. He, W. Ren, T. Zhu, and K.-K. R. Choo, "BoSMoS: a blockchain-based status monitoring system for defending against unauthorized software updating in Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 948–959, 2020.

[29] M. A. Sulaiman, "Evaluating data mining classification methods performance in Internet of Things applications," *Journal of Soft Computing and Data Mining*, vol. 1, no. 2, pp. 11–25, 2020.

[30] L. Fu, W. Zhang, X. Tan, and H. Zhu, "An algorithm for detection of traffic attribute exceptions based on cluster algorithm in industrial Internet of Things," *IEEE Access*, vol. 9, pp. 53370–53378, 2021.

[31] E. Baraneetharan, "Role of machine learning algorithms intrusion detection in WSNs: a survey," *Journal of Information Technology*, vol. 2, no. 3, pp. 161–173, 2020.

[32] X. Li, J. Shu, W. Gu, and L. Gao, "Deep neural network for plasmonic sensor modeling," *Optical Materials Express*, vol. 9, no. 9, pp. 3857–3862, 2019.

[33] L. Xiao, K. Li, Z. Tan et al., "Nonlinear gradient neural network for solving system of linear equations," *Information Processing Letters*, vol. 142, pp. 35–40, 2019.

[34] T. Saleem and M. Chishti, "Assessing the efficacy of logistic regression, multilayer perceptron, and convolutional neural network for handwritten digit recognition," *International Journal of Computing and Digital Systems*, vol. 9, no. 2, pp. 299–308, 2020.

[35] H. Zhu, H. Zeng, J. Liu, and X. Zhang, "Logish: a new nonlinear nonmonotonic activation function for convolutional neural network," *Neurocomputing*, vol. 458, pp. 490–499, 2021.

[36] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," *IEEE Access*, vol. 7, pp. 64366–64374, 2019.

[37] J. Kim, J. Moon, E. Hwang, and P. Kang, "Recurrent inception convolution neural network for multi short-term load forecasting," *Energy and Buildings*, vol. 194, pp. 328–341, 2019.

[38] X. Xu, X. Liu, X. Yin, S. Wang, Q. Qi, and L. Qi, "Privacy-aware offloading for training tasks of generative adversarial network in edge computing," *Information Sciences*, vol. 532, pp. 1–15, 2020.

[39] A. Nascita, A. Montieri, G. Aceto, D. Ciuonzo, V. Persicoand, and A. Pescapé, "XAI meets mobile traffic classification: understanding and improving multimodal deep learning architectures," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4225–4246, 2021.