Computers, Materials & Continua
DOI: 10.32604/cmc.2023.035077
Article

Tech Science Press

Check for updates

Internet of Things Intrusion Detection System Based on Convolutional Neural Network

Jie Yin[1,2,3,*], Yuxuan Shi[1], Wen Deng[1], Chang Yin[1], Tiannan Wang[1], Yuchen Song[1], Tianyao Li[1] and Yicheng Li[1]

[1]Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China
[2]Engineering Research Center of Electronic Data Forensics Analysis, Nanjing, China
[3]Key Laboratory of Digital Forensics, Department of Public Security of Jiangsu Province, Nanjing, China
*Corresponding Author: Jie Yin. Email: yinjiejspi@163.com
Received: 06 August 2022; Accepted: 08 December 2022

Abstract: In recent years, the Internet of Things (IoT) technology has developed by leaps and bounds. However, the large and heterogeneous network structure of IoT brings high management costs. In particular, the low cost of IoT devices exposes them to more serious security concerns. First, a convolutional neural network intrusion detection system for IoT devices is proposed. After cleaning and preprocessing the NSL-KDD dataset, this paper uses feature engineering methods to select appropriate features. Then, based on the combination of DCNN and machine learning, this paper designs a cloud-based loss function, which adopts a regularization method to prevent overfitting. The model consists of one input layer, two convolutional layers, two pooling layers and three fully connected layers and one output layer. Finally, a framework that can fully consider the user's privacy protection is proposed. The framework can only exchange model parameters or intermediate results without exchanging local individuals or sample data. This paper further builds a global model based on virtual fusion data, so as to achieve a balance between data privacy protection and data sharing computing. The performance indicators such as accuracy, precision, recall, F1 score, and AUC of the model are verified by simulation. The results show that the model is helpful in solving the problem that the IoT intrusion detection system cannot achieve high precision and low cost at the same time.

Keywords: Internet of things; intrusion detection system; convolutional neural network; federated learning

1 Introduction

Mobile Edge Computing (MEC) is essentially the relationship between edge computing and mobile technology in the broadest sense which means applications in mobile or telemedicine, Internet of Things, virtual reality, intelligent connected cars and other scenarios [1,2]. With the wide applications of its technology, IoT involves a large number of interconnected devices, including public

facilities, wearable devices and drones, etc. It brings a lot of convenience to our life, however, its security issues are also prominent. The environment of the IoT network is very complex, and the huge scale of the network makes it very difficult to manage [3,4]. IoT devices facing security vulnerabilities are more easily attacked than traditional networks.

In recent years, IoT security issues have occured frequently and eventually caused widespread concern in the academic community. Many countries have proposed corresponding industry norms, laws, and regulations. For example, China has released the "Internet of things—Reference architecture" [5], "Information Security Technology IoT Security Reference Model and General Requirements" [6], and the United States has released the "2017 IoT Cybersecurity Improvement Act" [7]. In 1980, James P. Anderson in "Computer Security Threat Monitoring and Surveillance" [8] firstly detailed the concept of intrusion detection and proposed the classification of computer system threats and the use of audit trail data, and the idea of monitoring intrusion activities. From 1984 to 1986, Dorothy Denning et al. at Georgetown University developed a real-time Intrusion Detection Systems (IDS) model. After 1988, the United States carried out research on Distributed Intrusion Detection Systems (DIDS) by integrating host-based and web-based IDS. DIDS was a milestone in the history of distributed intrusion detection systems. In 1990, L.T. Heberlein of the University of California and others developed Network Security Monitor (NSM). First, it directly uses network flow as the source of audit data. This allows monitoring of heterogeneous hosts without the need to convert audit data to web pages in a uniform format. So far, the history of intrusion detection systems has turned into a new page. Two camps have been formally formed, namely network-based IDS and host-based IDS. From the 1990s to the present, the development of intrusion detection systems has shown even more prosperous situations and has made great progress in intelligence and distribution [9].

The concept of IoT security has been in the hot zone of research since it was mentioned at the European IoT Conference [10] in 2008, and on December 1, 2008, Henan Hanwei Electronics Company [11] first added the concept of IoT to its own safety production monitoring and management information system to apply IoT in use of production safety. In 2009, Rolf [12] proposed the security and privacy issues of IoT itself in their paper for the first time, which set off a wave of research in IoT security. At present, IoT security is mostly integrated with blockchain technology. For example, Zhao et al. [13] and others use blockchain technology in IoT electric power supply industry to enhance security of the production. However, due to the immaturity of blockchain technology itself and its unfriendliness of data storage [14], it is not a good solution to the security of IoT devices such as smart audio that store a lot of personal privacy information. And because IoT technology is still an emerging high-end technology, its compatibility with home IoT devices such as smart audio and smart cameras also needs to be examined.

This paper selects NSL-KDD as the base dataset, which is collected, processed and verified by tools such as Wire Shark. After centrally computing and processing the dataset using standardized methods such as feature engineering, a cloud-based loss function is designed. The model consists of one input layer, two convolutional layers, two pooling layers and three fully connected layers and one output layer. Finally, the detection accuracy is compared with Long Short Term Memory (LSTM) and Recurrent Neural Network (RNN) models. This paper achieves a balance between cost and accuracy based on packet capture analysis, Convolutional Neural Network (CNN), federated learning and machine learning.

The innovations of this paper are summarized as follows:

- A CNN intrusion detection system for IoT devices is proposed. First, the NSL-KDD dataset is cleaned and preprocessed. Then, feature engineering methods are used to select appropriate features. Finally, the safety problems of IoT system are identified with CNN.
- A loss function based on clouds is designed. It includes one input layer, two convolutions, two pool layers and three full connection layers with one output layer. Regularization methods are adopted to prevent overfitting.
- An improved mobile edge computing solution is proposed. Federated learning technology is used to solve the problems of distributed computing capability and privacy protection.

The next step of this article is as follows. The second part introduces the relevant work in this field. The third part is data set selection and preprocessing. The fourth part introduces the framework and method of the Internet of Things intrusion detection system based on CNN. The fifth and sixth parts are simulation and summary respectively.

2 Related Work

Few of the current intrusion detection systems are based on the IoT technology. As an extension of Internet, the IoT has been widely used in daily life and its complexity makes it vulnerable to attack which thus necessitates an appropriate intrusion detection system.

Metongnon et al. [15] proposed a metric study against these protocols or attacks based on the problem. The study shows that there are many devices in the IoT that only have default credentials and some even lack proper security protocols resulting in providing only inadequate security. Demetriou et al. [16] proposed a new technique called HanGuard to control the communication between IoT devices and their applications in a unified and backward compatible way by observing the statistics of smart home systems that authenticate other devices through WIFI routers. Derhab et al. [17] proposed a novel intrusion detection system based on the study of the security of commands against forged and misdirected commands in the industrial IoT. This system addresses the problem of increasingly sophisticated network attacks on industrial control systems.Vinayakumar et al. [18] developed a highly scalable intrusion detection system based on the deep neural networks called Scale-hybrid-IDS-Alert Net, which effectively monitors network traffic in real time. This system also detects and classifies different types of network attacks so as to warn them of possible network attacks in advance. Lueckenga et al. [19] proposed a generic weight calculation function as well as a generic weight calculation function in order to improve the detection performance of anomaly intrusion detection system. The proposed function solves the problem of poor intrusion detection in smart grid detection systems.

In 2020, Tama et al. [20] proposed an eXtreme Gradient Boosting-Random Forest (XGBoost-RF) model for IoT intrusion detection, which divides intrusion detection into feature selection phase and classification phase. The features of NSL-KDD dataset are performed for feature importance analysis in the first phase. Then, the second stage iteratively constructs each tree in the random forest and updates the weights of each sample after making the final decision using a weighted voting mechanism. In 2021, Lu et al. [21] focused on the exploration of information security of electric-power IoT and suggested that the current methods for protecting IoT devices need to be improved. Abbas et al. [22] proposed an intrusion detection system based on integrated learning. On the basis of using some existing advanced technologies to analyze the performance of the model, the voting classifier is deployed using logical regression, naive Bayes and decision tree. The accuracy of the

proposed model has been significantly improved in the two-category and multi-category scenarios. Khan et al. [23] introduced a new intrusion detection method based on integrated voting classifiers. In this method, multiple traditional classifiers are combined as basic learners, and the prediction of traditional classifiers is voted to obtain the final prediction. Ullah et al. [24] proposed an intrusion detection system based on deep convolution neural network. The model consists of two convolutional layers and three fully connected dense layers, which can improve performance and reduce computing power. Driss et al. [25] proposed an attack detection framework for vehicle sensor networks based on federated learning. The scheme uses a group of gated recursive units and a signal group unit based on a random forest. MEC and other basic theories are required for the distributed learning model represented by federated learning. Liang et al. [26] systematically summarized the research results of MEC computing resource allocation in recent years. Saha et al. [27] detected outliers by Euclidean distance in logistic regression to identify intrusions. An intrusion detection model based on network detection data learning mechanism is proposed. In 2022, Shitharth et al. [28] proposed an innovative cluster-based classification method to accurately detect intrusions from different types of IDS datasets. First, data preprocessing is performed to normalize the dataset to eliminate irrelevant attributes and organize features. Then, a spatial clustering algorithm is applied by using intelligent expected distance-based clustering combined with density-based noise. Finally, data separation is applied by forming clusters. Mebawondu et al. [29] tried to optimize the IDS model by using a set of decision tree (DT) algorithms to build a network IDS. By using the C4.5 DT classifier, and the ensemble technique of bagging and AdaBoost, the performance of IDS is significantly improved. Rashid et al. [30] study a tree-based stacking ensemble technique for IDS and test the effectiveness of the proposed model on two intrusion datasets (NSL-KDD and UNSW-NB15). The proposed model can better identify normal and abnormal traffic in the network than other existing IDS models. In 2023, Gopi et al. [31] combined the chaotic cuckoo search optimization algorithm and the optimal wavelet kernel extreme learning machine, and designed an IDS scheme for the 4.0 platform. This scheme uses a classification method for feature selection which achieves minimal computational complexity and maximal detection accuracy. Sivanantham et al. [32] proposed a new network security IDS framework by using the modified frequent patterns through the K-means algorithm. Gautami et al. [33] divided WSN IDS into data collection (DG) and intrusion detection (ID) stages. In the DG stage, sensor nodes form clusters in the WSN, and then the cluster heads are selected by a distance-based Drosophila fuzzy algorithm. During the ID phase, data is collected through the discovered paths and tested with the trained IDS. Alikhanov et al. [34] explored the impact of packet sampling on the performance and efficiency of ML-based Network Intrusion Systems (NIDS). The effects of various sampling techniques on the NIDS detection rate and false positive rate were further investigated. Kavitha et al. [35] address security and privacy issues in the Industrial Internet of Things (IIoT) by using IDS. A deep learning-enabled privacy-preserving technique for IDS in an IIoT environment is proposed which determines the presence of intruders in an IIoT network by using DL and feature selection techniques. Thakkar et al. [36] investigate the IDS problem by considering algorithms from the fields of ML, DL, and Swarm and Evolutionary Algorithms (SWEVO). The authors discuss the different datasets for IDS and focus on methods for incorporating feature selection into their models for performance evaluation.

In 2019, Yuan et al. [37] experimentally argued that federated learning is trustworthy and has benefits for privacy protection, even "without revealing any private information". In the same year, Wang et al. [38] proposed an intrusion detection approach based on federated learning and CNN. This approach argued that the combination of federal learning and CNN intrusion detection approach can largely reduce the training time and maintain a high detection rate while protecting user privacy.

In 2020, Latif et al. [39] proposed an intrusion detection model based on federated learning and claimed the use of genetic algorithms with feedforward neural networks can better improve the accuracy of IDS. In 2022, Alevizos et al. [40] consider a new security model called Zero Trust Architecture (ZTA) where no endpoint (i.e. device), user or application can be trusted. A blockchain-enabled intrusion detection and prevention system is proposed which enhances ZTA onto endpoints. Fedorchenko et al. [41] reviewed existing federated learning-based IDS solutions and studied their advantages as well as the open challenges they still face. The architecture of the proposed intrusion detection system and the method used to model data partitioning across clients are analyzed with emphasis.

All these researches have been effective in IoT intrusion detection to some extent, but none of them can simultaneously achieve both high accuracy and low cost of intrusion.

3 IoT Intrusion Detection System

3.1 Data Set Selection and Data Preprocessing

The model used in this paper is NSL-KDD dataset [42] selected by Wang et al. [43] in a machine learning based IoT intrusion detection system. This dataset is formed by expanding and developing the KDD99 dataset, which is based on the network connection communication data recorded in the 1999 KDD Cup competition and solves the existing problems in the KDD99 dataset. The KDD99 dataset is mainly divided into eight parts: KDDTrain+. ARFF, KDDTrain+. TXT, KDDTrain+_20Percent. ARFF, KDDTrain+_20Percent. TXT, KDDTest+. ARFF, KDDTest+. TXT, KDDTest-21. ARFF, KDDTest-21. TXT, with reasonable settings of training set and test set. None of these parts contain redundant records which thus makes the classifier and detection more accurate and can be used as an effective benchmark dataset to help researchers compare the advantages of different intrusion detection methods. In order to achieve a more efficient and cost effective operation, the dataset is initially modeled based on algorithms such as legal value screening and NULL value cleaning.

In addition, one of the advantages of this model is to improve the deficiency of filtering feature vectors for specific IoT devices by Zhendong Wang et al. The project team analyzes and verifies the traffic data collected from specific IoT devices using the network packet analysis tool called Wire shark. Based on the theoretical analysis and practical application, a modified NSL-KDD dataset including Hyper Text Transfer Protocol (HTTP), Secure Sockets Layer (SSL) and other feature vectors is selected.

In this paper, the physical layer data frame (Frame), data link layer Ethernet frame (Ethernet II, Src), Internet layer IP packet (Internet Protocol Version 4, Src), and Internet Control Message Protocol (Internet) are selected for intrusion detection of IoT devices. Control Message Protocol and other identification data are used as criteria to determine whether the intrusion is legitimate. The relevant data such as ack, duration and domain are contained in the above information.The data are selected and abstracted into numerical symbols to form a feature vector. In Fig. 1, a flow chart of data processing is illustrated.

The accuracy of the results could not be determined because the feature vectors selected by the project team would be different after processing. Therefore, the project team used the zero-mean normalization method to convert the feature values into data that could be centrally calculated and processed without changing their variance, so that the original appearance of the data could be better preserved. The null values are removed to lose some data, and the desired set is finally obtained. The distribution of the dataset is shown in Table 1.

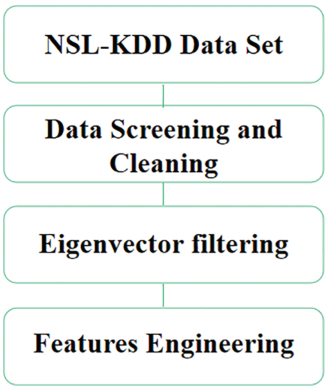


Figure 1: Data processing flow chart

Table 1: Data set

Attack type	Normal attack	Dos attack	Probe attack	R2L attack	U2R attack	Total
Sample size	97277	397458	4107	1126	52	494020
Percentage of attacks	19. 6909	79. 2393	0. 8313	0. 02279	0. 0105	100

Similar to the traditional predictive analytics model, this model divides the data into two major parts. 80% is used as training data for building the model and 20% is used as test data for testing the model.

3.2 An IoT Intrusion Detection System Framework Based on CNN

In order to achieve the effects of artificial intelligence in IoT device intrusion detection, this paper combines CNN and machine learning to establish an intrusion detection system model for IoT devices. Based on the traditional deep learning centralized training-based approach, which cannot guarantee data security and has poor learning results due to insufficient or monotonous data under attack, a federal learning algorithm is combined to improve it.

The IoT IDS framework based on CNN is shown in Fig. 2.

3.3 Cloud-based Loss Function Computational Design

A CNN is a feed-forward neural network that responds to a portion of the surrounding units in the coverage area and is well suited for large image processing. CNN consists of one or more convolutional layers and a top fully connected layer. It also includes associative weights and pooling layers. This structure allows CNN to take advantage of the two-dimensional structure of input data. Compared to other deep learning structures, CNN can provide better results in image and speech recognition. CNN requires fewer parameters to be considered than other deep feedforward neural networks, which makes it an attractive deep learning structure.

LSTM and RNN models are mainly used to solve the gradient disappearance problem in the backpropagation process and are good at short-term memory. LSTM and RNN models are mainly used to solve the problem of gradient disappearance in the process of back propagation. They are

good at short-term memory, but poor in long-term memory and in the face of apt attacks and bot attacks [24], so it is difficult to train efficient IOT attack prevention models. As shown in Fig. 3, in full consideration of the characteristics of CNN model, RNN and LSTM, we decided to use CNN as the main framework of neural network design.

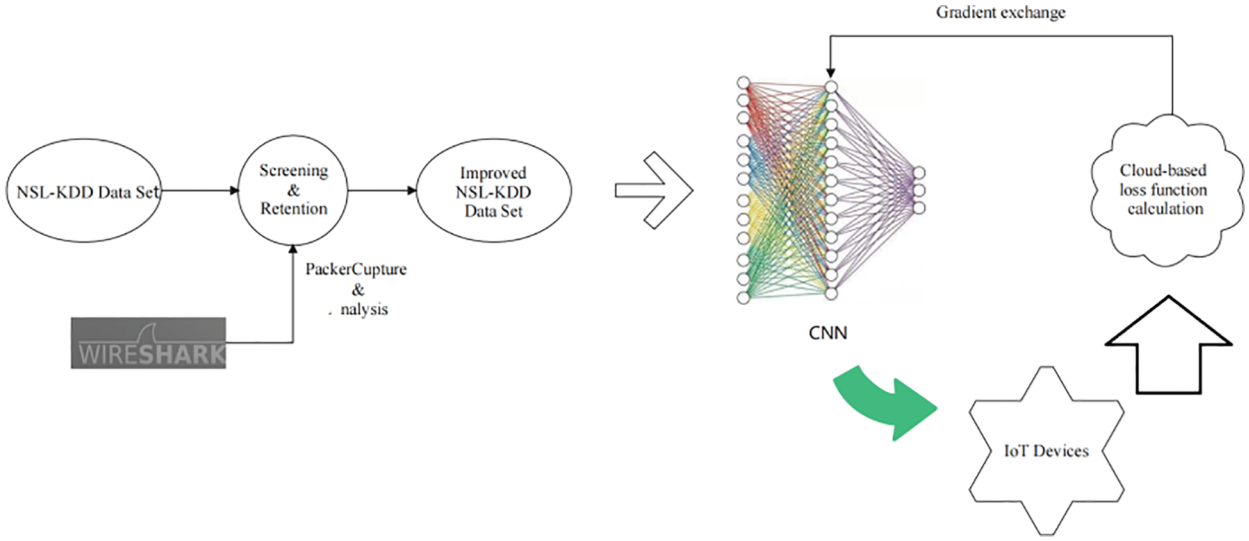


Figure 2: The IoT IDS framework based on CNN

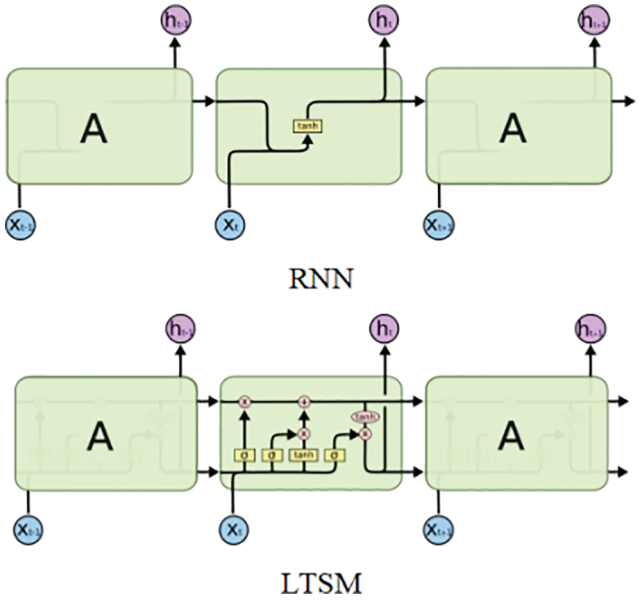


Figure 3: Comparison of RNN model and LSTM model

CNN needs no fully connected architecture between layers and can reduce both the number of parameters and the degree of overfitting through parameter sharing mechanism. On the contrary, through sparse connections, shared weights, and pooling, CNN can also effectively reduce the difficulty of processing data and greatly improve modeling efficiency. In this paper, a 1:9 ratio is used

to split the data set by dividing 10% of the data set samples as the test set and 90% of the samples as the training set to test the robustness of the model for preventing the model from overfitting at the same time.

As shown in Fig. 4, the composition of the design model in this paper is divided into one input layer, two convolutional, two pooling layers, and three fully connected layers with one output layer. In order to prevent overfitting, this paper adopts a regularization method and uses a Dropout layer between the flattened model and the first fully connected layer to discard neurons from the neural network with a 40% probability. The Sigmoid function is used as an activation function for the hidden layer. The input layer represents streaming data with a two-dimensional matrix. The second layer is a convolutional layer with a convolutional kernel of 32, a convolutional window of size 3×3, an input thickness of 1, and an output thickness of 32. The third layer is a maximum pooling layer with all-zero padding to reduce the size of the model, increase the computational speed, and improve the robustness of the extracted features. The fourth layer, similar to the second layer, is a convolutional layer with 64 convolutional kernels. The activation function of the last layer is a Soft-max function for the output of the classifier, which is designed for multi-classification. The batch size used for training the network is set to 1000. The optimizer is selected as Adam, and the learning rate is set to 0. 0001.

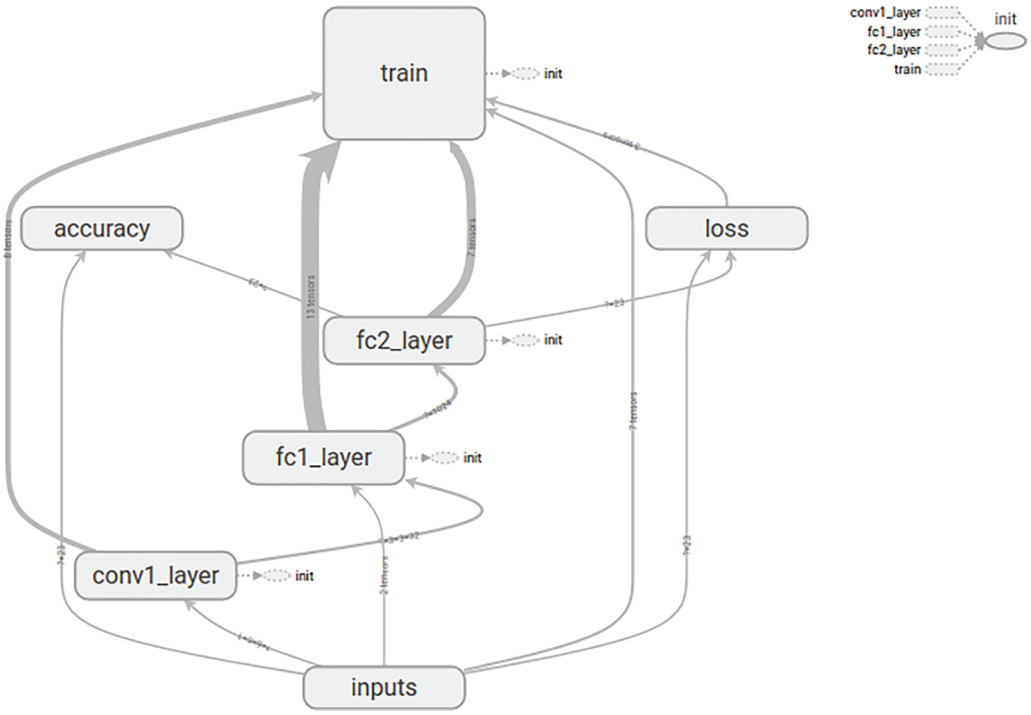


Figure 4: CNN design schematic

The improved NSL-KDD dataset belongs to typical imbalanced data, and the normal sample size is much larger than the sample size of other categories, especially the u2r sample category. Therefore in this paper, we choose Focal Loss as the loss function to train the neural network [44] and upload it to the cloud, so as to improve the accuracy of the model and reduce the cost of the server at the same time. The traditional cross-entropy loss function focuses on positive and negative samples equally. Focal Loss can adjust the weights of both positive and negative samples, and meanwhile control the weights of difficult and easy classification samples. It has good performance for unbalanced samples.

3.4 An IoT Intrusion Detection Algorithm Combining Federated Learning and CNN

In this paper, we explore the feature vectors of IoT devices by combining CNN and machine learning to form an artificial intelligence intrusion detection system. It has a high degree of intrusion detection and autonomous learning. However, the richness of learning of both network-based and host-based intrusion detection systems can lead to poor learning results due to the insufficient or monotonous amount of attacked data.

The reliability of federated learning, the possibility of combining it with IDS, and the possibility of artificial intelligence of IDS can be seen. However, the above-mentioned articles or projects only use federated learning as a method for future development or system maintenance. No experimental validation has been conducted. The usability and accuracy of applying federated learning to artificial intelligence intrusion detection systems are yet to be verified. This paper focuses on the introduction of federated learning into existing AI intrusion detection systems as a necessary path for the future development of IDS technology. Federated learning is essentially a distributed machine learning framework. It achieves data sharing and joint modeling on the basis of ensuring data privacy security and legal compliance. Fig. 5 shows a schematic diagram of the federated learning algorithm. When k independent data sources $B_1, B_2, \ldots, B_k$ jointly participate in model training, there is no need to transfer the original data. Server A acts as a coordinator that centrally manages the intermediate parameters of the model. Model joint training is only performed between data sources through the interaction of the intermediate parameters of the model, and the original data may not be local. Thus the data privacy protection mode of "data availability is invisible".

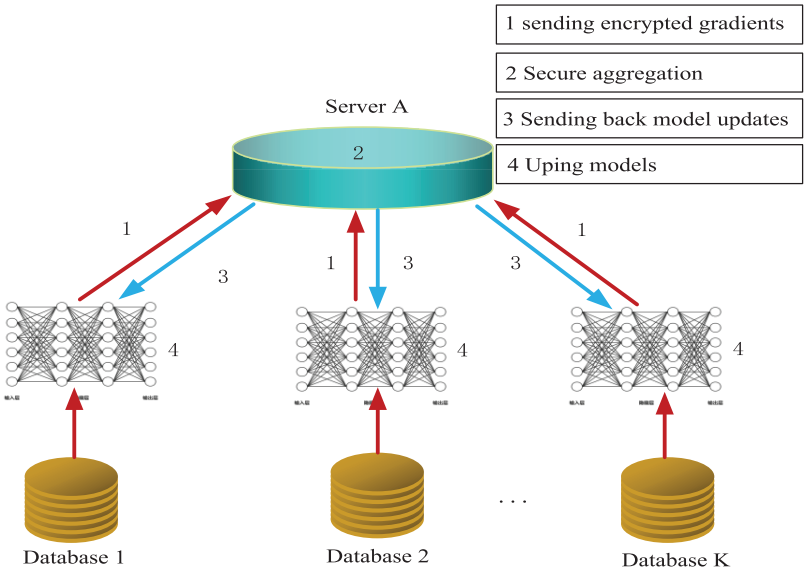


Figure 5: Federal learning algorithm

As shown in Table 2, combining CNN and federated learning algorithms, we propose a new IoT intrusion detection algorithm. n is the number of distributed machines. $p(n)$ is the local model parameter of each machine. $P(n)$ is the local model of each machine after encryption. *coordinator* is the coordinator. *new_p* is the new model parameter obtained by the coordinator through gradient descent and other methods. is a new parameter distributed to each machine. *new_model* (n) is based

on the *new_data* (*n*). *F* (*x*) is the set of functions that the coordinator aggregates data. *Encrypt* () is a cryptographic function. *update* () is an update parameter function.

Table 2: An IoT intrusion detection algorithm

Algorithm 1: An IoT intrusion detection algorithm combining federated learning and CNN.

Input: tarin_data (n) //local learning achievements from n
Output: new_model (n) //new model after federal learning
1. p(n) ← train_data(n) //get local learning achievements from n
2. P (n) ← encrypt (p (n))
3. coordinator ← all (P (n))
4. new_p ← F(coordinator) //F (x) was designed to aggregate data
5. new_data (n) ← new_p
6. new_model (n) ← update (new_data (n))

First, *n* distributed machines train and learn locally on their own data via CNN. Thereby, the respective models and corresponding parameters are obtained. On the premise that there is no need to exchange local individuals or sample data, the *n* data sources with local data each perform distributed model training. Then, the parameters of the *n* models are extracted, encrypted and uploaded to the unified coordinator. The coordinator aggregates the data into new model parameters through methods such as gradient descent. Finally, the new model parameters are reassigned to each machine to update the respective model. The algorithm achieves a balance between data privacy protection and data sharing computing at the expense of increasing machine costs.

4 Simulation and Discussion

4.1 Experimental Environment

Since false reports and omissions are inevitable during the practice of the project, this paper uses the Correct Report Rate (CR), Loss Report Rate (LR), and Mistake Report Rate (MR) as the basis for evaluation. Table 3 shows the confusion matrix used for evaluation.

Table 3: Confusion matrix

Predicted actual category	TRUE	FALSE
TRUE	TP	FN
FALSE	FP	TN

Corresponding to the data in the table, the accuracy rate is calculated as

$$CR = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

The underreporting rate is calculated as

$$LR = \frac{TP}{TP + FN} \tag{2}$$

The false alarm rate is calculated as

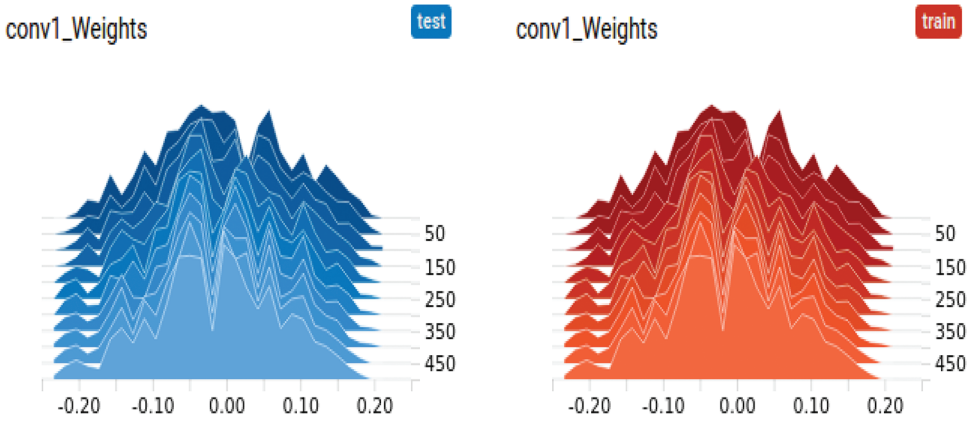
$$MR = \frac{FP}{FP + TN} \tag{3}$$

The intrusion detection system experiments are performed with computer memory 8G, processor i5-10500, single-core3. 0 ghz full-core 3.7 ghz, and dual-core quad-thread gauge. The operating system is Ubuntu 18. 04. 05 LTS version. The language environment is python, and the framework is built by using a Tensor-flow environment.

4.2 Experimental Results

The results of this experiment show that the artificial intelligence training model of intrusion detection system using CNN algorithm on the basis of improved NSL-KDD dataset has feasibility, high accuracy and can test loss function. The experiments are divided into training and testing groups. The Tensor-board visualization interface is used to derive the corresponding results.

The training set weight comparison is shown in Fig. 6a, and the test set weight comparison is shown in Fig. 6b. The training group peaks at 25. 7 in the second slice at a horizontal coordinate of −0. 0494, while the test group peaks at 25. 8 in the second slice at a horizontal coordinate of −0. 0494, and the rest of the slices are basically the same.



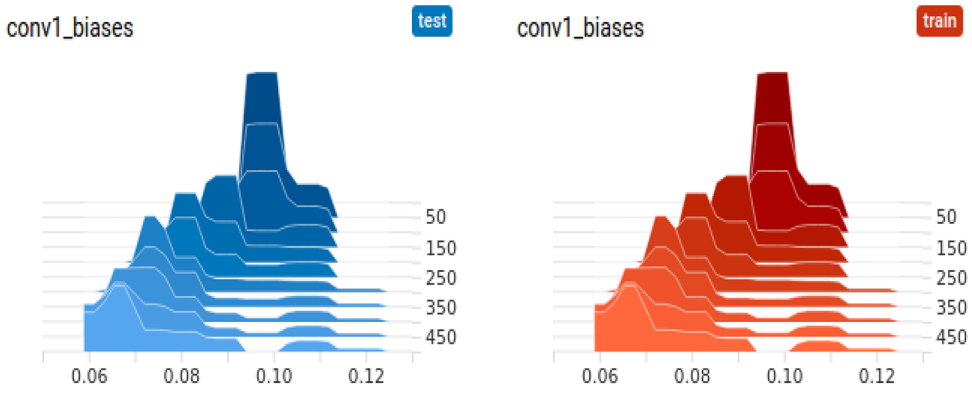
(a) training set weights (b) test set weights

Figure 6: Training set's and test set's wights

The training set bias pairs shown in Fig. 7a and the test set bias pairs shown in Fig. 7b do not differ in the representation of the curves at the horizontal coordinate unit of 0. 01 and the vertical coordinate of 100. Both training set bias pairs and test set bias pairs take the maximum value of 7. 57 in the interval of [0. 0964, 0. 101].

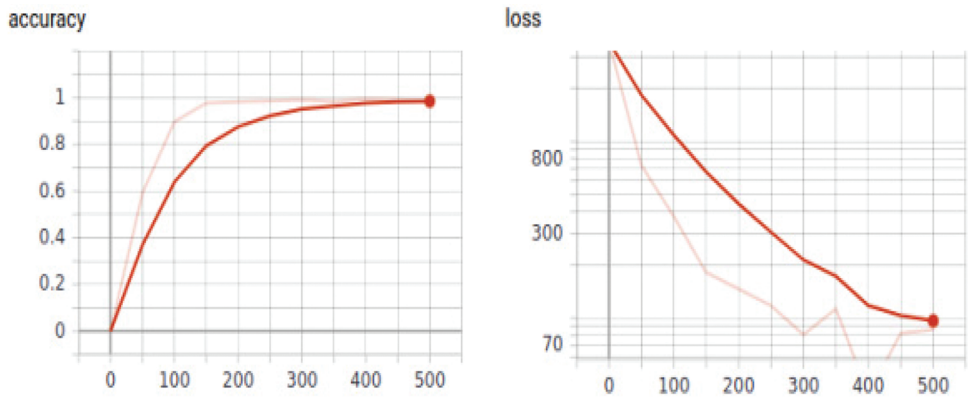
After calculating the weights and biases of this model, the accuracy and loss rates of the training and test sets are mathematically and statistically analyzed and are presented through visualization. After multiple algorithm tuning, the training time for the training set was 35 min and 50 s. The results are shown in Fig. 8a (the curvature of the curve is 0. 600). Although the NSL-KDD dataset used by this model is pruned, the introduction of a loss function makes the training set accuracy still as high as 97.2%. Not far off the CNN-based 99.5% accuracy on the full NSL-KDD dataset [45]. Meanwhile, as shown in Fig. 8b, due to the fact that the Focal-loss loss function is invoked in the experiments,

the accuracy of the deep learning-based model is greatly improved due to the Focal-loss loss function invoked in the experiments.



(a) bias values in the training set (b) bias values in the test set

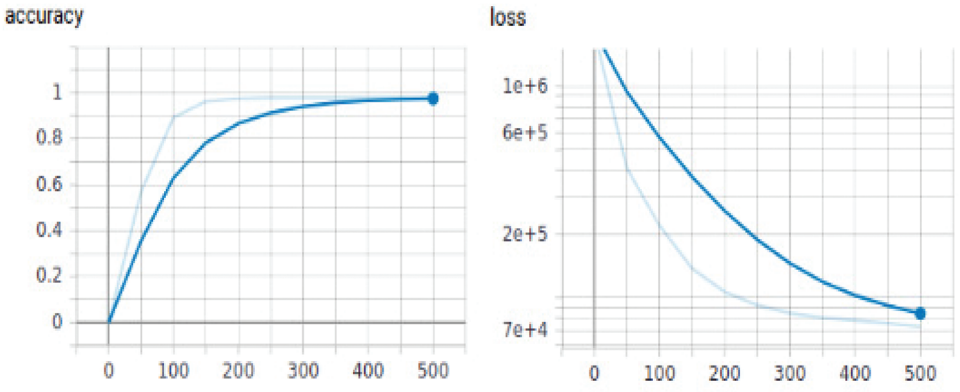
Figure 7: Bias values in the training set and test set



(a) Accuracy plot of training set (b) Loss function plot

Figure 8: Training set's accuracy plot and loss function

In this paper, a test set is then trained and tested which takes 35 min and 46 s. As shown in Fig. 9a (the curvature of the curve was set to 0. 600), the test set accuracy was 96. 5%. The loss function is shown in Fig. 9b. The parameters of Accuracy, Precision, Recall and F1 of our proposed algorithm are shown in Table 4.



(a) Test set accuracy plot (b) Loss function plot

Figure 9: Test set's accuracy plot and loss function

Table 4: The parameters of our proposed algorithm

Our model	Accuracy	Precision	Recall	F1
Train	97.2	97.9	99.5	98.7
Test	96.5	97.6	98.9	98.2

The experimental results of this experiment are shown in Table 5.

Table 5: Experimental results

Type	Percentage	CR	MR	LR
Train Set	90. 1	97	2. 1	0. 5
Test Set	9. 9	96. 5	2. 4	1. 1

As shown in Table 5, in this experiment, the accuracy, false alarm, and missed alarm rates of the training group were 97. 2%, 2. 1% and 0. 5%, respectively. While the accuracy, false alarm, and missed alarm rates of the test group were 96. 5%, 2. 4% and 1. 1%, respectively.

In the field of machine learning, the AUC value is often used to evaluate the training effect of a binary classification model. The research on the IDS system in this paper is to distinguish whether it is a malicious attack, or to distinguish the specific form of the attack. Different from the CNN algorithm proposed in this paper, the mainstream algorithms include decision tree [29], Naive Bayes [28], Logist regression [27], ensemble algorithm [30] and so on.

As shown in Fig. 10, the CNN algorithm proposed in this paper has a good classification effect. Although the performance is not as good as decision tree [29], it is comparable to Logist regression [27] and better than Naive Bayes [28] and ensemble algorithm [30] for classification.

As shown in Fig. 11, in the performance of category classification, CNN is not inferior to decision tree [29], Naive Bayes [28], Logist regression [27], and ensemble algorithm [30]. More importantly, the CNN algorithm proposed in this paper combines the distributed architecture of federated learning,

which can fully consider the privacy protection of users. Distributed nodes exchange model parameters or intermediate results without exchanging local individuals or sample data. By building a global model based on virtual fusion data, the balance between data privacy protection and data sharing computing can be achieved.

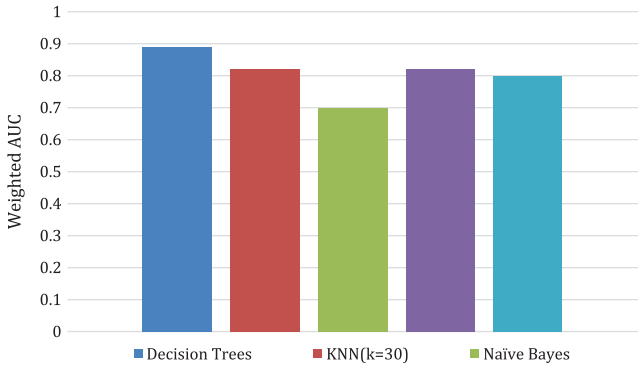


Figure 10: AUC for binary classification with different algorithms.

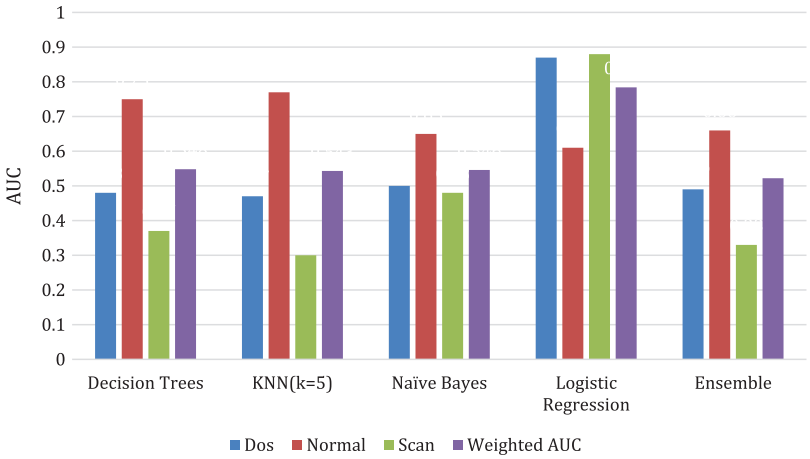


Figure 11: AUC for category classification with different algorithms

5 Conclusions

The IoT environment will be a big data environment. Due to the uneven distribution of features and data volume, the detection results may be inaccurate. Data cleaning and analysis will help reduce additional system overheads. By introducing the loss function, the accuracy can be improved and the problem of data set imbalance caused by data deletion can be alleviated. However, this paper does not detect and analyze real-time data in the Internet of Things environment. Therefore, the Internet of Things intrusion detection model based on CNN and federated learning can be improved in future research to solve the above problems. This paper attempts to establish the Internet of Things intrusion detection system to protect users' personal privacy and property interests. In addition, by selecting a large number of eigenvalues and optimizing the algorithm, the model has a high accuracy.

Acknowledgement: Jie Yin and Yuxuan Shi conceived and designed the experiments; Wen Deng, Chang Yin and Tiannan Wang performed the experiments; Yucheng Song, Tianyao Li and Yicheng Li analyzed the data; Jie Yin wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding Statement: This research has been supported by the Open Project of the State Key Laboratory of Nanjing University "Research on Intrusion Signal Detection Technology Based on Deep Learning in Complex Electromagnetic Environment", the Open Project of the State Key Laboratory of CAD&CG, Zhejiang University, "Analysis and Visualization of Heterogeneous and Multi-source Cyber Threat Intelligence Data", Jiangsu Province Big Data Management Center Project "Research on Network Security Perception of Jiangsu E-government Extranet".

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Xu, Z. Fang, J. Zhang, Q. He, D. Yu *et al.,* "Edge content caching with deep spatiotemporal residual network for IoV in smart city," *ACM Transactions on Sensor Networks*, vol. 17, no. 3, pp. 1–33, 2021.

[2] X. Xu, Z. Fang, L. Qi, X. Zhang, Q. He *et al.,* "TripRes: Traffic flow prediction driven resource reservation for multimedia IoV with edge computing," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2, pp. 1–21, 2021.

[3] P. Shanmugapriya, J. Baskaran, C. Nayanatara and D. P. Kothari, "IoT based approach in a power system network for optimizing distributed generation parameters," *CMES: Computer Modeling in Engineering & Sciences*, vol. 119, no. 3, pp. 541–558, 2019.

[4] Y. Zhang and X. Ran, "A step-based deep learning approach for network intrusion detection," *CMES-Computer Modeling in Engineering & Sciences*, vol. 128, no. 3, pp. 1231–1245, 2021.

[5] H. Breivold, "A survey and analysis of reference architectures for the internet-of-things," in *Proc. of ICSEA*, Athens, Greece, pp. 132–138, 2017.

[6] Q. Qin, "Security standards and measures for massive IoT in the 5G era," *Mobile Networks and Applications*, vol. 27, no. 1, pp. 392–403, 2022.

[7] S. Maria, "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[8] T. Lunt, "A survey of intrusion detection techniques," *Computers & Security*, vol. 12, no. 4, pp. 405–418, 1993.

[9] R. Gai, X. Du, S. Ma, N. Chen and S. Gao, "A summary of 5G applications and prosprcts of 5G in the Internet of things," in *Proc. of ICBAIE*, Nanchang, China, pp. 858–863, 2021.

[10] N. Kong, "Research on key technologies for addressing resources of internet of things," Ph.D. dissertation, Graduate School of Chinese Academy of Sciences (Computer Network Information Center), 2008.

[11] A. Ostroukh and T. Yuan, "Development of the information and analytical monitoring system of technological processes of the automobile industry enterprise," *World of Scientific Discoveries*, vol. 2, no. 1, pp. 91–102, 2014.

[12] H. Rolf, "Internet of things-new security and privacy challenges," *Computer Law and Security Review: The International Journal of Technology and Practice*, vol. 26, no. 1, pp. 23–30, 2009.

[13] B. Zhao, D. Wang, X. Qian and J. Li, "Design and implementation of blockchain based trust gateway for power IoT," *China Power*, vol. 1, no. 1, pp. 1–6, 2021.

[14] S. Kamble, A. Gunasekaran and H. Arha, "Understanding the blockchain technology adoption in supply chains-indian context," *International Journal of Production Research*, vol. 57, no. 7, pp. 2009–2033, 2019.

[15] L. Metongnon and R. Sadre, "Beyond telnet: Prevalence of IoT protocols in telescope and honeypot measurements," in *Proc. of WTMC*, Budapest, Hungary, pp. 21–26, 2018.

[16] S. Demetriou, N. Zhang and Y. Lee, "HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps," in *Proc. of WiSC*, Boston, MA, USA, pp. 122–133, 2017.
[17] A. Derhab, M. Guerroumi and A. Gumaei, "Blockchain and random subspace learning-based ids for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, pp. 1–24, 2019.
[18] R. Vinayakumar, M. Alazab and K. P. Soman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, no. 4, pp. 41525–41550, 2019.
[19] J. Lueckenga, D. Engel and R. Green, "Weighted vote algorithm combination technique for anomaly based smart grid intrusion detection systems," in *Proc. of IJCNN*, Vancouver, BC, Canada, pp. 2738–2742, 2016.
[20] B. A. Tama and L. Sunghoon, "Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation," *Computer Science Review*, vol. 39, no. 2, pp. 100357–100367, 2021.
[21] Y. Lv, X. Zhao and X. Lu Xiaoxiao, "Exploring the information security of power IoT," *Science and Technology Information*, vol. 19, no. 1, pp. 53–55, 2021.
[22] A. Abbas, M. A. Khan, S. Latif, M. Ajaz and A. A. Shah, "A new ensemble-based intrusion detection system for internet of things," *Arabian Journal for Science and Engineering*, vol. 47, no. 1, pp. 1805–1819, 2022.
[23] M. A. Khan, M. A. Khattk, S. Latif, A. A. Shah *et al.,* "Voting classifier-based intrusion detection for IoT networks," in *Proc. of AISC*, New York, NY, USA, pp. 313–328, 2021.
[24] S. Ullah, J. Ahmad, M. A. Khan, E. H. Alkhammash, M. Hadjouni *et al.,* "A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering," *Sensors*, vol. 22, no. 10, pp. 3607–3622, 2022.
[25] M. Driss, I. Almomani, Z. Huma and J. Ahmad, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Complex & Intelligent Systems*, vol. 8, no. 1, pp. 4221–4235, 2022.
[26] G. Liang, Q. Wang, J. Xin, M. Li and W. Xu, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Journal of Information Security*, vol. 6, no. 3, pp. 227–256, 2021.
[27] R. Saha, G. Kumar, M. Kumar Rai and H. Kim, "Adaptive classifier-based intrusion detection system using logistic regression and Euclidean distance on network probe vectors in resource constrained networks," *International Journal of Information and Computer Security*, vol. 16, no. 3, pp. 226–238, 2021.
[28] S. Shitharth, P. R. Kshirsagar, P. K. Balachandran, K. H. Alyoubi and A. O. Khadidos, "An innovative perceptual pigeon galvanized optimization (ppgo) based likelihood naïve bayes (lnb) classification approach for network intrusion detection system," *IEEE Access*, vol. 10, no. 5, pp. 46424–46441, 2022.
[29] O. J. Mebawondu, O. D. Alowolodu, A. O. Adetunmbi and J. O. Mebawondu, "Optimizing the classification of network intrusion detection using ensembles of decision trees algorithm," In: Misra, S., Muhammad-Bello, B. (eds) "Information and Communication Technology and Applications," in *Proceedings of ICTA*, New York, NY, USA, 286–300, 2021.
[30] M. Rashid, J. Kamruzzaman and T. Imam, "A tree-based stacking ensemble technique with feature selection for network intrusion detection," *Applied Intelligence*, vol. 2022, no. 9, pp. 9768–9781, 2022.
[31] R. Gopi, R. Sheeba, K. Anguraj, T. Chelladurai, H. Mesfer Alshahrani *et al.,* "Intelligent intrusion detection system for industrial internet of things environment," *Computer Systems Science and Engineering*, vol. 44, no. 2, pp. 1567–1582, 2023.
[32] S. Sivanantham, V. Mohanraj, Y. Suresh and J. Senthilkumar, "Association rule mining frequent-pattern-based intrusion detection in network," *Computer Systems Science and Engineering*, vol. 44, no. 2, pp. 1617–1631, 2023.
[33] A. Gautami, J. Shanthini and S. Karthik, "A quasi-newton neural network based efficient intrusion detection system for wireless sensor network," *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 427–443, 2023.
[34] J. Alikhanov, R. Jang, M. Abuhamad, D. Mohaisen, D. Nyang *et al.,* "Investigating the effect of traffic sampling on machine learning-based network intrusion detection approaches," *IEEE Access*, vol. 10, pp. 5801–5823, 2022.
[35] G. Kavitha, "Deep learning enabled privacy preserving techniques for intrusion detection systems in the industrial internet of things," *Adhoc & Sensor Wireless Networks*, vol. 52, pp. 223–247, 2022.

[36] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence*, vol. 55, pp. 453–563, 2022.
[37] H. Yuan, C. Ma, Z. Zhao, X. Xu and Z. Wang, "A privacy-preserving oriented service recommendation approach based on personal data cloud and federated learning," in *Proc. of ICWS*, Barcelona, Spain, pp. 322–330, 2022.
[38] R. Wang, C. Ma and P. Wu, "Intrusion detection method based on federal learning and CNN," *Technology Research*, vol. 1, no. 4, pp. 47–54, 2020.
[39] S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 1, no. 8, pp. 89337–89350, 2020.
[40] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi and J. Read, "Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture," *IEEE Access*, vol. 10, pp. 89270–89288, 2022.
[41] E. Fedorchenko, E. Novikova and A. Shulepov, "Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges," *Algorithms*, vol. 15, no. 7, pp. 1–26,2022, 2022.
[42] J. Rene and D. Shalini, "An efficient mixed attribute outlier detection method for identifying network intrusions," *International Journal of Information Security and Privacy*, vol. 14, no. 3, pp. 115–133, 2020.
[43] Z. Wang, L. Zhang and H. Li, "A review of machine learning based intrusion detection system for IoT," *Computer Engineering and Applications*, vol. 57, no. 4, pp. 18–273, 2021.
[44] A. Verma, H. Saxena, M. Jaiswal and P. Tanwar, "Intelligence embedded image caption generator using LSTM based RNN model," in *Proc. of ICCES*, Coimbatre, India, pp. 963–967, 2021.
[45] A. Hadeel, A. Sharieh and K. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," *Expert Systems with Applications*, vol. 148, no. 1, pp. 1–10, 2020.