Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3359721, 12 pages
https://doi.org/10.1155/2022/3359721

Research Article

Front-End Model of Wireless Network Combined with Artificial Intelligence in Computer Information Management System

Yu Wang

Modern Education Technology Center, Qiqihar Medical University, Qiqihar, 161006 Heilongjiang, China

Correspondence should be addressed to Yu Wang; wangyu@qmu.edu.cn

Received 29 January 2022; Revised 22 March 2022; Accepted 28 March 2022; Published 25 May 2022

Academic Editor: Narasimhan Venkateswaran

To address the security problem of computer information management, an artificial intelligence- (AI-) based information intrusion detection model is built in combination with wireless network. Firstly, the background and characteristics of wireless local area network (WLAN) technology are analyzed, and the relationship between AI technology and deep learning is introduced. Secondly, an intrusion detection model on account of long short-term memory (LSTM) neural network and gated recursive unit (GRU) is constructed after analysis of different neural network models. The L2 weight attenuation and dropout regularization strategies are combined with the neural network model. Finally, an intrusion detection front-end model combining wireless network and AI is established. From the comparison of intrusion detection experiments, the generalization ability of the model can be improved by using L2 weight attenuation and dropout regularization strategies. Nevertheless, the performance improvement is only slight, so the early stop method is adopted instead of the regularization strategy. Compared with the existing classification models, the overall performance of LSTM and GRU models is improved by about 17%. The performance of GRU model is not much different from that of LSTM model, but the amount of computation is reduced. Therefore, GRU model is the optimal choice to construct intrusion detection system. The intrusion detection models in WLAN and GRU can improve the security performance of computer information management system. To sum up, this work provides reference for the development of computer management system.

1. Introduction

With the progression of computer network technology, the security performance of computer information management system becomes more and more important [1]. The information management systems of many enterprises store abundant internal confidential information, which will bring huge losses once it is invaded [2]. In recent years, as technology has improved, cyberattacks have become more diverse. Although network intrusion detection technology has been developing, there are still some problems. Intelligent wireless networks can be built by integrating wireless networks and artificial intelligence (AI). In essence, low-delay communication can ensure the stability of information transmission. However, the construction of decision environment also brings unprecedented challenges in network design, optimization, and scalability. AI breakthroughs, especially in deep learning, have moved from facial recognition, medical diagnosis, and natural language processing to almost every aspect of our lives. AI technology has increased data availability and more computing power, and the performance of computing devices has improved. These new application requirements are generating great interest in reliable new forms of computer information management.

For computer information management system, scholars in the world have done a lot. Magán-Carrión et al. [3] proposed a structured approach and evaluate the UGR'16 dataset to test its applicability to network attack detection. Verma and Ranga [4] generated the RPL-NIDDS17 dataset, which consists of seven modern routing attack patterns and normal traffic patterns. In the proposed dataset, 22 attributes are considered, including features of traffic, temporal types, and two additional label attributes. The effectiveness of RPL-NIDDS17 is demonstrated by statistically analyzing the correlation between the probability distribution of features and the features. Thapa et al. [5] proposed an intrusion detection system using different machine learning (ML) and deep learning (DL) models. A comparative analysis of different ML and DL models is performed on the Coburg Intrusion Detection Dataset. Different ML and DL models are compared on the dataset, and an ensemble model is proposed that combine the optimal DL algorithm with ML algorithm to achieve high performance metrics. Finally, the best model is benchmarked with the CIC-IDS2017 dataset and is compared with the state-of-the-art model. Choi et al. [6] developed a network intrusion detection system using the unsupervised learning algorithm autoencoder and verify its performance. As the results show, the model achieves an accuracy of 91.70%, surpassing the accuracy of 80% of previous researches using clustering algorithms. Musafer et al. [7] come up with a novel mathematical model for further development of robust, reliable, and efficient software, and it is applied for practical intrusion detection. The hyperparameters of high-performance sparse autoencoder are tuned to optimize features and classify normal and abnormal traffic patterns. The proposed framework allows the parameters of the backpropagation learning algorithm to be adjusted through a series of triangular simple designs, to suit the performance and structure of sparse autoencoders. The framework proposed by Le et al. [8] is composed of two main parts. The first part is to build the sequential forward selection decision tree, which is a feature selection model. It is to generate the optimal feature subset from the original feature set, as a hybrid sequential forward selection algorithm and decision tree model. The second part is to build various intrusion detection models to train on the subsets of optimal selected features. Various recursive neural networks are geared to traditional recurrent neural network (RNN), long short-term memory (LSTM), and gated recurrent unit (GRU).

To enhance the security system of computer information management system, the front-end modeling is carried out by combining wireless network and AI, and the intrusion detection system applied to computer information management system is designed to improve the security performance of information management system. According to the different structure and characteristics of neural network, intrusion detection models under LSTM and GRU are constructed, respectively. Moreover, the validity of the neural network-based intrusion detection system is verified by experiments. It is beneficial to improve the security of computer system management system and promote the development of computer information management system. The innovation of this work lies in combining neural network technology with wireless network to improve the security of computer information management.

2. Materials and Methods

2.1. Overview of Wireless Local Area Network (WLAN) Technology. Wireless network is a network realized by wireless communication technology [9]. It includes not only global voice and data networks that allow users to establish long-distance wireless connections but also infrared and radio frequency technologies optimized for short-range wireless connections. It is very similar to the use of wired networks, but the biggest difference lies in the transmission medium. Wireless technology replaces the network cable, which can be used as a backup of the wired network [10]. The mainstream applications of wireless network are classified into wireless network and wireless local area network (WLAN). The former, such as fourth-generation mobile network, third-generation mobile network, or general packet radio service (GPRS), is realized through public mobile communication network [11]. Traditional wireless networks collect and process large amounts of data, which is usually achieved through relatively inefficient operations, and the accuracy and availability of data cannot be guaranteed in this process. However, with the development of AI technology, the data collection capability of AI technology can effectively improve the data collection performance of wireless network. Using computer system to deal with the data problem of wireless network can get better application effect.

In this experiment, WLAN is the application of wireless communication technology to connect computer devices, constituting a network system that can communicate with each other and realize resource sharing. A station (STA) is an entity with wireless access capability, and access point (AP) is an entity that uses wireless media (WM) to provide STA with distributed system (DS) access to the local area network [12]. WM is the transmission medium of WLAN. The main function of WM is transmitting information between WLAN entities. The main WM used is radio frequency [13]. DS is not a necessary part of WLAN. However, to realize the communication between WLANs and other LANs, the APs of these WLANs must be connected in series to expand the signal range of WLANs and provide communication services for STA of each WLAN. Therefore, the system composed of AP series is a DS [14]. The basic structure of a WLAN is shown in Figure 1.

The basic element of WLAN is basic service set (BSS). STAs in the same BSS can communicate with each other within the propagation range of WM [15]. BSS can be divided into standalone BSS and infrastructure BSS. Independent BSS do not require AP, and direct communication between STAs is a temporary network for temporary use only. In infrastructure BSS, STAs require to communicate through APs. The STA is connected to the AP, and the packet is transmitted to the AP, which then transmits the packet directly to the target location, so that the infrastructure BSS can effectively reduce consumption [16]. DS is linked to BSS and can also form an extended set of services with a wider range of services. WLAN communication information is transmitted through 802.11 MAC frames. Figure 2 (a) shows the specific type of 802.11 MAC frames. Figures 2 (b) and 2(c) show the frame structure and general frame format, respectively.

The data in WLAN is mainly transmitted in the form of electromagnetic waves, and it is necessary of encryption measures to protect the data security in the WLAN [17]. In the encryption authentication mode, the open system authentication mode is empty authentication, which is basically not used. The wired equivalent protection authentication is that the terminal sends an authentication request to

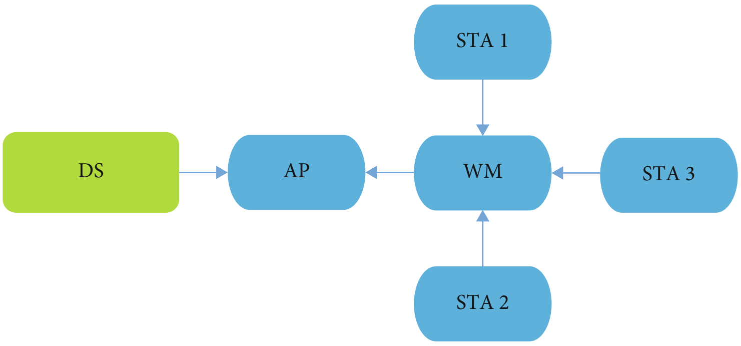


Figure 1: Structure diagram of WLAN.

the AP, and the AP sends a random number to the terminal after receiving the request. The terminal synthesizes the received random numbers into a shared key for encryption, and then, the key is sent to the AP. The AP gets the decryption key for decryption and compares it with the original random numbers. If they are same, the authentication is successful, while if they are different, the authentication fails.

Computer information management system is the information management and information system. It refers to a human-machine system composed of computers and their related and supporting equipment and facilities (including networks); it collects, processes, stores, transmits, and searches information according to certain application goals and rules [18]. Information is the description of the motion state and characteristics of things, while data is the physical symbol of load information. An information system can help business leaders obtain and analyze information about decision-making quickly and help companies reduce uncertainty and risk in decision-making. If there is insufficient information, the fundamental basis for decision-making will be lost. The information management is the process of collection, transmission, processing, judgment, and decision-making of information [19].

Computer information management system can effectively organize relevant data and achieve dynamic and efficient management [20]. The security protection of computer information management system is a very important part of management system. The deficiencies of wireless LAN are reflected in the following aspects: (I) performance: wireless LAN relies on radio waves for transmission, so it will be hindered in the transmission process, affecting the transmission performance of electromagnetic waves; (II) transmission rate: the transmission rate of wireless channel is much lower than that of wired channel and is only suitable for personal terminals and small-scale network applications; and (III) safety: radio signals are divergent and therefore easy to listen to within the range of radio waves. With the progress of computer network information technology, the intrusion of hackers or viruses has also been improved, and the network attack intrusion detection technology in computer information management system has also been greatly developed. Intrusion detection is a kind of security technology that collects and collates network information, analyzes the information, determines whether it is invaded or attacked by someone using a certain method, and deals with this special situation.

2.2. AI and DL. AI is a new technical science that researches and develops theories, methods, technologies, and application systems for simulating, extending, and expanding human intelligence. As part of computer science, the purpose of AI technology is generating a way to deal with related problems in a manner similar to human intelligence. The main application areas include robotics, language recognition, image recognition, and natural language processing. AI can simulate the information processing of human consciousness and thinking, while at the beginning, AI systems can only complete fixed tasks assigned by humans. If AI systems are to be used to perform more intelligent tasks, they will need to learn from different scenarios in the same way that humans learn. After many training tasks, ML can extract data features and calculate the results with relevant algorithms [21]. Feature extraction is one of the problems often encountered in ML implementation of AI, and DL can solve this problem. DL is mainly adopted for automatic data extraction by deep combination of simple features.

DL is a way to learn the internal rules and represent levels of sample data. Such research has a good performance in analyzing words, images, and sounds, so that the established model can analyze problems like human. Compared with traditional ML algorithm, DL algorithm has more advantages in model building and feature data extraction. With the development of DL, many problems in the development of AI have been effectively dealt with [22]. While AI gives machines intelligence, ML uses algorithms to analyze data and perform specific tasks. DL optimizes ML's earlier algorithm and is a better technique. The fusion of AI technology and wireless network is in line with the trend of the development of the times, and the fusion of the two also has technical rationality. With the complexity of wireless data information, the data generated under wireless network becomes more and more heterogeneous. Therefore, relevant information needs to be collected from the source. These data have different formats and complex correlation. AI technology can better obtain and analyze these data, improving the effectiveness and feasibility of data acquisition. This experiment is conducted to explore the feasibility and effectiveness of the fusion of AI technology and wireless network.

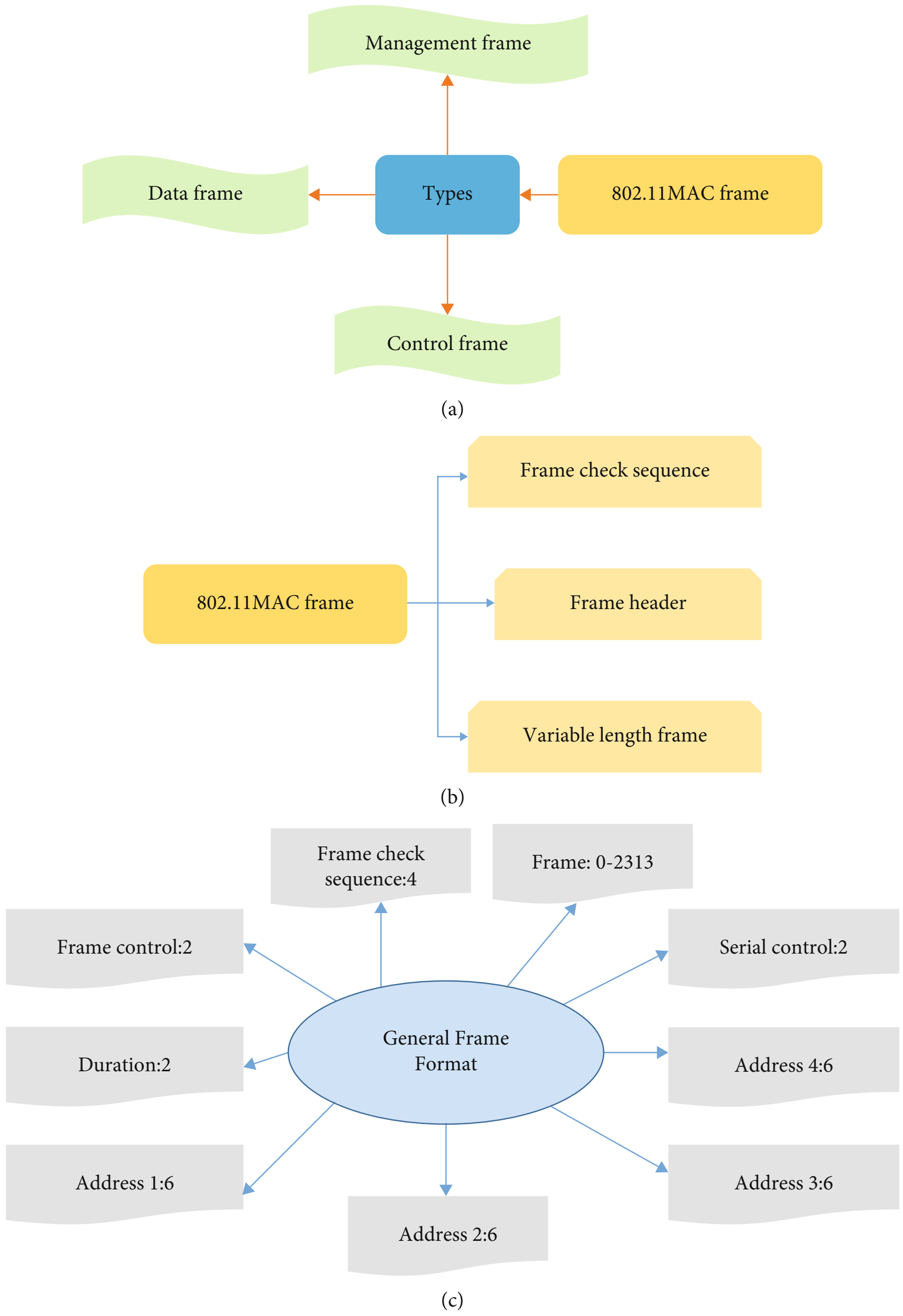


Figure 2: Diagram of WLAN composition types. (a) 802.11MAC frame types. (b) Composition of the frame. (c) Framework of general frame format.

2.3. Back Propagation (BP) Neural Network, RNN, and Their Derivatives. In the classical neural networks, the main learning methods of BP neural network are forward propagation and back propagation [23]. In the BP neural network, the generally used activation function is the sigmoid function, which can convert the output of a hidden layer into a non-negative value. It is shown in the following.

$$f(x) = \frac{1}{1 + e^{-x}}. \tag{1}$$

In the forward propagation process of BP neural network, the k-th input sample and output are as equation (2). The input and output of hidden layer and output layer neurons are expressed as equation (3), and the error function is defined as equation (4).

$$\begin{aligned} x(k) &= (x_1(k), x_2(k), \cdots, x_n(k)), \\ d_o(k) &= (d_1(k), d_2(k), \cdots, d_n(k)), \end{aligned} \tag{2}$$

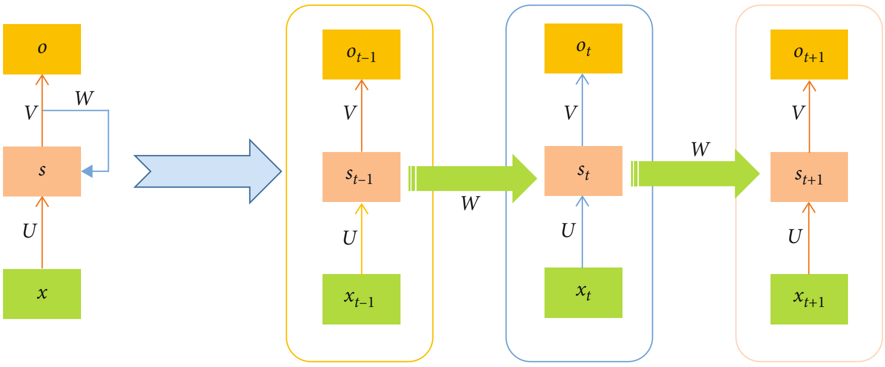


FIGURE 3: Structure diagram of RNN.

$$\begin{aligned}
hi_h(k) &= \sum_{i=1}^{n} w_{ih}x_i(k) - b_h, && h = (1, 2 \cdots, p),\\
ho_h(k) &= f(hi_h(k)), && h = (1, 2 \cdots, p),\\
yi_n(k) &= \sum_{h=1}^{p} w_{ho}ho_h(k) - b_o, && o = (1, 2 \cdots, p),\\
yo_o(k) &= f(yi_o(k)), && o = (1, 2 \cdots, p),
\end{aligned} \tag{3}$$

$$e = \frac{1}{2}\sum_{o=1}^{q} (d_0(k) - yo_o(k))^2, \tag{4}$$

$$\frac{\partial e}{\partial w_{ho}} = \frac{\partial e}{\partial yi_o}\frac{\partial yi_o}{\partial w_{ho}}, \tag{5}$$

$$\frac{\partial yi_o(k)}{\partial w_{ho}} = \frac{\partial\left(\sum_h^p w_{ho}ho_h(k) - b_o\right)}{\partial w_{ho}} = ho_h(k), \tag{6}$$

$$\begin{aligned}
\frac{\partial e}{\partial yi_o} &= \frac{\partial\left(1/2\sum_{o=1}^{q}(d_o(k) - yo_o(k))\right)^2}{\partial yi_o}\\
&= \partial(d_o(k) - yo_o(k))yo_o(k)\\
&= -(d_o(k) - yo_o(k))f(yi_o(k)) = \delta_o(k),
\end{aligned} \tag{7}$$

where ω is the weights, b is the threshold, e is the error function, $ho_h(k)$ is the output of the hidden layer on the h-th node, and $yo_o(k)$ is the output of the output layer on the n -th node. The training result is measured by the error function, and the weights must be corrected to reduce the error function value. The smaller the error function value the better, as shown in equation (8). After correction of the error function, the connection weight is updated and the threshold change equation is worked out like equation (9). The final global error calculation equation is expressed as equation (10).

$$\begin{gathered}
\frac{\partial e}{\partial hi_h(k)} = \frac{\partial\left(1/2\sum_{o=1}^{q}(d_o(k) - yo_o(k))^2\right)}{\partial h0_h(k)}\frac{\partial ho_h(k)}{\partial hi_h(k)},\\
\frac{\partial e}{\partial hi_h(k)} = \frac{\partial\left(1/2\sum_{o=q}^{q}(d_o(k) - f(yi_o(k)))^2\right)}{\partial ho_h(k)}\frac{\partial ho_h(k)}{\partial hi_h(k)},\\
\frac{\partial e}{\partial hi_h(k)} = \frac{\partial\left(1/2\sum_{n=1}^{q}\left(\left(d_o(k) - f\left(\sum_{h=1}^{p} w_{ho}ho_h(k) - b_o\right)^2\right)\right.\right.}{\partial ho_h(k)}\frac{\partial ho_h(k)}{\partial hi_h(k)},\\
\frac{\partial e}{\partial hi_h(k)} = -\sum_{o=1}^{q}(d_o(k) - yo_o(k))f'(yi_o(k))w_{ho}\frac{\partial ho_h(k)}{\partial hi_h(k)},\\
\frac{\partial e}{\partial hi_h(k)} = -\left(\sum_{o=1}^{q}(d_o(k)w_{ho})f'(hi_h(k))\right.\\
\frac{\partial e}{\partial hi_h(k)} = \delta_h(k),
\end{gathered} \tag{8}$$

$$\begin{gathered}
\Delta w_{ho}(k) = -\eta\frac{\partial e}{\partial w_{ho}} = \eta\delta_o(k)ho_h(k),\\
w_{ho}^{N+1} = w_{ho}^{N} + \eta\delta_o(k)ho_h(k),\\
\Delta b_o(k) = \eta * \delta_o(k),\\
\Delta b_h(k) = \eta * \delta_h(k),
\end{gathered} \tag{9}$$

$$E = \frac{1}{2m}\sum_{k=1}^{m}\sum_{o=1}^{q}(d_o(k) - y_o(k))^2, \tag{10}$$

where w_{ho} is the connection weight and η is the learning rate. If the final error of the BP neural network reaches the expected value, or the training reaches the maximum set number of times, the training will be stopped. If the expected value is not reached at last, the next round of training will be performed. The RNN is a neural network for classification tasks, in which the input is time series data. The neurons in the network strictly follow the time change, and the specific structure diagram is shown in Figure 3.

x is the input layer, s is the hidden layer, U is the weight matrix between the input layer and the hidden layer, o is the output layer, and V is the weight matrix between the hidden layer and the output layer. The value of s is determined by the current input and the previous hidden layer. Usually, the unit state of RNN at time t and the RNN output node are defined as the linear functions in

$$h_{(t)} = g\left(s_{(t-1)}, x_{(t)}, W, V\right),$$
$$o_{(t)} = g(Vs_t) = vh_{(t)} + c. \tag{11}$$

h stands for the system state of RNN, g is the activation function, and c and v are the weight coefficients. The state of each unit of the RNN is affected by the state of the current moment and the previous moment, and the cyclic unit of the next moment is constrained by the output of the previous moment. The overall connection is carried out at last. The prediction model is constructed through the input and output of RNN, which is expressed as equation (12); the network output mode of RNN is as equation (13).

$$h^{(t)} = f\left(uh^{(t-1)} + wX^{(t)} + b\right),$$
$$h^{(t)} = f\left(uo^{(t-1)} + wX^{(t)} + b\right), \tag{12}$$
$$h^{(t)} = f\left(uX^{(t-1)} + wh^{(t-1)} + Ry^{(t-1)}\right),$$

$$o_t = g(V\mathrm{s}_t),$$
$$o_t = Vf(Ux_t + Wf(Ux_{t-1} + W\mathrm{s}_{t-2})),$$
$$o_t = Vf(Ux_t + Wf(Ux_{t-1} + Wf(Ux_{t-2} + W\mathrm{s}_{t-3}))),$$
$$o_t = Vf(Ux_t + Wf(Ux_{t-1} + Wf(Ux_{t-2} + Wf(Ux_{t-3}+\cdots)))). \tag{13}$$

LSTM is a kind of temporal recurrent neural network, which is specially designed to solve the long-term dependence problem existing in general RNN. All RNNs have a chain form of repeating neural network modules. LSTM neural network, as a derivative of RNN, has a more complex internal structure, and the control and training of the model are realized by adding gate structure [24]. LSTM is a type of neural network that contains LSTM blocks or other neural networks. It is also described as a structure with intelligent network units that can remember values of varying lengths of time. There is a gate in the block that determines whether the input is important enough to be remembered and whether it can be output. Gate structure is mainly composed of input gate, output gate, and forget gate. LSTM neural network has cell storage structure, but RNN does not. LSTM neural network can process the data that needs to be remembered and determine the forgotten information by activation function. These results are output through the output gate and the forward propagation is shown in

$$f_t = \sigma\left(W_f * [h_{t-1}, x_t] + b_f\right),$$
$$i_t = \sigma(W_i * [h_{t-1}, x_t] + b_i),$$
$$o_t = \sigma(W_o * [h_{t-1}, x_t] + b_o), \tag{14}$$
$$C_t \approx \tanh\,(W_C * [h_{t-1}, x_t] + b_C),$$

where x_t is the current input, h_{t-1} is the unit information at the last moment, and f_t is the forgetting function. The back propagation of LSTM neural network is more complicated, and the chain derivation of the LSTM is described as equation (15). $l(t)$ is the hypothetical loss function, $h(t)$ is the output, $y(t)$ is the true label, L is the back propagation loss, and T is the entire time series.

$$l(t) = f(h(t), y(t))) = \|h(t) - y(t)\|^2,$$
$$L = \sum_{t=1}^{T} l(t), \tag{15}$$
$$\frac{dL}{dw} = \sum_{t=1}^{T}\sum_{i=1}^{M}\frac{dL}{dh_i(t)}\frac{dh_i(t)}{dw} = \sum_{s=1}^{T}\frac{dl(s)}{dh_i(t)} = \frac{dL(s)}{dh_i(t)}.$$

GRU is a highly effective variant of LSTM network. Compared with the structure of LSTM, the structure of GRU model is simpler and has a good effect. Since GRU is a variant of LSTM, it can also solve the long dependency problem in RNN networks. Moreover, GRU requires less computation and is concise [25]. The essence of GRU is also a special RNN, in which the activation function in the RNN is replaced by a gated cyclic neural network structure. Three gate functions are introduced in LSTM, including input gate, forget gate, and output gate, to control input value, memory value, and output value. In the GRU model, there are only two gates, namely, the update gate and the reset gate. Based on LSTM neural network, the input gate and the forget gate are combined into an update gate, which reduces the training parameters and improves the convergence speed [26]. The status update of GRU is shown in

$$r_t = \sigma(U_r * x_t + W_r * h_{t-1} + b_r),$$
$$z_t = \sigma(U_z * x_t + W_z * h_{t-1} + b_z),$$
$$c_t = \varphi(U_c * x_t + W_c(h_{t-1} \times r_t) + b_c), \tag{16}$$
$$h_t = z_t \times h_{t-1} + (1 - z_t) \times c_t.$$

2.4. Construction of Intrusion Detection Model of WLAN Information Management System under RNN. An interception device is designed to generate a traffic sequence describing the LAN. The interceptor receives air interface data of the target network and uses the collected data in the form of message authentication code (MAC) frames to construct a traffic sequence dataset of the WLAN. Intrusion detection of WLAN information management system under RNN realizes WLAN status classification and identification by associating traffic sequence with status information [27]. The specific model structure of classification prediction is shown in Figure 4. The collected data is entered into the RNN model and classified output, which is finally taken as the output result of the model.

The input layer of the entire neural network is the sequence embedding layer, and the traffic sequences of WLAN are divided into subsequences and transmitted to the hidden layer in order. The expression results of the RNN hidden layer enter the classification representation

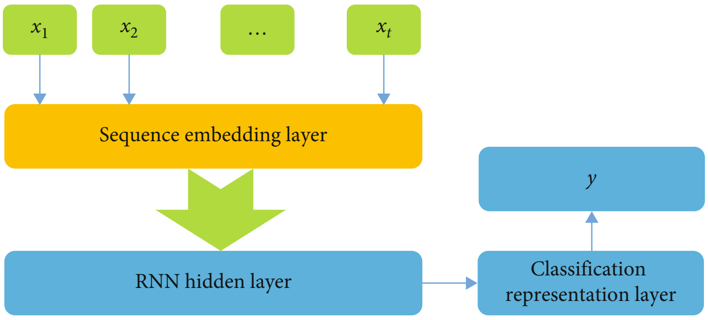


FIGURE 4: Structure diagram of specific classification prediction model.

layer, which is represented as category information by the classification representation layer [28]. For such a multiclassification, the prediction results of the RNN are processed using the softmax unit, as expressed in

$$\begin{aligned} z &= W^T h + b, \\ \operatorname{softmax}(z)_i &= \frac{\exp\,(z_i)}{\sum_j z_j}, \\ \log\ \operatorname{softmax}(z)_i &= z_i - \log \sum_j \exp\left(z_j\right), \end{aligned} \tag{17}$$

where z is the predicted log probability, W is the weight matrix, h is the output, b is the bias matrix, and i and j are the category subscripts. RNN unit is established according to the LSRM neural network and the GRU structure, and different models are constructed. The performance of different models is compared through experiments, to determine the best detection method. The methods of the two classification prediction models are as follows. The objective loss function is obtained using the categorical cross-entropy, as expressed in

$$J = -\sum_{i=1}^{n} \sum_{j=1}^{m} \hat{y}_{ij} \log y_{ij}, \tag{18}$$

where J is the original objective function, $\hat{y}_{ij}$ is the predicted probability distribution, i is the number of samples, j is the number of classifications, and y is the sample distribution. As the L^2 weight decay and dropout regularization are applied to constrain the learning process, the generalization error in the learning process can be reduced, and the model has a good generalization effect [29]. The L^2 regularization strategy selects 10^{-6} weight decay, and the objective function is modified as equation (19). The process of dropout regularization in the LSTM neural network model is shown as equation (20).

$$\tilde{J}(W\,; x, y) = J(W\,; x, y) + \frac{\alpha}{2} W^T W, \tag{19}$$

$$\begin{aligned} a_t &= \varphi(U_a * D(x_t) + W_a * h_{t-1} + b_a), \\ i_t &= \sigma(U_i * D(x_t) + W_i * h_{t-1} + b_i), \\ f_t &= \sigma\left(U_f * D(x_t) + W_f * h_{t-1} + b_f\right), \\ o_t &= \sigma(U_o * D(x_t) + W_o * h_{t-1} + b_o), \\ c_t &= a_t \times i_t + c_{t-1} \times f_t, \\ h_t &= \varphi(c_t) \times o_t, \end{aligned} \tag{20}$$

where $J^{\sim}$ is the objective function after the regularization strategy, α is the weight decay parameter, W is the weight parameter affected by regularization, and D is the dropout operation. The Adam random optimization algorithm is adopted as the optimization algorithm. The early stopping method is used to terminate the model learning process in advance, to ensure the best generalization performance of the model.

2.5. Experiment and Evaluation Methods. The logistic regression classifier is selected for comparison of LSTM neural network model and GRU model. The area under curve (AUC) indicator is adopted as the main evaluation criterion, to evaluate the generalization ability of the classifier. For a positive and negative sample pair D (D^+, D^-), true positive rate (TPR), and false positive rate (FPR), AUC is expressed as

$$\begin{aligned} \mathrm{TPR}_D &= \frac{\mathrm{TP}_\mathrm{D}}{\mathrm{TP}_D + \mathrm{FN}_D}, \\ \mathrm{FPR}_D &= \frac{\mathrm{FP}_D}{\mathrm{TN}_D + \mathrm{FP}_D}, \\ \mathrm{AUC} &= \frac{1}{p+n} \sum_{x^+ \in D^+} \sum_{x^- \in D^-} \left(1_{\{\mathrm{true}\}}\left(f(x^+) > f(x^-)\right) \right. \\ &\quad \left. - \frac{1}{2} 1_{\{\mathrm{true}\}}\left(f(x^+) = f(x^-)\right)\right), \end{aligned} \tag{21}$$

where TP_D (true positive) is the number of true positive examples, FN_D (false negative) is the number of false negative examples, TN_D (true negative) is the number of true negative examples, FP_D (false positive) is the number of false positive examples, p is the number of positive examples, n is the number of negative examples, $1_{\{\mathrm{true}\}}$ is the indicator function, and f is the classifier. For category A, TP_A is the number of samples correctly classified into category A, FP_A is the number

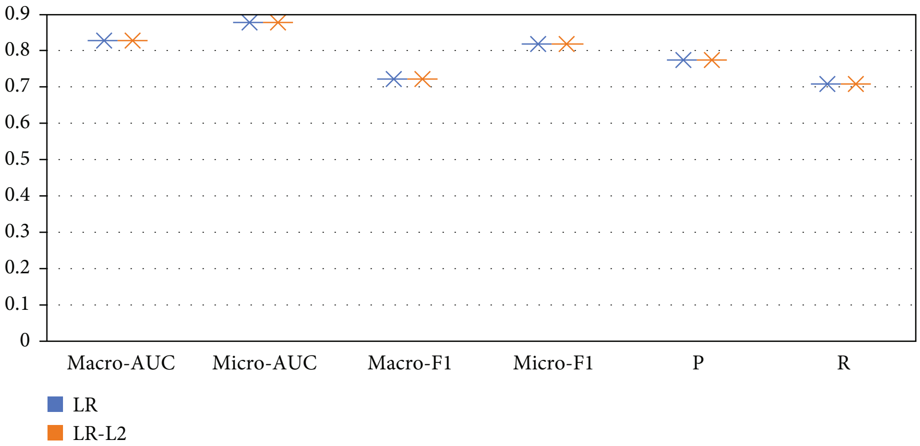
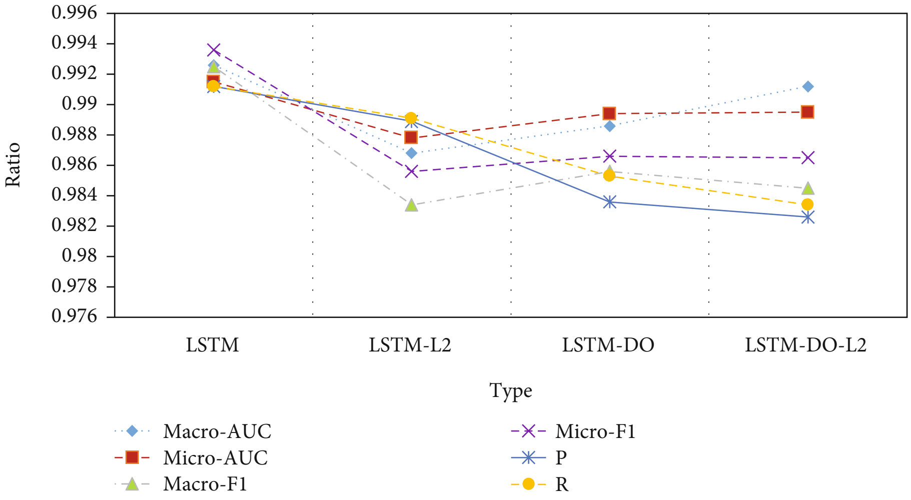
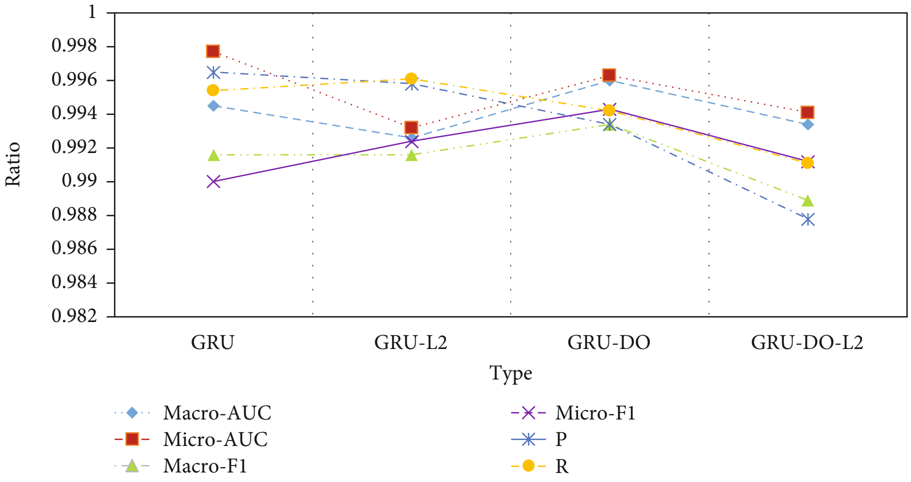


Figure 5: Comparison of the experimental results of the LR model.



(a)



(b)

Figure 6: Comparison of LSTM and GRU models. (a) Comparison of experimental results of LSTM model. (b) Comparison of results of GRU model.

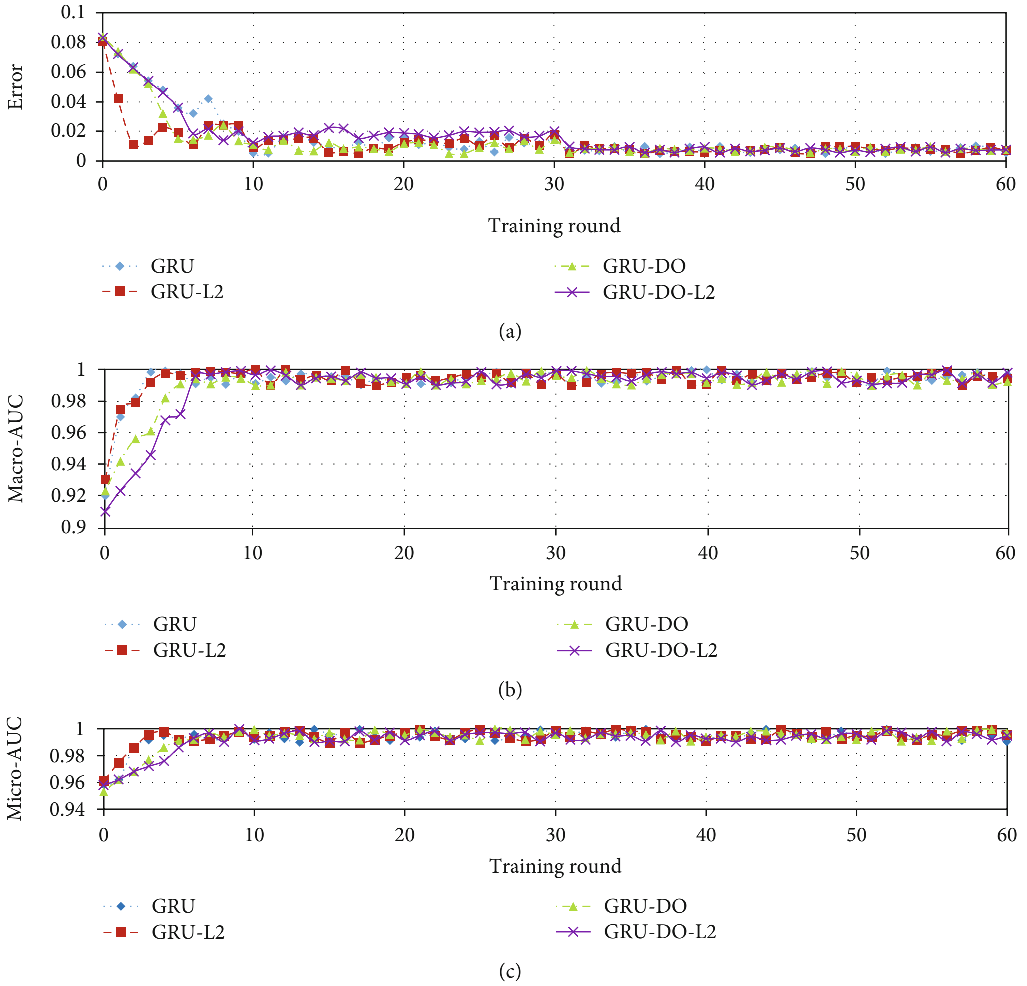


Figure 7: Result comparison of the simulation experiment of GRU model. (a) Comparison of the error of GRU model. (b) Comparison of macro-AUC of GRU model. (c) Comparison of micro-AUC of GRU model.

of samples incorrectly classified into category A, and FN_A is the number of samples incorrectly classified into other categories. In equation (22), R_A is the recall ratio, and P_A is the precision ratio.

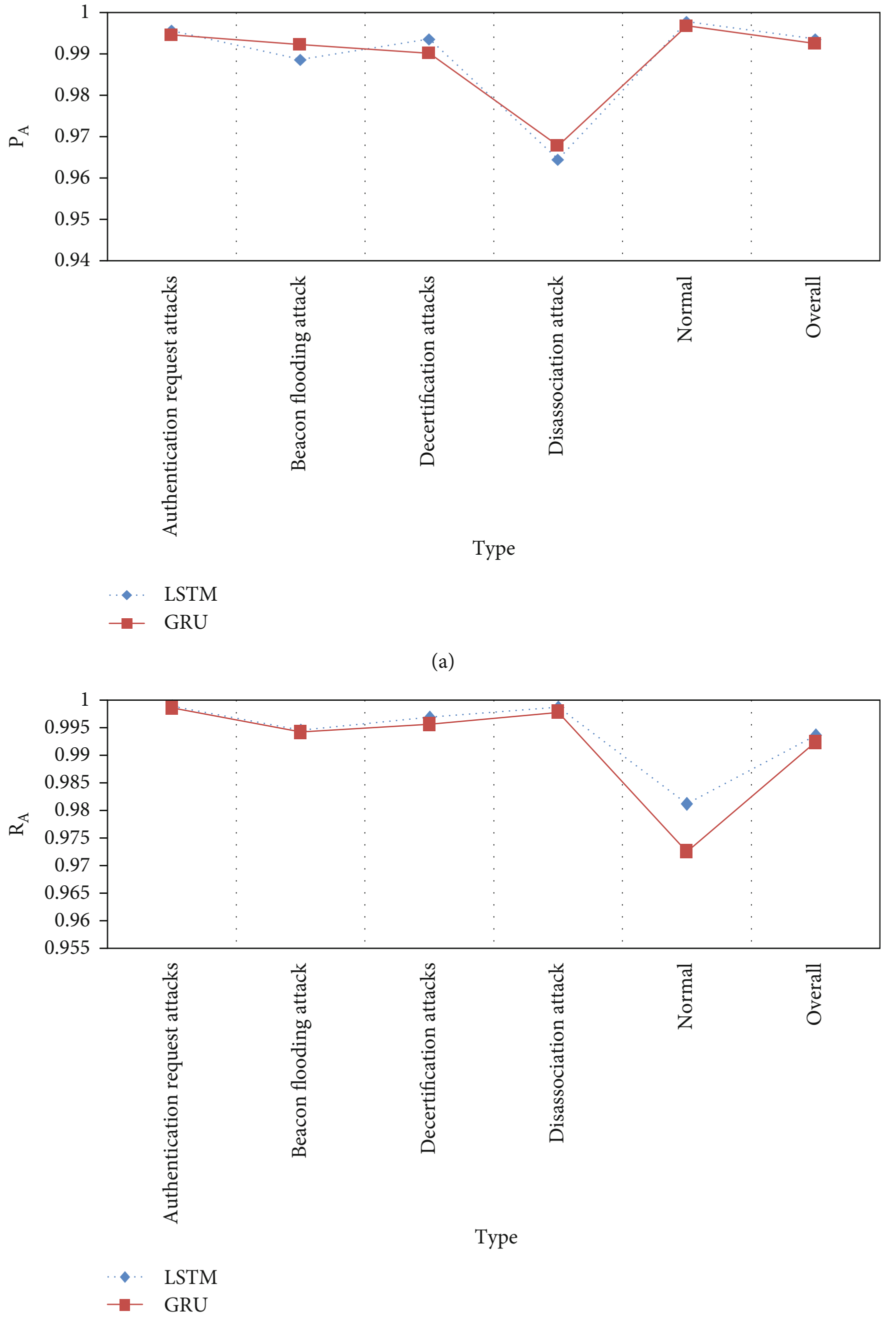
$$P_A = \frac{\mathrm{TP}_A}{\mathrm{TP}_A + \mathrm{FP}_A},$$
$$R_A = \frac{\mathrm{TP}_A}{\mathrm{TP}_A + \mathrm{FN}_A}, \qquad (22)$$
$$F_1 = \frac{2pr}{p + r}.$$

The intrusion detection system is established under the RNN, to construct the security protection system of the computer information management system, realize the intrusion detection for WLAN, and improve the security performance of the system. The front-end model is constructed by using the cloud, terminal, and control site structure. The cloud is arranged in the server, the control site is implemented by a web page, and the terminal involves in and monitors WLAN with a smart device. Positive data collection and user management are carried out in the cloud. Intrusion detection results and user interaction instructions are directly presented to users at the control site. The terminal has a monitoring module, which is for data and results processing and communication.

3. Results and Discussion

3.1. Comparison of Experimental Results of Various Intrusion Detection Models under Neural Networks. Figure 5 displays the comparison chart of the experimental results of the logical regression (LR) model.

Figure 5 shows the results of LR model and the LR model applied with the L^2 regularization strategy. The micro-AUC and macro-AUC indicators of the LR model reach 0.8854 and 0.8324, respectively, while those of the LR-L^2 model reach 0.8836 and 0.8315, respectively. It is suggested that the LR model has a better generalization ability. The macro F1 and micro F1 of the LR model are 0.7256 and 0.8236, respectively; and those of the LR-L^2 model are 0.7214 and 0.8211, respectively. The classification accuracy of the LR model is better.



(a)

(b)

Figure 8: Experimental result comparisons of LSTM and GRU models. (a) Comparison of precision ratio. (b) Comparison of recall ratio.

Figure 6 shows the comparison of the experimental results between the LSTM neural network model and the GRU model.

It can be found from Figure 6(a) that in the LSTM model, the micro-AUC and macro-AUC of reach 0.9915 and 0.9926, respectively. In the other three models, the LSTM model applied with the dropout regularization strategy gives the best AUC indictors, as the macro-AUC and micro-AUC of the long short-term memory-dropout (LSTM-DO) model are 0.9886 and 0.9894, respectively. The LSTM neural network model without regularization strategy generalizes better. Moreover, the macro F1 and micro F1 of the LSTM model are computed as 0.9925 and 0.9936, respectively, and its classification accuracy is also the highest. In each model of GRU in Figure 6(b), the macro F1 and micro F1 of GRU are 0.9916 and 0.9902, respectively, which also has a high classification accuracy. As all models are compared, the LSTM neural network model is presented to be the best, and the performance is improved by about 17% compared to micro F1 of the LR model.

3.2. Result Analysis of Intrusion Detection Classification Models under Neural Network Models. Figure 7 shows the learning curves of LSTM neural network model and GRU prediction model.

In Figure 7, GRU errors in Figure 7(a) decrease continuously with the increase of training period, and there are differences in errors among different methods. In Figure 7(b), the macroscopic AUC values of different GRU models fluctuate greatly, and the value of GRU-DO-L2 is relatively low in the initial stage. In Figure 7(c), the difference of micro-AUC of different GRU models is small. Therefore, when the model does not adopt the regularization strategy, the curve fluctuation is large, and after the regularization strategy is adopted, the fluctuation decreases. As the number of training rounds increases, the generalization performance of the regularization model improves and the error decreases. In the absence of regularization strategy, the generalization ability of the model decreases, but the error increases. However, the model using regularization strategy has little improvement in classification performance, so there is no need to use regularization strategy, and the early stop method can be adopted.

Figure 8 displays a detailed comparison of the experimental results of the LSTM and GRU models.

It can be discovered from Figure 8 that both LSTM and GRU have high performance in the comparisons of the precision ratio and recall ratio. Although the LSTM model has better classification performance than the GRU model, the performance gap is not large. The convergence speed of the GRU model is faster than that of the LSTM model. The GRU model is simpler and has fewer parameters, so the calculation amount is smaller and the speed is faster. Therefore, it is better to choose GRU as the classification prediction model in intrusion detection, and it can be applied to some devices with limited computing power.

4. Conclusions

To address the security system problem of computer information management system, an AI-based wireless network front-end model is proposed. The intrusion detection system is constructed in the computer information management system, which improves the security performance of the computer information management system. Firstly, according to the different structure and characteristics of neural network, intrusion detection models under LSTM and GRU are established, respectively. Experiments show that the generalization ability of the model can be further improved by using L2 weight attenuation and dropout regularization strategies, but the performance improvement is not notable. Therefore, the regularization strategy can be replaced by the early stop method. Compared with the existing classification models, the classification accuracy of the neural network model is improved by about 17%, which can achieve good detection performance. Finally, after LSTM model is compared with GRU model, GRU model with less computation is selected. However, there are still some shortcomings in the research, the dataset and algorithm should be further optimized, and the accuracy of the design method for intrusion detection should be improved. The subsequent work will further improve the performance of the design method combined with wireless network and further applied to the actual computer information management research.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Qiqihar Science and Technology Bureau Directive Project, research on practice of university smart cloud classroom service platform construction based on mobile Internet era (Project No. GYGG-201923).

References

[1] I. Muslihah and S. A. Nastura, "Transaction processing system analysis using the distribution management system (DMS) nexsoft distribution 6 (ND6)," *International Journal of Computer and Information System (IJCIS)*, vol. 1, no. 1, pp. 31–34, 2020.

[2] Y. S. Lee and Y. C. Mun, "Design and implementation of data processing middleware and management system for IoT based services," *Journal of the Korea Society of Computer and Information*, vol. 24, no. 2, pp. 95–101, 2019.

[3] R. Magán-Carrión, D. Urda, I. Díaz-Cano, and B. Dorronsoro, "Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches," *Applied Sciences*, vol. 10, no. 5, p. 1775, 2020.

[4] A. Verma and V. Ranga, "Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1571–1594, 2019.

[5] N. Thapa, Z. Liu, D. B. Kc, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," *Future Internet*, vol. 12, no. 10, p. 167, 2020.

[6] H. Choi, M. Kim, G. Lee, and W. Kim, "Unsupervised learning approach for network intrusion detection system using autoencoders," *The Journal of Supercomputing*, vol. 75, no. 9, pp. 5597–5621, 2019.

[7] H. Musafer, A. Abuzneid, M. Faezipour, and A. Mahmood, "An enhanced design of sparse autoencoder for latent features extraction based on trigonometric simplexes for network intrusion detection systems," *Electronics*, vol. 9, no. 2, p. 259, 2020.

[8] T. T. H. Le, Y. Kim, and H. Kim, "Network intrusion detection based on novel feature selection model and various recurrent neural networks," *Applied Sciences*, vol. 9, no. 7, p. 1392, 2019.

[9] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, "Wireless network intelligence at the edge," *Proceedings of the IEEE*, vol. 107, no. 11, pp. 2204–2239, 2019.

[10] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[11] M. Shahidul Islam, M. T. Islam, A. F. Almutairi, G. K. Beng, N. Misran, and N. Amin, "Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system," *Applied Sciences*, vol. 9, no. 9, p. 1884, 2019.

[12] Y. O. Halchenko, K. Meyer, B. Poldrack et al., "DataLad: distributed system for joint management of code, data, and their relationship," *Journal of Open Source Software*, vol. 6, no. 63, p. 3262, 2021.

[13] E. Basar, "Media-based modulation for future wireless systems: a tutorial," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 160–166, 2019.

[14] H. Hashida, Y. Kawamoto, and N. Kato, "Efficient delay-based Internet-wide scanning method for IoT devices in wireless LAN," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1364–1374, 2019.

[15] N. Ma and M. Diao, "CoFi: coding-assisted file distribution over a wireless LAN," *Symmetry*, vol. 11, no. 1, p. 71, 2019.

[16] N. Egashira, K. Yano, J. Webber et al., "Prototype development of wireless LAN with multiband simultaneous transmission and its experiment," *IEICE Technical Report; IEICE Tech. Rep*, vol. 118, no. 474, pp. 175–180, 2019.

[17] I. L. Gaol and E. Ekadiansyah, "Penerapan Metode Hill Cipher Dan Caesar Cipher Pada Aplikasi Wireless Lan Chatting," *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer*, vol. 1, no. 1, pp. 1087–1100, 2020.

[18] D. M. Steininger, "Linking information systems and entrepreneurship: a review and agenda for IT-associated and digital entrepreneurship research," *Information Systems Journal*, vol. 29, no. 2, pp. 363–407, 2019.

[19] M. Gebre-Mariam and B. Bygstad, "Digitalization mechanisms of health management information systems in developing countries," *Information and Organization*, vol. 29, no. 1, pp. 1–22, 2019.

[20] Y. H. S. Al-Mamary, M. M. Al-Nashmi, A. Shamsuddin, and M. Abdulrab, "Development of an integrated model for successful adoption of management information systems in Yemeni telecommunication organizations," *International Journal of Scientific & Technology Research*, vol. 8, no. 11, pp. 3912–3939, 2019.

[21] A. Bashar, "Survey on evolving deep learning neural network architectures," *Journal of Artificial Intelligence*, vol. 2019, no. 2, pp. 73–82, 2019.

[22] M. T. Pandian, S. N. Prasad, and M. Sharma, "Correction to: a detailed evolutionary scrutiny of PEIS with GPS fleet tracker and AOMDV-SAPTV based on throughput, delay, accuracy, error rate, and success rate," *Wireless Personal Communications*, vol. 121, no. 4, pp. 2653–2653, 2021.

[23] A. Saxe, S. Nelli, and C. Summerfield, "If deep learning is the answer, what is the question?," *Nature Reviews Neuroscience*, vol. 22, no. 1, pp. 55–67, 2021.

[24] K. Cui and X. Jing, "Research on prediction model of geotechnical parameters based on BP neural network," *Neural Computing and Applications*, vol. 31, no. 12, pp. 8205–8215, 2019.

[25] A. Sagheer and M. Kotb, "Unsupervised pre-training of a deep LSTM-based stacked autoencoder for multivariate time series forecasting problems," *Scientific Reports*, vol. 9, no. 1, pp. 1–16, 2019.

[26] B. Fu, W. Yuan, X. Cui et al., "Correlation analysis and augmentation of samples for a bidirectional gate recurrent unit network for the remaining useful life prediction of bearings," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 7989–8001, 2020.

[27] E. Urtnasan, J. U. Park, and K. J. Lee, "Automatic detection of sleep-disordered breathing events using recurrent neural networks from an electrocardiogram signal," *Neural Computing and Applications*, vol. 32, no. 9, pp. 4733–4742, 2020.

[28] M. T. Pandian and R. Sukumar, "Performance enhancement with improved security an approach for formulating RFID as an itinerary in promulgating succour for object detection," *Wireless Personal Communications*, vol. 109, no. 2, pp. 797–811, 2019.

[29] M. T. Pandian and R. Sukumar, "RFID: an appraisal of malevolent attacks on RFID security system and its resurgence," in *2013 IEEE International Conference in MOOC, Innovation and Technology in Education (MITE)*, pp. 17–20, Jaipur, India, 2013.