Hindawi
Journal of Control Science and Engineering
Volume 2023, Article ID 9759028, 1 page
https://doi.org/10.1155/2023/9759028

Retraction

Retracted: Application of Artificial Intelligence Technology in Computer Network Security Communication

Journal of Control Science and Engineering

Received 15 August 2023; Accepted 15 August 2023; Published 16 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] F. Li, "Application of Artificial Intelligence Technology in Computer Network Security Communication," *Journal of Control Science and Engineering*, vol. 2022, Article ID 9785880, 6 pages, 2022.

Hindawi
Journal of Control Science and Engineering
Volume 2022, Article ID 9785880, 6 pages
https://doi.org/10.1155/2022/9785880

Research Article

Application of Artificial Intelligence Technology in Computer Network Security Communication

Fulin Li

Guangdong University of Science and Technology, Dongguan, Guangdong 523000, China

Correspondence should be addressed to Fulin Li; 1512440331@st.usst.edu.cn

Received 19 May 2022; Revised 22 June 2022; Accepted 3 July 2022; Published 21 July 2022

Academic Editor: Jackrit Suthakorn

In order to cope with the frequent challenges of network security issues, a method of applying artificial intelligence technology to computer network security communication is proposed. First, within the framework of computer network communication, an intelligent protocol reverse analysis method is proposed. By converting the protocol into an image and establishing a convolutional neural network model, artificial intelligence technology is used to map the data to the protocol result. Finally, use the model to test the test data to adjust the model parameters and optimize the model as much as possible. The experimental results show that compared with the test model, the results obtained after training with the deep convolutional neural network model in this paper have increased the accuracy by 2.4%, reduced the loss by 38.2%, and reduced the running time by 42 times. The correctness and superiority of the algorithm and model are verified.

1. Introduction

With the development of 5G, 6G technology has also begun to be studied. The Internet has spread all over the world and has become a part of contemporary life. As one of the future development directions, various IoT devices such as smart homes are developing even faster. Communication between different IoT devices [1], collaborative processing, and information transmission are all realized by sending data packets on the network.

In recent years, the frequency of botnets, darknets, illegal transactions, and network intrusions has gradually increased. As a bridge of communication between these means, the analysis of protocols can help to seize the lifeblood of network security and ensure network security. Network protocols can be divided into two categories according to their protocol format, process openness, and other conditions: public protocols and nonpublic protocols. Public protocols refer to those protocols that disclose the protocol format and content, and are generally widely used by people. For example, common network protocols such as TCP, UDP, DNS, and SMTP. The nonpublic protocol refers to the format set for some needs, which is usually a unique and untouched protocol type, so it is also often referred to as a private network protocol and an unknown protocol format. However, according to the current research, the traditional protocol reverse analysis method has low processing efficiency for the obtained binary bit stream data set. The method is relatively simple and has certain limitations, which cannot meet the needs of secure communication in today's network systems. In addition, common protocol reverse analysis tools can basically only parse common protocol types. For that kind of unknown and unrecognized data packets, due to the lack of corresponding prior knowledge, are very difficult to analyze.

Although the reverse analysis technology of the known protocol format [2] already exists, the reverse analysis of the unknown protocol format, the related work is still less, or the limitations are relatively large. Therefore, the main research of this paper is to apply artificial intelligence technology to unknown network protocols for feature extraction and then perform intelligent reverse analysis. Figure 1 lists the basic applications of artificial intelligence technology in the field of computer network information security.

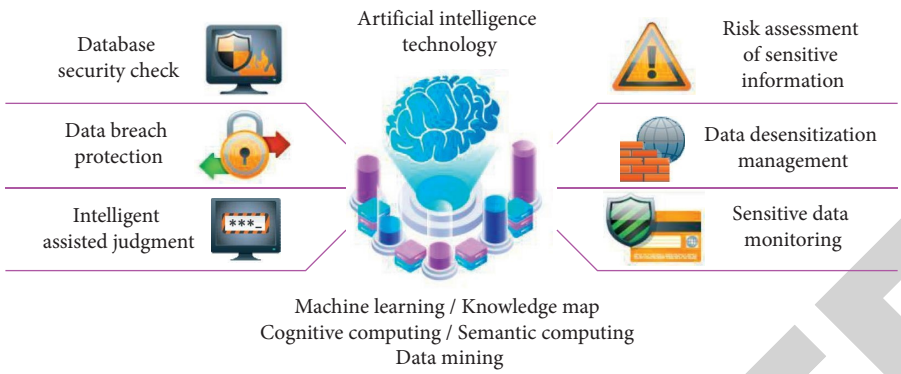

Figure 1: Application of artificial intelligence technology in the field of computer network information security.

2. Literature Review

Netzob is a semiautomatic method proposed by Wang et al. to automate some of the reasoning process of the protocol structure. Netzob focuses on automating the reasoning process and does not involve the work of experts. A detailed lexical model and method are designed for this purpose. Netzob uses an unweighted method of arithmetic mean for group method processing. A cluster message is defined as a symbol. A symbol refers to a group of messages that have the same format and role from the perspective of the protocol [3]. Alireza et al. used the Needleman Wunsch algorithm for each symbol in the network to achieve ordering of common strings. Generic strings are defined as static fields and alternative fields for the rest of the message. A field refers to a set of tokens that have a common meaning from a protocol perspective. A symbol consists of several fields, each of which can accept one or more values [4].

AutoReEngine is a method proposed by Dinh et al. AutoReEngine receives network traffic of a single protocol as input. AutoReEngine mainly includes four steps: data preprocessing, protocol keyword extraction, message format extraction, and state machine inference. In the data preprocessing step, the input traffic is divided into a flow and the packets in the flow are reassembled into messages. Protocol keyword extraction is mainly carried out in two steps [5]. Liu and Yangjun proposed that in the first frequency string extraction step, the Apriori algorithm be used to input and extract message sequences from field format candidate keywords. At this time, the length-1 item in the Apriori algorithm consists of 1 byte, the transaction consists of each message sequence, and the support units include the session support rate (Rssr) and the site-specific session set support rate (Rset) [6]. Bistron and Piotrowski report that Rssr represents the proportion of candidate sequences that encompass the entire stream, and Rset represents the proportion of candidate sequences that encompass the entire site-specific session. A site-specific session refers to a group of streams with the same server. In other words, for item groups and candidate item groups that appear gradually from length-1 to length-K, determine Rsr and Rset, where frequently occurring item groups are not extracted according to the default Apriori algorithm. Two terms that satisfy both sets of threshold session support rate (Tssr) and threshold point specific session sets (Tsets) are simultaneously determined. Byte sequences containing the final set of all frequently extracted items are extracted and enclosing strings are determined for these byte sequences [7].

FieldHunter is a method proposed by Mathew, which receives network traffic of a single protocol as input-FieldHunter first receives network flow as input and divides the network flow into network messages. FieldHunter divides the unit of network message into TCP's PUSH flag and UDP's one packet. The syntax inference step first checks whether it is a text-based or binary-based protocol and performs the tokenization of the message differently in the message tokenization module. A key step of FieldHunter is semantic reasoning [8]. Misra heuristically finds fields corresponding to predefined meaning types in the semantic reasoning step, where six predefined meanings are used: message type, message length, host identifier, session identifier, transaction identifiers, and accumulators [9]. And Vollertsen et al. believe that the main way to judge whether a field corresponds to each type of meaning is to use completely different concepts for different field types in vertical analysis; that is, each field has statistical characteristics in different traces. For example, to derive fields corresponding to host identifiers, the system provides a field that always contains the corresponding unique value for each source IP address for different traces [10].

In recent years, protocol reverse engineering has achieved fruitful results in various fields. Especially in the field of network security, the emergence of automatic protocol reverse technology has brought dawn to network analysis. By studying network protocols, Dou et al. took reverse engineering as the entry point of protocol analysis, from the perspective of traffic syntax analysis and instruction timing analysis as protocol reverse analysis, but due to the wide research area, the research depth of the protocol is insufficient [11]. In the paper, Iwendi et al. proposed a reverse protocol analysis technology based on network traffic. By analyzing the characteristics of traffic syntax and instruction execution timing, the state machine analysis of the protocol was carried out, but the two lacked systematic analysis of the protocol[12]. This paper is different from the above. This paper mainly studies from the aspect of grammar, mainly conducts a reverse analysis of the feature information of the protocol grammar, and starts from

different angles and different algorithms to verify each other, so as to systematically analyze the protocol grammar intelligently.

3. Research Method

3.1. Feature Extraction Algorithm Based on Neural Network. A convolutional neural network (CNN) is a deep learning architecture that works in a similar way to how the human eye sees things and then feeds back. They have great potential for applications in image classification, natural language processing, image caption generators, etc. In the past period, CNN was unable to solve complex problems due to lack of computing power [13]. But with the advent of graphics processing units (GPUs) and their use in machine learning, CNNs have re-emerged and surpassed other architectures in computer vision tasks. CNN has attracted attention in many fields, and medical diagnosis is no exception. Image classification plays a key role in computer vision. It includes preprocessing image data, image segmentation, extracting key features, and classifying images into corresponding classes. Using CNN to classify images effectively and accurately, this technology can be applied to medical diagnosis, face recognition, security and other fields [14].

Since the convolutional neural network has a better effect on image processing, and the convolutional operation is required when using the convolutional neural network, the convolutional layer can only identify the image data of the matrix type. Therefore, it is necessary to convert the input data to an image. On the basis of data preprocessing, the protocol data is put together every 8 bits and converted into image data between 0–255. Each protocol will generate 40 image data between 0–255 [15]. A one-stage convolution Piotrowskial network consists of a convolutional layer and a max-pooling layer. The convolution kernel of the convolution layer is kernel_size, which includes the number of filters and strides. The input input_ranges of the first convolutional layer, a pool_size after the max-pooling layer. When the input data set of the neural network is small, it is easy to overfit, which makes the model fall into the local optimal solution and reduces the training effect of the model. This article uses the dropout function to prevent this from happening [16]. In order to make the model training faster and better solve complex function problems, the ReLU activation function is used here for processing. The ReLU activation function is shown in the following formula:

$$\mathrm{ReLU}(x) = \begin{Bmatrix} x, & \text{if } (x > 0) \\ 0, & \text{if } (x \le 0) \end{Bmatrix}. \quad (1)$$

The advantages of the ReLU activation function are: (1) when backpropagating, the gradient disappearance can be avoided. (2) Due to the particularity of the ReLU function, the output of the input on the left side of the X axis is 0, so the effect of some neurons disappears, thereby reducing the number of parameters in the network and alleviating the problem of overfitting. (3) Compared with the sigmoid activation function and the tanh activation function, the derivation is simple.

The sigmod function is an exponential function, which requires derivation during backpropagation, which is difficult to calculate. Using the ReLU function will cost less. The second section of the convolutional neural network is similar to the first section, and the size of the convolution kernel is still 3×3, but the number of convolution kernels here has been increased to 128. Then, through the regularization method of dropout, some redundant information is randomly deleted to prevent the model from overfitting, thereby improving the generalization ability of the model [17]. The result is then fed into the flatten layer. The flatten layer is used to "flatten" the input data, that is, to map the multidimensional input to one dimension, while the fully connected layer, the function of the fully connected layer, is to use a series of functions to calculate all the feature-extracted data sets and map each dataset to the corresponding label classification, so that the expected results are as close as possible to the actual results. The fully connected layer plays a classification role in the entire neural network layer. It just performs a matrix multiplication, which is equivalent to spatial transformation of the features and statistical extraction and integration of the previous information [18]. Then use the activation function to perform nonlinear mapping so that the data of this class corresponds to the result one-to-one. It can also change the dimensions without pressing, and can turn high-dimensional information into low-dimensional information, and at the same time, it can retain useful information. For the last layer of full connection, it is the explicit expression of the classification category. The fully connected layer consists of two parts. First, the data of the upper layer is flattened (Flatten) and then input into the fully connected network. The fully connected network has two layers. The first layer has 128 nodes, and the last layer has 8 nodes. The first layer of the fully connected network has 128 nodes, and the activation function is still the ReLU function. The last layer has 8 nodes, and the activation function is the Softmax function [19].

3.2. Model Training and Prediction. The process of model training using a neural network based on artificial intelligence technology is shown in Figure 2.

The cross-entropy loss function is used as the loss function for model training, and the stochastic gradient descent method is used to optimize the model. The initial learning rate is set to 0.1, and the indicator to measure the model is selected as accuracy. The amount of data selected during training is 64, and the loop is 100 times [20]. Use tensorboard as a callback function. Cross-entropy loss function The cross-entropy loss function is to reflect the effect of model training by calculating the difference between the actual output and the expected output of the model, and by continuously adjusting parameters and calculations, the value of the loss function is reduced, so that the actual value is closer to the expected value. The cross-entropy loss function is shown in the following formula[21]:

$$C = -\frac{1}{n}\sum_{x}[y \ln a + (1-y)\ln(1-a)]. \quad (2)$$

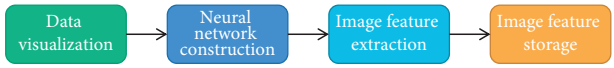

Figure 2: Neural network feature extraction process.

In the formula: y is the expected output of the model, a is the actual output of the model, n is the number of categories of the output, and x is the input of the model. The neural network algorithm is mainly used for classification and identification, and each piece of data has one and only one category. The general activation function is mainly used for binary classification, like the sigmoid function. The Softmax function is an extension of the Sigmoid function, which can do multiple classifications and is not limited by the number of categories. The sigmoid function is defined by the following formula[22]:

$$S(t) = \frac{1}{1 + e^{-1}}. \tag{3}$$

The image of the sigmoid function is similar to softmax, and it also maps the input data to (0, 1). In addition, the sigmod function is monotonically increasing, and the reciprocal form is very simple, which is a more suitable function. However, the sigmoid function can only do two classifications, and softmax is an extension of sigmoid. It maps the k-dimensional input variable x to a probability-like interval, and then selects the largest subscript according to the output probability. The corresponding label is the most data category. The formula of the softmax algorithm is shown in the following formula[23]:

$$\sigma(z)_j = \frac{e^z j}{\sum_{k=1}^{K} e^z k}. \tag{4}$$

Because Softmax is an exponential function, when the input value is large, the value will increase exponentially, and when the input is negative, it will be greatly reduced, and the effect of model classification will be improved when the degree of discrimination is increased. Softmax is a continuously differentiable function, which can be better applied in the gradient descent algorithm [24].

4. Result Analysis

4.1. Experiment Environment. In this article, set nbytes = 320, so nimage = nbytes/8 = 40. In this paper, 8 protocols are selected for identification, so $N = 8$. The test dataset D contains 8 kinds of labels, corresponding to the ARP-like protocol, DNS-like protocol, HTTP-like protocol, ICMP-like protocol, OICQ-like protocol, SSDP-like protocol, tcp-like protocol, and udp-like protocol. In the convolutional neural network module, set kernel_size = 3, filters1 = 64, strides = 1, input_ranges = $5 \times 8 \times 240000$ and pool_size = 2. The dropout regularization method is necessary, let dropout = 0 : 25. The number of second convolutional neural network filters is filters2 = 128. The number of nodes in the first layer of the fully connected network is node1 = 128 and the number of nodes in the last layer is node2 = 8. The learning rate of the resulting module is learn_rate = 0 : 1, and the number of training epochs = 100. The total amount of data used in this paper is shown in Table 1. Put all the protocols together to get the train data set, randomly shuffle the order of the train data set, and then take the first 78,000 shuffled sequences for training, and then use the 2000 for testing [25].

4.2. Experiment Result. After analyzing and training the protocol and testing 1029 unknown protocols, we compared the three aspects of accuracy, loss, and running time. The experimental results are shown in Figure 3–5 below. It can be seen that the recognition effect of the convolutional neural network method for unknown protocols is very good, and the recognition rate is above 99%.

The analysis is as follows: During the experiment, the training set adopts the CNN deep neural network algorithm, and the test set adopts the transfer learning algorithm (DNN). The experimental results including the comparison of the training set are shown in Figures 3–5 above. It can be seen from the figure that the performance of CNN and DNN is quite different. The accuracy of CNN is about 2.4% higher than that of DNN, while the loss is reduced. 38.2%, and the running time is reduced by 42 times. The accuracy of transfer learning is obviously not as good as that of CNN in the early stages, and it is not as stable as CNN in the later tests. This is because when using the convolutional neural network in this paper, it is hoped that the model should be as close as possible to the distribution of the training data, the predicted data, and the distribution of the real data, so the cross-entropy loss function is often used to calculate the two-class loss function.

When using a neural network for protocol syntax analysis, a large-scale training set is usually required. If batch gradient descent is used, the amount of computation will be very large and require a lot of resources. In this case, the stochastic gradient descent method is used instead of batch gradient descent. The stochastic gradient descent algorithm first needs to randomly select a group from the sample data for training, sort it according to the loss degree of the output, and then extract a group. It continues to operate in the above method until it drops to a certain threshold. Therefore, during training, it is possible to obtain a satisfactory model without training all the data. Using the CNN algorithm can quickly analyze the results when the sample size is large. And the time complexity of CNN is basically stable at O (knp), where k is the number of iterations, and p is the average number of nonzero features of each sample. Using the stochastic gradient descent method, although the accuracy will decrease and there may be many detours, the overall trend is towards the minimum loss value, which will save a lot of time and make the algorithm faster. When predicting the result, the CNN algorithm puts the remaining 2000 pieces of data into the test set to test and outputs its label and accuracy. When converting the label, since the similarity is stored in the model prediction, and the highest similarity can be identified as the label of the protocol, so this chapter only needs to find the position with the highest similarity and find the protocol type it represents. It can be seen that the CNN

Table 1: Protocol dataset.

Protocol type	Total number of data frames	The total size of the data frame(KB)
ARP	10000	880
DNS	10000	854
HTTP	10000	867
ICMP	10000	856
OICQ	10000	848
TCP	10000	865
UDP	10000	855
Train	80000	7096

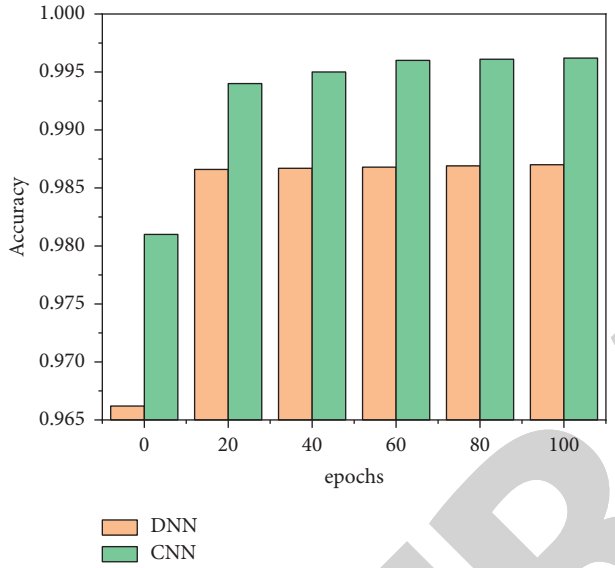

Figure 3: Accuracy comparison chart of the training set and test set.

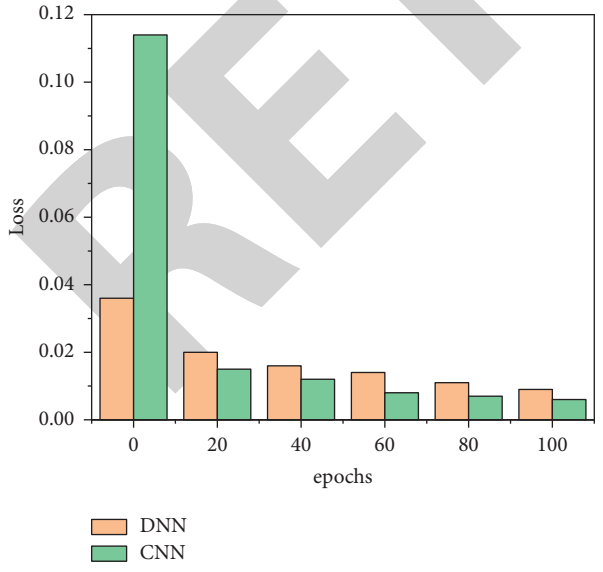

Figure 4: Comparison chart of training set and test set loss.

deep neural network algorithm can quickly and efficiently identify unknown protocols and then output the predicted protocol type and similarity. In the comparison experiment

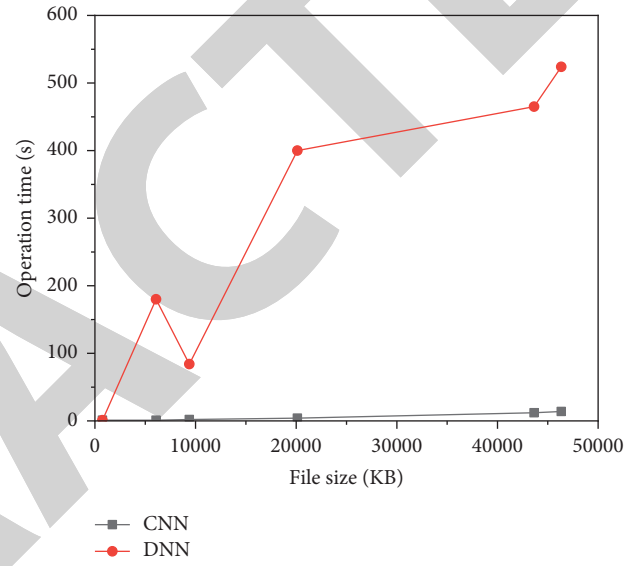

Figure 5: Comparison chart of the running time of a training set and a test set.

with DNN, it was found that it could achieve significantly superior performance indicators.

5. Conclusion

This paper mainly does some research work on the bitstream protocol. Including the intelligent reverse analysis method of the bitstream protocol and the feature extraction method of the bitstream protocol, on one hand, the research work is to convert the data protocol frame into an image, and then use the deep neural network algorithm in artificial intelligence technology to train the image data frame and pass the training. A good model identifies the protocol type adopted by the unknown protocol frame so as to extract the characteristic string in the network protocol frame to ensure the security of computer network communication.

This paper takes the bitstream protocol data frame as the research object and multiprotocol identification as the goal and focuses on network communication security under the support of artificial intelligence technology. However, due to the limitations of the experimental environment and conditions, the experimental data set in this paper is mainly obtained in real time through the Wireshark tool. In the follow-up research, the previous research can also be

improved and deepened from the following aspects: 1. This paper focuses on the feature mining and automatic identification of the bitstream protocol data; that is, the analysis of the syntax of the protocol. The next step can be from the protocol. The semantics and timing directions provide a more comprehensive analysis of the bitstream protocol data. 2. The system designed in this paper is a protocol identification system based on the B/S architecture, and the cross-platform compatibility is relatively poor. In the future, a C/S architecture protocol identification system needs to be studied to improve the compatibility of the platform.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C. Zhao, "Application of virtual reality and artificial intelligence technology in fitness clubs," *Mathematical Problems in Engineering*, vol. 2021, Article ID 2446413, 11 pages, 2021.

[2] C. He and B. Sun, "Application of artificial intelligence technology in computer aided art teaching," *Computer-Aided Design and Applications*, vol. 18, no. S4, pp. 118–129, 2021.

[3] Y. Wang, J. Ma, A. Sharma et al., "An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks," *Journal of Sensors*, vol. 2021, Article ID 5558860, 11 pages, 2021.

[4] F. Alirezaf, F. Reza, R. Javad, and M. Roberto, "Application of internet of things and artificial intelligence for smart fitness: a survey," *Computer Networks*, vol. 189, no. 5, pp. 2105–2107, 2021.

[5] D. L. Dinh, H. N. Nguyen, H. T. Thai, and K. H. Le, "Towards ai-based traffic counting system with edge computing," *Journal of Advanced Transportation*, vol. 2021, Article ID 5551976, 15 pages, 2021.

[6] S. Liu and L. Yangjun, "Application of human movement and movement scoring technology in computer vision feature in sports training," *IETE Journal of Research*, vol. 8, no. 6, pp. 1–7, 2021.

[7] M. Bistron and Z. Piotrowski, "Artificial intelligence applications in military systems and their influence on sense of security of citizens," *Electronics*, vol. 10, no. 7, p. 871, 2021.

[8] A. Mathew, "Artificial intelligence and cognitive computing for 6g communications & networks," *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 3, pp. 26–31, 2021.

[9] B. B. Misra, "Advances in high resolution gc-ms technology: a focus on the application of gc-orbitrap-ms in metabolomics and exposomics for fair practices," *Analytical Methods*, vol. 13, no. 20, pp. 2265–2282, 2021.

[10] A. R. Vollertsen, A. Vivas, B. Van Meer, A. Van Den Berg, M. Odijk, and A. D. Van Der Meer, "Facilitating implementation of organs-on-chips by open platform technology," *Biomicrofluidics*, vol. 15, no. 5, Article ID 051301, 2021.

[11] Z. Dou, J. Tian, Q. Yang, and L. Yang, "Design and analysis of cooperative broadcast scheme based on reliability in mesh network," *Mobile Information Systems*, vol. 2021, Article ID 5554563, 18 pages, 2021.

[12] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan, and G. Srivastava, "Sustainable security for the internet of things using artificial intelligence architectures," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–22, 2021.

[13] N. Sun, T. Li, G. Song, and H. Xia, "Network security technology of intelligent information terminal based on mobile internet of things," *Mobile Information Systems*, vol. 2021, no. 8, 9 pages, Article ID 6676946, 2021.

[14] P. R. Jena and R. Majhi, "An application of artificial neural network classifier to analyze the behavioral traits of smallholder farmers in Kenya," *Evolutionary Intelligence*, vol. 14, no. 2, pp. 281–291, 2021.

[15] F. H. Khan, M. A. Pasha, and S. Masud, "Advancements in microprocessor architecture for ubiquitous AI—an overview on history, evolution, and upcoming challenges in AI implementation," *Micromachines*, vol. 12, no. 6, p. 665, 2021.

[16] Y. Wang, B. Bai, X. Hei, L. Zhu, and W. Ji, "An unknown protocol syntax analysis method based on convolutional neural network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 5, 2021.

[17] S. Lee, A. Abdullah, N. Z. Jhanjhi, and S. H. Kok, "Honeypot coupled machine learning model for botnet detection and classification in iot smart factory—an investigation," *MATEC Web of Conferences*, vol. 335, no. 1, 2021.

[18] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, 2021.

[19] X. Du, W. Susilo, M. Guizani, and Z. Tian, "Introduction to the special section on artificial intelligence security: adversarial attack and defense," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 905–907, 2021.

[20] G. Kabanda, "Performance of machine learning and big data analytics paradigms in cybersecurity and cloud computing platforms," *Global Journal of Computer Science and Technology*, vol. 21, no. 2, p. 2128, 2021.

[21] A. Efe, "Usage of artificial intelligence to improve secure software development," *The Journal of International Scientific Researches*, vol. 6, no. 1, pp. 46–57, 2021.

[22] A. Sharma, R. Kumar, M. W. A. Talib, S. Srivastava, and R. Iqbal, "Network modelling and computation of quickest path for service-level agreements using bi-objective optimization," *International Journal of Distributed Sensor Networks*, vol. 15, no. 10, Article ID 155014771988111, 2019.

[23] S. Shriram, B. Nagaraj, J. Jaya, S. Shankar, and P. Ajay, "Deep learning-based real-time AI virtual mouse system using computer vision to avoid COVID-19 spread," *Journal of Healthcare Engineering*, vol. 2021, Article ID 8133076, 8 pages, 2021.

[24] R. Huang, "Framework for a smart adult education environment," *World Transactions on Engineering and Technology Education*, vol. 13, no. 4, pp. 637–641, 2015.

[25] X. Liu, J. Liu, J. Chen, F. Zhong, and C. Ma, "Study on treatment of printing and dyeing waste gas in the atmosphere with Ce-Mn/GF catalyst," *Arabian Journal of Geosciences*, vol. 14, no. 8, pp. 737–746, 2021.