An Optimization Technique for Intrusion Detection of Industrial Control Network Vulnerabilities Based on BP Neural Network

Wenzhong Xia
Zhaotong University
Rahul Neware (rane@hvl.no)
Western Norway University of Applied Sciences: Hogskulen pa Vestlandet https://orcid.org/0000-0002-9771-6288
S.Deva Kumar
Vignan's Foundation for Science Technology and Research
Dimitrios A Karras
University of Athens: Ethniko kai Kapodistriako Panepistemio Athenon
Ali Rizwan
King Abdulaziz University

Research Article

Keywords: BP neural network, AdaBoost algorithm, One-Class Support Vector Machine, Fuzzy-based abnormal data detection, Intrusion Detection

Posted Date: November 30th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-990908/v1

Version of Record: A version of this preprint was published at International Journal of System Assurance Engineering and Management on January 4th, 2022. See the published version at https://doi.org/10.1007/s13198-021-01541-w.

An optimization technique for intrusion detection of industrial control network vulnerabilities based on BP neural network

Wenzhong Xia [1], Rahul Neware [2*],S.Deva Kumar[3], Dimitrios A. Karras[4], Ali Rizwan[5]

[1*]School of physics and information engineering, Zhaotong University, Zhaotong Yunnan, 657000, China

[2*]Department of Computing, Mathematics and Physics, Høgskulen på Vestlandet Bergen Norway

[3]Department Of Computer Science And Engineering , Vfstr Deemed To Be University

[4]National and Kapodistrian,University of Athens (NKUA), School of Science, Dept. General, Athens, Greece

[5]Department of Industrial Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia.

Email: WenzhongXia723@126.com[1] , rane@hvl.no[2*] , sdk_cse@vignan.ac.in[3], dakarras@uoa.gr[4] , arkhan71@kau.edu.sa[5]

Abstract: The aim of this research is to solve the problem that the intrusion detection model of industrial control system has low detection rate and detection efficiency against various attacks, a method of optimizing BP neural network based on Adaboost algorithm is proposed. Firstly, principal component analysis (PCA) is used to preprocess the original data set to eliminate its correlation. Secondly, Adaboost algorithm is used to continuously adjust the weight of training samples, to obtain the optimal weight and threshold of BP neural network. The results show that there are 13817 pieces of data collected in the industrial control experiment, of which 9817 pieces of data are taken as the test data set, including 9770 pieces of normal data and 47 pieces of abnormal data. In addition, as a test data set of 4000 pieces, there are 3987 pieces of normal data and 13 pieces of abnormal data. It can be seen that the average detection rate and detection speed of the algorithm of optimizing BP neural network by Adaboost algorithm proposed in this paper are better than other algorithms on each attack type. It is proved that Adaboost algorithm can effectively solve the intrusion detection problem by optimizing BP neural network.

Key words: BP neural network; AdaBoost algorithm; One-Class Support Vector Machine; Fuzzy-based abnormal data detection; Intrusion Detection

1 Introduction

Intrusion detection is the process of identifying attempted, ongoing, or already occurring intrusions. The standard TCP/IP protocol in the communication protocol is widely used in the

vast majority of the current network environment, leading to the vast majority of the current intrusion objects are also aimed at this protocol. Therefore, the interception and analysis of data packets based on TCP/IP protocol is the focus of data analysis in intrusion detection system. Generally speaking, intrusion detection is divided into abuse and anomalies. The former has the advantage of high detection rate and low false positive rate, but its disadvantage is that it can only detect known attack model patterns. Therefore, to maintain or improve the efficiency, it is necessary to continuously update the detection method. The advantage of anomaly detection lies in the detection of unknown intrusion behavior. From the current usage situation, the abuse detection is more applied, but various forms of anomaly, intrusion detection technology and anomaly detection module are also increasing attention. Intrusion detection mainly includes data fusion, data mining, genetic algorithm, computer immunology, neural network and so on among which the application of neural network is increasing extensive.

The most representative one is BP neural network algorithm. The BP neural network technology used in intrusion detection system has obvious advantages and disadvantages, such as slow learning speed and convergence. The convergence speed of traditional BP network algorithm is slow and the network is easy to fall into the local minimum. Therefore, many related improved algorithms have emerged to solve these problems, and some achievements have been made. For example, Adaboost algorithm, when testing the intrusion detection system, KDD99 data set contains more than 7 million data (these data include TCP connection data and TCP test records), so it is often used in the simulation test of the intrusion detection system. In the TCP records used for testing, 41 characteristics existed in each TCP connection record. These characteristics could be divided into four categories: Basic TCP characteristics, capacity characteristics, time-based traffic characteristics, and host-based traffic characteristics. The data in the training data set has been marked as normal or attacked, and there are a total of 38 types of attacks. Among the 24 types of original attacks, 4 new attacks have been added for the test data. Among the four new attack methods, including unauthorized access to local root privilege (U2R), denial of service attack (DoS), data resource theft (Probing), unauthorized access to remote computers (R2L), the supply of denial of service accounts for nearly 50%, which is the largest among all attack categories.

As of January 24, 2017, there were 979 industrial control system vulnerabilities published by the national new security vulnerability sharing platform, of which Siemens vulnerability accounted for 40.86%, Advantech vulnerability accounted for 19.43%, Schneider vulnerability accounted for 15.43, Rockwell vulnerabilities accounted for 12%, The rest, the Parallels bug for virtualization, accounted for 12.29%. Among these vulnerabilities, high risk vulnerability accounted for 48.18%, medium risk vulnerability accounted for 45.97%, and low risk vulnerabilities accounted for 5.85%. The common industrial control system vulnerabilities include communication transmission protocol vulnerability, industrial control equipment vulnerability, industrial control, software vulnerability, configuration error

vulnerability, etc. The communication transmission protocol vulnerability is mainly TCP/IP, RPC, UDP, and other protocols. The industrial control software vulnerability is mainly due to the lack of unified security protection specifications of industrial control software and the widespread existence of security design defects. Therefore, the industrial control software is easy to be attacked by attackers and obtain the control of the equipment, resulting in serious consequences.

According to this research problem, scholars proposed a series of IDS related algorithm models. Chen, T., Lin, P. et al. proposed the intrusion detection of improved genetic algorithm to optimize the neural network [1]. They optimized BP neural network by using rough set and improved genetic algorithm and proposed the best initial parameters to solve the problem of slow detection speed and local minimization of BP neural network. Lai, Y., Liu, Z. et al. studied the intrusion detection method based on PCA-BP neural network by using PCA to preprocess the data set, to accelerate the convergence speed and detection efficiency, but the effect of this method was not obvious in the detection of U2R and R2L attack types [2]. Y Lai, Gao, H. et al. combined the intrusion detection method of whitelist filtering and neural network, and constantly improved the whitelist rule base according to the detection results of neural network to improve the detection rate of abnormal communication, but this method did not optimize the detection speed [3]. Nuraeni, N. Astuti, P. et al. proposed an improved fish swarm algorithm optimization method for communication anomaly detection of industrial control network. Shang, W., Zeng, P. et al. introduces a new intrusion detection algorithm based on One-Class Support Vector Machine (OCSVM) where a normal communication behavior model is established by using OCSVM, and the Particle Swarm Optimization algorithm is designed to optimize OCSVM model parameters [4]. The optimization method uses the improved fish swarm algorithm to optimize the initial input weights and thresholds of the neural network for optimization. The method improves the accuracy of anomaly detection and shortens the detection time, but the detection effect is not obvious to each typical attack type.

To sum up, although the current industrial control system vulnerability detection has adopted many methods, the main ones are Fuzzy-based abnormal data detection method, eigenvalue matching method and rule judgment method. The BP (Back Propagation) neural network, a multi-layer feedforward network trained by error Back Propagation algorithm, is mostly used for pattern recognition and rarely appears in the field of industrial control system vulnerability mining. Due to the real-time operation of the industrial control system, the vulnerability of the industrial control system can not be mined online, there is no way to analyze the relationship between data, there is also a lack of automatic learning ability, to solve the current problem, we published a BP neural network based on the vulnerability of the industrial control system automatic mining method.

2 Experimental Methods

An automatic mining method of industrial control system vulnerability based on BP neural network is presented. The method includes data acquisition module, neuron design module, neural network structure design module and algorithm implementation module of the industrial control system. Data acquisition module of industrial control system: Including original data collection and data normalization processing; original data acquisition of industrial control system, sensor data acquisition of industrial control system, including temperature, pressure, humidity, speed, switching state information, such as valve state and control command; data normalization processing: due to the different types of data collected, the range of data expression is also very different, so it can not be directly used as the input vector of BP neural network. Therefore, it is necessary to normalize the data, define the conversion method, and convert it into the input data that can be accepted by BP neural network.

Principal component analysis (PCA) and Adaboost algorithm are added to the router between the administrator's network client and web server to optimize the intrusion detection model of BP neural network, and the abnormal communication data between the administrator and the server are detected by using the data characteristics in the communication network, to improve the detection accuracy and detection speed [5].

2.1 Feature selection in intrusion detection

In the KDD99 data set used in the experiment in this paper, the data of intrusion attacks are mainly divided into:

(1) DoS attack attackers attack network protocol defects or system resources, so that the normal system is paralyzed, thus denying users access to the service.

(2) A common method used by an attacker to initiate an attack on a target and to obtain relevant information by this method.

(3) U2R attack attacks users with low permissions, obtaining permissions through system or website vulnerabilities, and then carrying out illegal operations.

(4) R2L Attack Attackers operate and access resources in an unauthorized way through a remote host.

2.2 Data Preprocessing

Through the analysis of KDD99 data set, there are a lot of repeated records in the data set, so the learning efficiency and detection rate of intrusion detection algorithm are low. To improve the learning efficiency and detection rate of the algorithm, this paper uses PCA to preprocess the data set and eliminate the correlation between the data. Standardization processing formula:

$$z_{ij} = \frac{x_{ij} - \bar{x}_j}{s_j} \qquad (i = 1,2,...,m;\ j = 1,2,...,p) \qquad (1)$$

Type $\bar{x}_j = \frac{\sum_{i=1}^{m} x_{ij}}{m}$, $s_j = \frac{\sum_{i=1}^{m} \left(x_{ij} - \bar{x}_j\right)}{m-1}$, x_{ij} is the value of each sample in the matrix, z_{ij} is the normalized matrix after data processing, $\bar{x}_j$ is the mean of each column, and s_j is the normalization of each column.

$$R = \left[r_{ij}\right]_p xp = \frac{z^T z}{m-1} \qquad (2)$$

Type $r_{ij} = \frac{\sum z_{kj} \cdot z_{kj}}{m-1}, i, j = 1,2,...,p;$ R is the correlation matrix, x is the random variable, z^T is the normalized matrix Z transpose. Calculate p eigenvalues λ_i through $\left|\lambda E_p - R\right| = 0$, the contribution rate $\frac{\lambda_i}{\sum_{i=1}^{p} \lambda_i}$ was used for feature extraction.

Calculate n principal components, and you get the matrix D_{m*n}

2.3BP neural network algorithm

BP neural network is a classic algorithm in neural network. Feature extraction is carried out according to the data and used as the input value of BP neural network to express the mapping relationship between input and output, as shown in Figure 1.

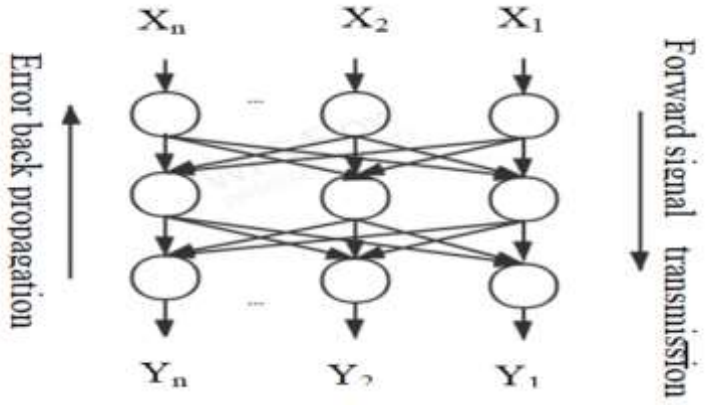

Figure 1 Structure topology of BP neural network

In Figure 1, $x_1, x_2, ..., x_n$ is the input value of BP neural network and $y_1, y_2, ..., y_m$ is the output value of BP neural network. When the signal is transmitted forward, it is assumed that

the weight between neuron i and neuron j is ω_{ij}, the threshold value of neuron j is b_j, the output value of each neuron is s_j, and the correlation is

$$S_j = \sum_{i=0}^{m-1} \omega_{ij} x_i + b_j \qquad (3)$$

$$x_j = f(S_j) \qquad (4)$$

Where, f is the S-shaped excitation function [6].

2.4 Adaboost -BP neural network algorithm

Adaboost algorithm seeks to combine the simplest weak classifiers to obtain a strong classifier [7]. In terms of the use of the algorithm, it only needs to specify the number of iterations, and all the parameters in the operation process are adjusted adaptively by the algorithm. The procedure of the algorithm is as follows:

Step 1: Select n data for training, set the weight distribution of training data as $D_t(i) = 1/m$, and obtain the initial weight and threshold values randomly by the algorithm.

Step 2: Weak classifier. The sum of the classification error of classification sequence $g(t)$ obtained when training the t weak classifier is

$$e_t = \sum_{i=1}^{n} D_t(i); g(t) \neq y \qquad (5)$$

Where, y is the expected value

Step 3: Calculate the weight of the classification sequence. Calculate the weight according to the classification error e_t

$$a_t = \frac{1}{2} \ln\left(\frac{1-e_t}{e_t}\right) \qquad (6)$$

Step 4 Adjust the weight. Adjust the weight of samples in the next round according to the weight a_t. The formula is as follows:

$$D_{t+1}(i) = \frac{D_t(i)}{B_t} \exp\left[-a_t y_i g_t(x_i)\right] \qquad (7)$$

In the formula, B_t is the normalization factor and y is the expected value.

Step 5: Strong classifier function. After T iterations, strong classifier $h(x)$ is generated from the weak classifier function $f(g_t, a_t)$ of T group.

$$h(x) = \mathrm{sgn}\left[\sum_{t=1}^{T} a_t f(g_t, a_t)\right] \quad (8)$$

2.5 Intrusion Detection Model of Adaboost BP Neural Network

The weight of BP weak classifier is adjusted continuously through Adaboost algorithm, and the training results are calculated. Several BP weak classifiers are combined into BP strong classifiers as the final decision classifier [8]. Thus, the intrusion detection model of industrial control network is established

3 Results and analysis

3.1 Validation of algorithm

(1) Description of experimental data

The data of the simulation experiment is KDD99 data set, which is widely used in intrusion detection. The data set includes 514,092 training data sets and 336,463 test data sets, respectively. Each data contains 41-dimensional features, the last of which is the label attribute. It mainly includes 6 categories of relevant data, namely, Normal, DoS attack, Probe attack, U2R attack, R2L attack, and Unknow.

(2) Experimental environment and relevant data

The hardware environment of the simulation test was INTELI5-7200U2. 70GHz, the memory is 4G, the operating system is Winows10, the software environment used is Matlab2016a, PyCharm2017. Relevant experimental data after processing [9].

Table 1 Experimental data information

The data type	The training sample	The test sample	The data type	The training sample	The test sample
Normal	107278	65591	U2R	52	42
DoS	401450	250294	R2L	1325	1087
Probe	3897	2476	Unknow		16973

Firstly, the principal component analysis method mentioned above was used to extract features from the data set, and PyCharm was used to conduct principal component analysis on 12 features of 514092 data. Then the corresponding principal component number can be extracted by using the above contribution rate calculation. Then, the carrying capacity of each principal component in the original data is compared. The larger the carrying capacity of each principal component is, the larger the corresponding data information quantity is. Finally, the main original data characteristics reflected by the 10 principal components were extracted [10-11].

Table 2 Principal components reflect the main original characteristics

The principal components	Reflects the primary primitive variable
1	Connection duration
2	Protocol type
3	The network service type of the destination address
4	The number of bytes of data from source address to destination address
5	Number of bytes of data from destination address to source address
6	Login successfully or not
7	The number of connections with the same service as the current connection in the past two seconds
8	The number of connections that have the same destination address as the current connection in the past two seconds
9	The percentage of the top 100 connections that have the same source destination port at the same destination address as the current connection
10	The number of connections in the top 100 that have the same service at the same destination address as the current connection

In the Matlab environment, the BP neural network improved by Adaboost algorithm is used to select the most widely used three-layer forward feedforward neural network. The number of neurons in the input layer is 10, the number of neurons in the hidden layer is 30, and the number of output neurons is 6, respectively, which are normal data. DoS attack, U2R attack, R2L attack, Probe attack, Unknow unknown attack [12-13].

According to the standard of intrusion detection, the detection rate and false positive rate of the intrusion detection model combined with Adaboost algorithm and BP neural network in this paper are compared, where:

$$\text{Detection rate} = \frac{\text{Normal detection of abnormal data}}{\text{Total number of abnormal data}}$$

$$\text{The rate of false positives} = \frac{\text{The error judgment is the total number of abnormal data}}{\text{Total normal data}}$$

Here, the detection rate of the intrusion detection method in this paper is compared with the following three methods, as shown in Figure 2.

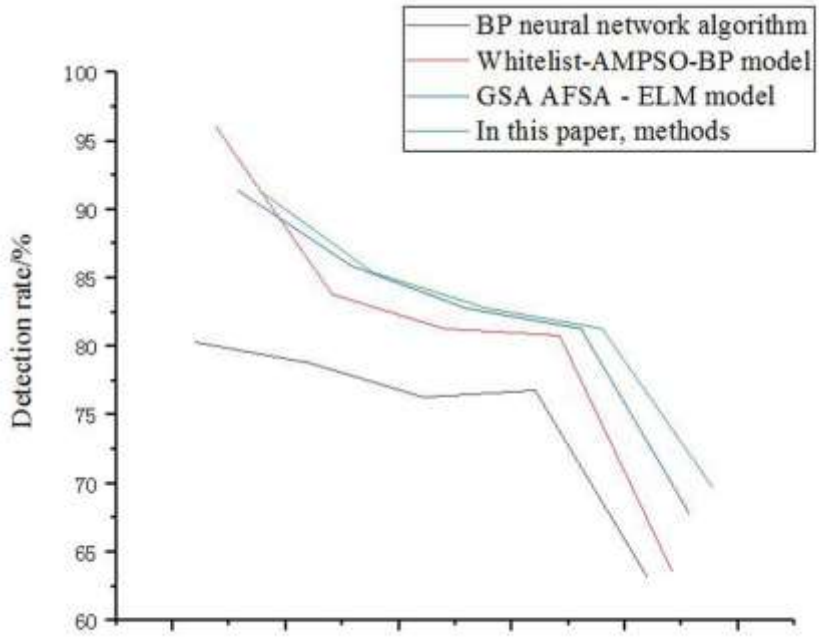

Figure 2 Comparison of detection rates of four systems

As shown in Figure 3 below, the false positive rate of the four groups of intrusion detection models is compared, and it is found that the false positive rate of the algorithm model optimized by Adaboost for BP neural network is reduced in some attack types.

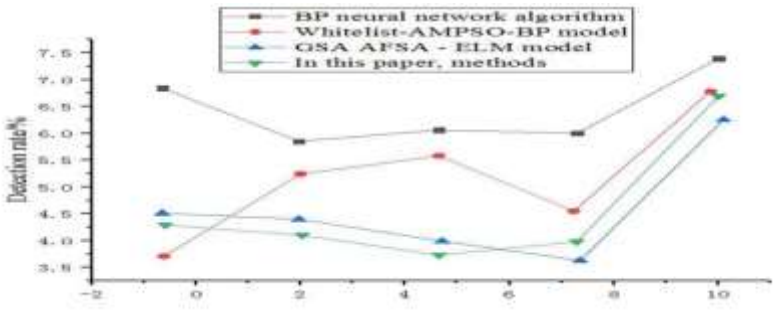

Figure 3 Comparison of false alarm rates

The training time of the BP neural network optimized by Adaboost is 3.256s, while the training time of the traditional BP neural network is 3.912s [14-15].The difference in training time is mainly due to the fact that Adaboost reduces the effect of a single BP neural network falling into the local optimum [16].

3.2 Industrial control simulation test

A total of 13,817 pieces of partially collected data were obtained from a wind power plant, including 13,757 pieces of normal data and 60 pieces of abnormal data. In the experiment of industrial control system, four groups of data features are extracted respectively: source IP address, target IP address, protocol and data length [17-18]. The obtained data were used to extract the features of the four groups of data by principal component analysis, and then were input as input nodes [19-20]. The output nodes of the algorithm model were normal and abnormal respectively. 13,817 pieces of data were collected in the industrial control experiment, among which 9817 pieces of data were taken as the test data set, including 9770 pieces of normal data and 47 pieces of abnormal data [21-22]. In addition, 4000 of them as test data sets contain 3987 normal data and 13 abnormal data. Now the proposed algorithm and the traditional BP algorithm are tested and compared by using the data collected by the industrial control system [23]. Due to the large normal database in the normal operation of the industrial control network, the false positive rate is not compared here.

4 Conclusions

An algorithm model of Adaboost algorithm to optimize BP neural network is proposed. The concrete content of this method is (1) using principal component analysis (PCA) to extract features and reduce dimensionality of data sets, (2) Adaboost algorithm to update the sample distribution constantly (3) combining multiple types of BP weak classifiers with BP strong

classifiers by Adaboost algorithm. Through experimental observation, a total of 13,817 pieces of partially collected data were obtained from a wind power plant, including 13,757 pieces of normal data and 60 pieces of abnormal data. In the experiment of industrial control system, four groups of data features are extracted respectively: source IP address, target IP address, protocol and data length. The obtained data were used to extract the features of the four groups of data by principal component analysis, and then were input as input nodes. The output nodes of the algorithm model were Normal and Abnormal respectively. 13,817 pieces of data were collected in the industrial control experiment, among which 9817 pieces of data were taken as the test data set, including 9770 pieces of normal data and 47 pieces of abnormal data. In addition, 4000 of them as test data sets contain 3987 normal data and 13 abnormal data. To prove that the average detection rate and detection speed of the BP neural network optimized by Adaboost algorithm for each attack type are better than other algorithms, better improve the detection speed and detection accuracy, solve the BP neural network into local optimal problem, and improve the detection rate and detection speed of abnormal data.

Compliance with Ethical Standards

The authors declare that they have no conflict of interest and all ethical issues including human or animal participation has been done. No such consent is applicable.

References

[1] Chen, T., Lin, P., & Ling, J. (2019, August). An Intrusion Detection Method for Industrial Control System Based on Gate Recurrent Unit. In Journal of Physics: Conference Series (Vol. 1302, No. 2, p. 022016). IOP Publishing.

[2] Zhanwei, S., & Zenghui, L. (2019). Abnormal detection method of industrial control system based on behavior model. Computers & Security, 84, 166–178. https://doi.org/10.1016/j.cose.2019.03.009

[3] Lai, Y., Gao, H., & Liu, J. (2020). Vulnerability Mining Method for the Modbus TCP Using an Anti-Sample Fuzzer. Sensors, 20(7), 2040. https://doi.org/10.3390/s20072040

[4] Shang, W., Zeng, P., Wan, M., Li, L., & An, P. (2015). Intrusion detection algorithm based on OCSVM in industrial control system. In Security and Communication Networks (Vol. 9, Issue 10, pp. 1040–1049). Wiley. https://doi.org/10.1002/sec.1398

[5] Sanober, S., Alam, I., Pande, S., Arslan, F., Rane, K. P., Singh, B. K., Khamparia, A., & Shabaz, M. (2021). An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication. Wireless Communications and Mobile Computing, 2021, 1–14. https://doi.org/10.1155/2021/6079582

[6] Nuraeni, N., Astuti, P., Irnawati, O., Darwati, I., & Harmoko, D. D. (2020, November). High Accuracy in Forex Predictions Using the Neural Network Method Based on Particle

Swarm Optimization. In Journal of Physics: Conference Series (Vol. 1641, No. 1, p. 012067). IOP Publishing.

[7] Chopra, S., Dhiman, G., Sharma, A., Shabaz, M., Shukla, P., & Arora, M. (2021). Taxonomy of Adaptive Neuro-Fuzzy Inference System in Modern Engineering Sciences. Computational Intelligence and Neuroscience, 2021, 1–14. https://doi.org/10.1155/2021/6455592

[8] Rizwan, A., & Alvi, M. S. I. (2010). Analysis of factors affecting the stress level of engineering students. The International journal of engineering education, 26(3), 681-686.

[9] Lai, Y., Zhang, J., & Liu, Z. (2019). Industrial anomaly detection and attack classification method based on convolutional neural network. Security and Communication Networks, 2019.

[10] Yuxia, Z. (2019). Optimization calculation of well function W (u, r/B) based on BP neural network. E3S Web of Conferences, 136, 04031. https://doi.org/10.1051/e3sconf/201913604031

[11] Fakhar, A., Jahanzaib, M., Sarfraz, M. H., Shafiq, M., & Rizwan, A. (2020). Investigating the Impact of Emotional Intelligence on Academic Performance of Engineering Students: An Exploratory Study in Pakistan. The Nucleus, 56(3), 105-111.

[12] Chen, J., Chen, L., & Shabaz, M. (2021). Image Fusion Algorithm at Pixel Level Based on Edge Detection. Journal of Healthcare Engineering, 2021, 1–10. https://doi.org/10.1155/2021/5760660

[13] Feng, X. (2020). Research on intrusion detection of industrial control system based on deep convolution network and k-means. Computer Science and Application, 10(11), 2141-2146.

[14] Prasanalakshmi, B., Kannammal, A., & Sridevi, R. (2011). Multimodal biometric cryptosystem involving face, fingerprint and palm vein. International Journal of Computer Science Issues (IJCSI), 8(4), 604.

[15] Shang, W., Zhang, G., Wang, T., & Zhang, R. (2021). A Test Cases Generation Method for Industrial Control Protocol Test. Scientific Programming, 2021, 1–9. https://doi.org/10.1155/2021/6611732

[16] Li, Z., Zhao, H., Shi, J., Huang, Y., & Xiong, J. (2019). An Intelligent Fuzzing Data Generation Method Based on Deep Adversarial Learning. IEEE Access, 7, 49327–49340. https://doi.org/10.1109/access.2019.2911121

[17] Sharma, C., Bagga, A., Singh, B. K., & Shabaz, M. (2021). A Novel Optimized Graph-Based Transform Watermarking Technique to Address Security Issues in Real-Time Application. Mathematical Problems in Engineering, 2021, 1–27. https://doi.org/10.1155/2021/5580098

[18] Anton, S. D. D., Fraunholz, D., Krohmer, D., Reti, D., Schneider, D., & Schotten, H. D.

(2021). The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World. IEEE Internet of Things Journal, 1–1. https://doi.org/10.1109/jiot.2021.3081741

[19] Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. In A. Jolfaei (Ed.), Wireless Communications and Mobile Computing (Vol. 2021, pp. 1–17). Hindawi Limited. https://doi.org/10.1155/2021/7154587

[20] Prasanalakshmi, B., & Pugalendhi, G. K. (2019, June). Two-Way Handshake User Authentication Scheme for e-Banking System. In International Conference on Intelligent Computing and Communication (pp. 135-141). Springer, Singapore.

[21] Deshmukh, S., Thirupathi Rao, K., & Shabaz, M. (2021). Collaborative Learning Based Straggler Prevention in Large-Scale Distributed Computing Framework. Security and Communication Networks, 2021, 1–9. https://doi.org/10.1155/2021/8340925

[22] Kumari, K. A., Sharma, A., Chakraborty, C., & Ananyaa, M. (2021). Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems. In Big Data. Mary Ann Liebert Inc. https://doi.org/10.1089/big.2021.0012

[23] Akpinar, K. O., & Ozcelik, I. (2019). Analysis of Machine Learning Methods in EtherCAT-Based Anomaly Detection. IEEE Access, 7, 184365–184374. https://doi.org/10.1109/access.2019.2960497

[24] Zegzhda, D. P., Kalinin, M. O., & Levykin, M. V. (2019). Actual Vulnerabilities of Industrial Automation Protocols of an Open Platform Communications Series. Automatic Control and Computer Sciences, 53(8), 972–979. https://doi.org/10.3103/s0146411619080339

[25] Tang, S., & Shabaz, M. (2021). A New Face Image Recognition Algorithm Based on Cerebellum-Basal Ganglia Mechanism. Journal of Healthcare Engineering, 2021, 1–11. https://doi.org/10.1155/2021/3688881

[26] Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C., & Pani, S. K. (2021). MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. In IEEE Access (Vol. 9, pp. 80931–80944). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2021.3085187

[27] Prasanalakshmi, B., & Kannammal, A. (2013). ECC Based Biometric Encryption of Compressed Image for Security over Network Channels. In Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012) (pp. 343-351). Springer, India.