Journal of Industrial Engineering and Applied Science
ISSN 3005-6071 (Print) | ISSN 3005-608X (Online) | Vol. 2, No. 2, 2024

An Analysis of the Application of Machine Learning in Network Security

ZHOU, Zhanxin [1*] XU, Changxin [1] QIAO, Yuxin [1] NI, Fanghao [2] XIONG, Jize [1]

[1] Northern Arizona University, USA
[2] Indian Institute of Technology, India

***** ZHOU, Zhanxin is the corresponding author, E-mail: zhouzhan098@gmail.com***

Abstract: In order to deal with the problem of imbalance and complex feature relationship in network data classification, this study proposes a machine learning classification method, combined with improved SMOTE technology and genetic algorithm optimization for XGBoost (GA-XGBoost). Sample balance is achieved by introducing local outlier factors in the SMOTE process, oversampling the minority classes, and randomly undersampling the majority classes. Meanwhile, the evolutionary iterative advantage of the genetic algorithm was used to optimize the XGBoost model parameters and improve the model fit. The experimental results on the UNSW _ NB 15 dataset show that the classification prediction accuracy reached 97.40%, average recall of 70.2% and average F1-score of 68.8%, showing a higher performance compared to the traditional machine learning algorithm and SMOTE + XGBoost method. In addition, the tests on the data collected by the industrial information security platform also confirmed the effectiveness of the proposed method, with a classification accuracy of 99%.

Keywords: Data Imbalance, SMOTE, GA-XGBoost, Network Data Classification.

DOI: https://doi.org/10.5281/zenodo.10775504

1 Introduction

With the rapid development of computer technology, network security has become an important issue in the present society. The statistical analysis and data mining of network traffic and alarm log are the core of network security analysis, which play a key role in monitoring network dynamics. However, with the exponential growth of network traffic, it becomes particularly important to classify effective network data traffic models [1]. In order to improve the classification accuracy in the unbalanced state of network security data samples, this study proposes a machine learning classification method of XGBoost (GA-XGBoost) combining improved SMOTE technology and genetic algorithm optimization, in order to solve the feature learning effect and classification accuracy of existing models when dealing with unbalanced data.

2 The Algorithm Principle and Analysis

2.1 SMOTE Technical Improvement

2.1.1 SMOTE Technical Basis

In response to the data imbalance problem, the SMOTE technology adopts a unique oversampling method. It uses linear interpolation between minority samples to create new "artificial" data points, so as to increase the number of minority samples and achieve the effect of balancing data sets [2]. Compared with the traditional random oversampling, this method can improve the learning ability of the model more effectively. The mathematical expression is provided as follows:

$$S_{\text{new}} = S + \lambda\left(S_i - S\right)$$

S_{new} S_i Where, it represents the sample generated by interpolation, S represents the selected data point represents a sample of the K neighbors around S, and λ belongs to the (0,1) interval. Through the above formula, linear interpolation between data points can provide richer few class sample features for learning.

In view of the problem that the traditional SMOTE algorithm may choose noise points or abnormal outlier points when selecting the nearest neighbor interpolation point, thus generating redundant samples and blurring the sample boundary, this paper introduces the local outlier factor (LOF) to optimize the SMOTE algorithm. LOF is a density-based method that quantify the degree of dispersion between samples to select the appropriate interpolation point during the SMOTE interpolation process. The main calculation steps of the LOF include:

x_i x_{ki} x_i x_{ai}

1) For the sample set X, if the K Euclidean distance nearest neighbor is one nearest neighbor, the accessible distance from each sample to the Kth nearest neighbor can

be calculated as:

$$D_{\text{reach\_dis}}(x_i, x_{ai}) = \max\{d(x_{ki}, x_{ai}), d(x_i, x_{ai})\}$$

2) Calculate the local accessible density for each sample:

$$R_k(x_i) = \frac{K}{\sum_{a=1}^{K} D_{\text{reach\_dis}}(x_i, x_{ai})}$$

3) Calculate the local outlier factor for each sample:

$$L_K(x_i) = \frac{1}{K}\sum_{a=1}^{K}\frac{R_K(x_{ai})}{R_K(x_i)}$$

2.2 XGBoost, and Combined with the Genetic Algorithm

2.2.1 Overview of the GA

In GA, the vector X in the decision space is encoded as a string of symbols, each representing a gene and the whole string representing a chromosome, a feasible solution to the problem. The operating agent of the algorithm is a group M containing multiple individuals. Each generation population is represented by p (t) [4]. As shown in Figure 1, the genetic algorithm produces a new generation population p (t + 1) by selecting, crossing over and varying the current generation population p (t). In the course of the genetic algorithm, the fitness of each individual is calculated, and the entire population is updated for that fitness. As the algorithm continues to iterate, the population with the optimal fitness values is eventually obtained.

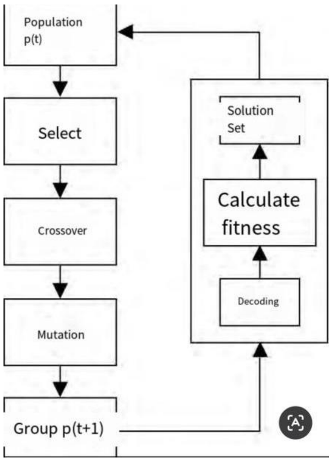

Figure 1 Iterative Process of the Genetic Algorithm

2.2.2 Overview of the XGBoost method

For the in-depth analysis of XGBoost algorithm, it is an advanced algorithm in the field of machine learning, which is especially suitable for classification and regression tasks. This algorithm is based on the lifting tree, and aims to minimize an objective function containing two parts: one part is the quantification of prediction error, and the other part is the control of model complexity [5]. The objective function can be expressed as follows:

$$Obj(\theta) = \sum_{i=1}^{n}\ell(y_i, \hat{y}_i) + \sum_{k=1}^{K}\Omega(f_k)$$

$\ell(y_i, \hat{y}_i)$ $\hat{y}_i$ y_i $\Omega(f_k)$ Here, the difference between the predicted value and the actual value of the i-th sample is measured, while expressing the complexity of the model, where K is the number of trees in the model.

By optimizing the objective function using a Taylor expansion, the XGBoost algorithm transforms into a convex optimization problem. During the optimization process, the output value of each node of the decision tree is accurately calculated precisely to minimize the objective function, and the optimal solution for this output value can be solved by the following formula:

$$\omega_j^* = -\frac{\sum_{i\in I_j} g_i}{\sum_{i\in I_j} h_i + \lambda}$$

I_j g_i h_i Here, is the set of samples of leaf node j, and are the first and second order gradients of sample i respectively, and λ is the regularization parameter.

In addition, the algorithm adopts a greedy strategy to gradually construct the tree structure and guide the tree growth by calculating the gain. This gain is given by the following formula:

$$\text{Gain} = \frac{1}{2}\left[\frac{\left(\sum_{i\in I_L} g_i\right)^2}{\sum_{i\in I_L} h_i + \lambda} + \frac{\left(\sum_{i\in I_R} g_i\right)^2}{\sum_{i\in I_R} h_i + \lambda} - \frac{\left(\sum_{i\in I} g_i\right)^2}{\sum_{i\in I} h_i + \lambda}\right] - \gamma$$

I_L and I_R Where I represents the set of nodes, the set of left and right children, and γ is another regularization parameter. This approach effectively strikes a balance between prediction accuracy and model simplicity, reducing the risk of overfitting, and making XGBoost superior in numerous machine learning tasks.

2.2.3 Combination of GA and XGBoost

When constructing the classification prediction model, combining the genetic algorithm and the XGBoost technology can realize the optimization of the model performance. XGBoost, As an efficient machine learning framework, it has many parameters, but its tuning may be complicated. The introduction of genetic algorithm can realize the automation and high efficiency of XGBoost parameter adjustment, so as to improve the model performance. As shown in Figure 2, the GA optimizes the parameters of the XGBoost model by simulating natural selection and genetics principles, including selection, crossover and variation. After multiple iterations, the optimal or nearly optimal parameter combinations can be obtained. This optimization strategy not only improves the learning ability of XGBoost, but also enhances the performance of the model in the global search range, reducing the possibility of falling into the local optima. While this may increase the computational cost, the benefits in improving the model accuracy and convergence rate are significant.

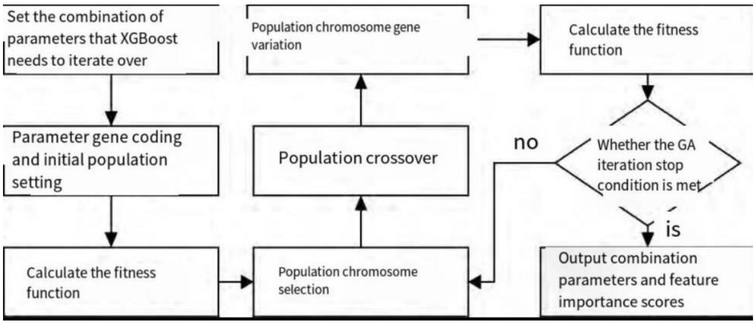

Figure 2 Optimization iteration of the GA with XGBoost

2.3 The XGBoost Model Optimized by Combining the SMOTE and the Genetic Algorithm

Facing the challenge of unbalanced datasets, especially in identifying minority samples, traditional machine learning methods are often limited. In order to improve the identification efficiency of these minority samples, an improved data oversampling technology, namely SMOTE, is adopted, which increases the sample size of minority samples by generating synthetic samples to improve the balance of the data. As shown in Figure 3, further, this enhanced SMOTE method is combined with the GA-XGBoost algorithm to improve the performance at the model building level. This combined approach covers various stages from data preprocessing to feature learning, dedicated to optimize the processing efficiency of unbalanced datasets. In the preprocessing phase, in response to the heterogeneous phenomena in the raw data, a series of techniques were employed to ensure the thoroughness of the data cleaning and preparation.

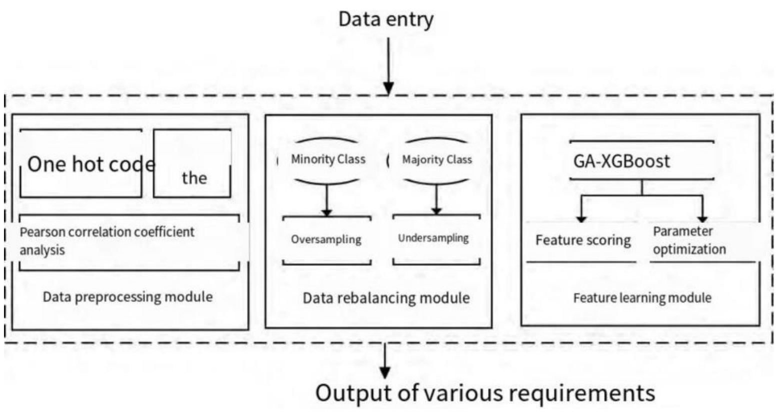

Figure 3 combines the XGBoost model optimized by SMOTE and GA

3 Data Processing and Sample Equalization Strategy

3.1 Pretreatment

The UNSW _ NB 15 dataset used in this study contains comprehensive data for network security intrusion detection, with 175,432 data points and 45 features. In the data preprocessing phase, the goal is to eliminate inconsistencies in the dataset, including cleaning numerical and character data, handling vacancies and outliers. Through one-hot encoding, character-type features are converted to numerical types to accommodate subsequent data processing requirements. For the large extreme difference in the original data, normalization was adopted and adjusted based on the minimum and maximum values of each feature column to improve the performance of the model. In order to address the possible curse of dimensionality caused by high-dimensional data, the association between features and labels was analyzed by the Pearson correlation coefficient. Features with correlation above 0.3 were selected as candidates for model training, achieving dimensionality reduction while avoiding possible performance problems caused by repeated features. After preprocessing, the valid data was reduced to 81,173 samples and the feature dimension decreased to 15. However, the preprocessed datasets, with the most sample and the backdoor attack category, still suffer from category imbalance.

3.3 Implementation of the Data-Balancing Strategy

In the experimental setting of machine learning, the UNSW _ NB 15 network intrusion dataset is studied in depth. The dataset contains 175,432 instances and 45 feature dimensions, while in the selected sample set, the data and features were finely picked. In the data preprocessing stage, the focus is on cleaning various data including numerical and character types. During the processing process, missing values and abnormal values are solved to ensure data consistency. Character type data are converted to numerical type by one-hot encoding to meet the requirements of the algorithm. At the same time, in order to deal with the extreme poor problems in the data and improve the processing performance of the model, the data is normalized. The formula is as follows:

$$X_{\text{scaled}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

In this formula, X represents the original data and is the minimum value, while the maximum value. $X_{\min}$ $X_{\max}$;

In response to the curse of dimensionality problem posed by high-dimensional data, this study used the Pearson coefficient to assess the correlation between features and labels. The correlation analysis is implemented according to the following formula:

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y} = \frac{E\left[\left(X-\mu_X\right)(Y-\mu Y)\right]}{\sigma_X \sigma_Y}$$

$\operatorname{cov}(X,Y)$ $\sigma_X \sigma_Y$ μ_X μ_Y Where, is the sample covariance between X and Y, the sample standard deviation of X and Y, their sample mean, and E is a function of taking the mean.

By using Pearson coefficient, we selected features with label correlation exceeding 0.3, achieved dimension reduction and reduced the impact of redundant features on model performance, and obtained 81,173 data containing 15 feature dimensions. After completing the initial processing of the dataset, the experiment took the steps of data rebalance in the original UNSW _ NB 15 dataset. A hierarchical data partitioning strategy was used, with 70% of the data as the training set and 30% as the test set, to ensure the diversity and comprehensiveness of the dataset. For categories with sample numbers of less than 300, we were oversampled using the modified SMOTE algorithm to increase the sample size of these categories to five times the original size. For categories with sample numbers between 5,000 and 20,000, random undersampling was used to reduce the sample size to half the original size. For categories with sample numbers over 20,000, a more aggressive strategy was used to retain only a quarter of the original sample size. These rebalancing measures not only solve the category imbalance problem, but also reduce the computational burden in the model training process by reducing the amount of data.

4 Experimental Analysis

4.1 Verify the Model Fit

Choosing the appropriate model parameters is crucial in developing machine learning models, especially when processing complex datasets. XGBoost Because of its parameter flexibility, the model shows a powerful ability in many aspects, especially in dealing with unbalanced data sets. As shown in Table 1, the key parameters of the XGBoost model were carefully optimized, including the learning rate, number of base learners, maximum depth of the tree, proportion of subsampling, and penalty terms. These parameters are automatically adjusted using a genetic algorithm, which is known for finding the best performing parameter configurations in the gradient lifting framework. The algorithm settings include the encoding of binary and Gray codes, 10 initial population numbers, 40 iterations, crossover probability of 0.8 and variation probability of 0.1, evaluating model performance using 3-fold cross-validation with the goal of achieving high fit on the test set.

Table 1 XGBoost Default Parameters Versus Optimized Parameters

parameter	Windows default	Optimize the value
learning rate	0.1	0.02
Number of base learner units	100	121
Maximum depth of the tree	6	8
Subsampling ratio	1	0.82
penalty term	0	0.1

After parameter optimization, the XGBoost model exhibits more stable volatility in processing the rebalancing training set. By comparing the parameter configuration before and after optimization. For example, the learning rate parameter is adjusted to update the step size with control to avoid overfitting; the number and maximum depth of tree models are optimized to prevent the model from becoming too complex, and the adjustment of subsampling rate and penalty items also aims to avoid overfitting and ensure the ability of the model to generalize the data set.

4.2 Network Data Feature Analysis and Model Optimization

In the field of network security, the analysis of data flow information is critical to identifying potential network threats. By exploiting the feature importance assessment capability of the XGBoost algorithm, the features can effectively affect the model classification accuracy. Analysis of the rebalancing training set revealed that a total of 10 features played a key role in the classification results of the model. Especially in TCP connections, temporal features such as synack, tcprtt and ackdat are important to determine whether the data is an abnormal attack.

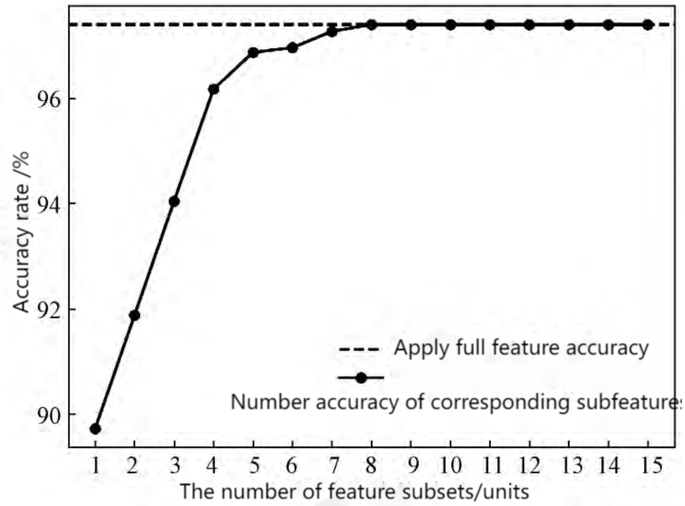

Figure 4 Experimental results for setting different feature threshold proportions

As shown in Figure 4, the experiment was conducted by setting different feature threshold proportions, and the results showed that with the increase of the number of feature subsets, the overall accuracy of the model gradually increased and reached a steady state. When the number of feature subsets is 8, the accuracy of the model reaches an initial equilibrium point, indicating that these eight features play a key role in correctly classifying the network data flow. These eight features were further divided into four key features (synack, tcprtt, ackdat, attcak_cat_Exploits) and four important features (attcak_cat_Analysis, attcak _ cat _ Dos, attcak_cat_Normal, service _ dns). The key features are closely related to the stable operation of network protocol and the security of operating system. The important features are related to external connection and attack behavior, emphasizing the importance of maintaining normal system services and enhancing network protection.

4.3 Practical Application Analysis

The improved SMOTE + GA-XGBoost model proposed in this study is verified on the industrial information security platform of Liaoning Province. By introducing Trojan programs and collecting packet information using the wireshark tool, 1000 data were collected, of which 234 were labeled as abnormal and 766 as normal. The dataset was divided into 70% training set and 30% test set to calculate the model accuracy (Acc) and F1-score. Compared with other machine learning models (MLP, KNN, decision tree and random forest), the model in this study showed excellent performance in identifying abnormal data, achieving a high single item detection rate and F1-

score, and effectively improving the detection effect of data from a small number of samples. Specific performance pairs are shown in Table 2:

Table 2. Actual performance comparison situation

class	MLP	KNN	decision tree	RF	XGBoost	This article model
0	0.99	0.99	0.97	0.99	0.99	0.99
1	0.96	0.94	0.98	0.96	0.97	0.99
F1-score	0.977	0.967	0.966	0.976	0.981	0.986
Acc (%)	98.33	97.67	97.67	98.33	98.67	99.00

5 Conclusion

In order to solve the problem of data imbalance and feature relationship complexity in the field of network security, this study proposes a new machine learning classification method, which combines improved SMOTE technology and genetic algorithm optimization for XGBoost (GA-XGBoost). This method achieves sample balance by introducing local outlier factors in the SMOTE process for oversampling of the minority class samples and random undersampling of the majority class samples. Meanwhile, the evolutionary iterative advantage of the GA was used to optimize the XGBoost model parameters and improve the model fit. Experimental results on the UNSW _ NB 15 dataset show that the proposed method shows high classification prediction accuracy, average recall, and average F1-score. In the application of the actual industrial information security platform, the classification accuracy has reached 99%. This study provides an effective solution for improving the classification accuracy under the unbalanced sample state of network security data, and also provides new ideas and methods for the future research in the field of network security.

Acknowledgments

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Author Contributions

Not applicable.

About the Authors

ZHOU, Zhanxin

Affiliation: Northern Arizona University.

XU, Changxin

Affiliation: Northern Arizona University.

QIAO, Yuxin

Affiliation: Northern Arizona University.

NI, Fanghao

Affiliation: Indian Institute of Technology, Guwahati.

XIONG, Jize

Affiliation: Northern Arizona University.

References

[1] Liu, T., Xu, C., Qiao, Y., Jiang, C., & Chen, W. (2024). News Recommendation with Attention Mechanism. Journal of Industrial Engineering and Applied Science, 2(1), 21-26.

[2] Liu, T., Xu, C., Qiao, Y., Jiang, C., & Yu, J. (2024). Particle Filter SLAM for Vehicle Localization. Journal of Industrial Engineering and Applied Science, 2(1), 27-31.

[3] Xu, C., Qiao, Y., Zhou, Z., Ni, F., & Xiong, J. (2024). Accelerating Semi-Asynchronous Federated Learning. arXiv preprint arXiv:2402.10991.

[4] Zhou, Z. (2024, February). ADVANCES IN ARTIFICIAL INTELLIGENCE-DRIVEN COMPUTER VISION: COMPARISON AND ANALYSIS OF SEVERAL VISUALIZATION TOOLS. In The 8th International scientific and practical conference “Priority areas of research in the scientific activity of teachers”(February 27–March 01, 2024) Zagreb, Croatia. International Science Group. 2024. 298 p. (p. 224).

[5] Xu, C., Yu, J., Chen, W., & Xiong, J. (2024, January). DEEP LEARNING IN PHOTOVOLTAIC POWER GENERATION FORECASTING: CNN-LSTM HYBRID NEURAL NETWORK EXPLORATION AND RESEARCH. In The 3rd International scientific and practical conference “Technologies in education in schools and universities”(January 23-26, 2024) Athens, Greece. International Science Group. 2024. 363 p. (p. 295).

[6] Su, J., Jiang, C., Jin, X., Qiao, Y., Xiao, T., Ma, H., ... & Lin, J. (2024). Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review. arXiv preprint arXiv:2402.10350.

[7] Qiao, Y., Jin, J., Ni, F., Yu, J., & Chen, W. (2023). Application of machine learning in financial risk early warning and regional prevention and control: A systematic analysis based on shap. WORLD TRENDS, REALITIES AND ACCOMPANYING PROBLEMS OF DEVELOPMENT, 331.

[8] Qiao, Y., Ni, F., Xia, T., Chen, W., & Xiong, J. (2024, January). AUTOMATIC RECOGNITION OF STATIC PHENOMENA IN RETOUCHED IMAGES: A NOVEL APPROACH. In The 1st International scientific and practical conference “Advanced technologies for the implementation of new ideas”(January 09-12, 2024) Brussels, Belgium. International Science Group. 2024. 349 p. (p. 287).

[9] Ni, F., Zang, H., & Qiao, Y. (2024, January). SMARTFIX: LEVERAGING MACHINE LEARNING FOR PROACTIVE EQUIPMENT MAINTENANCE IN INDUSTRY 4.0. In The 2nd International scientific and practical conference “Innovations in education: prospects and challenges of today”(January 16-19, 2024) Sofia, Bulgaria. International Science Group. 2024. 389 p. (p. 313).

[10] Su, J., Nair, S., & Popokh, L. (2022, November). Optimal Resource Allocation in SDN/NFV-Enabled Networks via Deep Reinforcement Learning. In 2022 IEEE Ninth International Conference on Communications and Networking (ComNet) (pp. 1-7). IEEE.

[11] Zhao, Z., Zhang, N., Xiong, J., Feng, M., Jiang, C., & Wang, X. (2024). Enhancing E-commerce Recommendations: Unveiling Insights from Customer Reviews with BERTFusionDNN. Journal of Theory and Practice of Engineering Science, 4(02), 38-44.

[12] Xiong, J., Feng, M., Wang, X., Jiang, C., Zhang, N., & Zhao, Z. (2024). Decoding sentiments: Enhancing covid-19 tweet analysis through bert-rcnn fusion. Journal of Theory and Practice of Engineering Science, 4(01), 86-93.

[13] Bao, W., Che, H., & Zhang, J. (2020, December). Will_Go at SemEval-2020 Task 3: An accurate model for predicting the (graded) effect of context in word similarity based on BERT. In Proceedings of the Fourteenth Workshop on Semantic Evaluation (pp. 301-306).

[14] Su, J., Nair, S., & Popokh, L. (2023, February). EdgeGym: A Reinforcement Learning Environment for Constraint-Aware NFV Resource Allocation. In 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.

[15] Su, J., Nair, S., & Popokh, L. (2022, November). Optimal Resource Allocation in SDN/NFV-Enabled Networks via Deep Reinforcement Learning. In 2022 IEEE Ninth International Conference on Communications and Networking (ComNet) (pp. 1-7). IEEE.

[16] Xiao, X. Y., An, S., Guo, F., Li, X., & Liang, Z. (2023, September). How Optimization Algorithm Can Contribute to Sustainability Development-A Case of Nepal. In Proceedings of the 2023 6th International Conference on Big Data Technologies (pp. 189-194).

[17] Xiao, X. Y., An, S., Guo, F., Li, X., & Lyu, C. (2023, September). Assessing the Impact of Olympic Games: A Study Based on Big Data Mining and Analysis. In Proceedings of the 2023 6th International Conference on Big Data Technologies (pp. 141-145).

[18] Guo, F. (2023, July). A Study of Smart Grid Program Optimization Based on K-Mean Algorithm. In 2023 3rd International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT) (pp. 711-714). IEEE.

[19] Guo, F., Wu, J. Z., & Pan, L. (2023, July). An Empirical Study of AI Model’s Performance for Electricity Load Forecasting with Extreme Weather

Conditions. In International Conference on Science of Cyber Security (pp. 193-204). Cham: Springer Nature Switzerland.

[20] Bian, J., Wang, L., Yang, K., Shen, C., & Xu, J. (2023). Accelerating Hybrid Federated Learning Convergence under Partial Participation. arXiv preprint arXiv:2304.05397.

[21] Wang, H., Bian, J., & Xu, J. (2023). On the Local Cache Update Rules in Streaming Federated Learning. arXiv preprint arXiv:2303.16340.

[22] Bian, J., Shen, C., & Xu, J. (2023, March). Federated Learning via Indirect Server-Client Communications. In 2023 57th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-5). IEEE.

[23] Bian, J., & Xu, J. (2022). Mobility improves the convergence of asynchronous federated learning. arXiv preprint arXiv:2206.04742.

[24] Bian, J., Fu, Z., & Xu, J. (2021). FedSEAL: Semi-supervised federated learning with self-ensemble learning and negative learning. arXiv preprint arXiv:2110.07829.

[25] Xu, J., & Sen, S. (2021). Decision Intelligence for Nationwide Ventilator Allocation During the COVID-19 Pandemic. SN Computer Science, 2(6), 423.

[26] Deng, Y., Kesselman, C., Sen, S., & Xu, J. (2019, December). Computational operations research exchange (core): A cyber-infrastructure for analytics. In 2019 Winter Simulation Conference (WSC) (pp. 3447-3456). IEEE.

[27] Xiaobin, L., Changlin, Y., & Wanting, W. (2023). CARASSISTNET: DESIGN AND IMPLEMENTATION OF A DRIVING ASSISTANCE SYSTEM USING COMPUTER VISION. Ответственный редактор, 28.

[28] Yuan, C., Liu, X., & Zhang, Z. (2021, May). The Current Status and progress of Adversarial Examples Attacks. In 2021 International Conference on Communications, Information System and Computer Engineering (CISCE) (pp. 707-711). IEEE.

[29] Xiao, T., Zeng, L., Shi, X., Zhu, X., & Wu, G. (2022, September). Dual-Graph Learning Convolutional Networks for Interpretable Alzheimer's Disease Diagnosis. In International Conference on Medical Image Computing and Computer-Assisted Intervention (pp. 406-415). Cham: Springer Nature Switzerland.

[30] Jin, X., & Wang, Y. (2023). Understand Legal Documents with Contextualized Large Language Models. arXiv preprint arXiv:2303.12135.