Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026477
Article

Tech Science Press

Optimized Artificial Neural Network Techniques to Improve Cybersecurity of Higher Education Institution

Abdullah Saad AL-Malaise AL-Ghamdi[1], Mahmoud Ragab[2,3,4,*], Maha Farouk S. Sabir[1], Ahmed Elhassanein[5,6] and Ashraf A. Gouda[4]

[1]Information Systems Department, Faculty of Computing and Information Technology King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Centre of Artificial Intelligence for Precision Medicines, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[4]Mathematics Department, Faculty of Science, Al-Azhar University, Naser City, 11884, Cairo, Egypt
[5]Mathematics Department, College of Science, University of Bisha, Bisha, Saudi Arabia
[6]Mathematics Department, Faculty of Science, Damanhour University, Damanhour, Egypt
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa
Received: 28 December 2021; Accepted: 22 February 2022

Abstract: Education acts as an important part of economic growth and improvement in human welfare. The educational sectors have transformed a lot in recent days, and Information and Communication Technology (ICT) is an effective part of the education field. Almost every action in university and college, right from the process from counselling to admissions and fee deposits has been automated. Attendance records, quiz, evaluation, mark, and grade submissions involved the utilization of the ICT. Therefore, security is essential to accomplish cybersecurity in higher security institutions (HEIs). In this view, this study develops an Automated Outlier Detection for CyberSecurity in Higher Education Institutions (AOD-CSHEI) technique. The AOD-CSHEI technique intends to determine the presence of intrusions or attacks in the HEIs. The AOD-CSHEI technique initially performs data pre-processing in two stages namely data conversion and class labelling. In addition, the Adaptive Synthetic (ADASYN) technique is exploited for the removal of outliers in the data. Besides, the sparrow search algorithm (SSA) with deep neural network (DNN) model is used for the classification of data into the existence or absence of intrusions in the HEIs network. Finally, the SSA is utilized to effectually adjust the hyper parameters of the DNN approach. In order to showcase the enhanced performance of the AOD-CSHEI technique, a set of simulations take place on three benchmark datasets and the results reported the enhanced efficiency of the AOD-CSHEI technique over its compared methods with higher accuracy of 0.9997.

Keywords: Higher security institutions; intrusion detection system; artificial intelligence; deep neural network; hyperparameter tuning; deep learning

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

The network environment of education institutions is uncontrollable, with different types of users namely residents, researchers, students, faculty, etc. [1]. There are several incidences where information in education institutions was the aim of hacking attempts. In education institutions, several measures have been taken to control suspected traffics. Novel attack takes advantage of computer vulnerability that doesn't have a solution at present. They are hard to identify, through reactive and proactive security methods. There is two technique for detecting attacks –anomaly detection and signature-based detection. Signature-based detection depends on matching attack patterns with signatures saved in a repository [2]. This technique isn't effective with attacks that signature is unavailable. In anomaly detection, standard profile pattern is preserved and any deviation or abnormality from this pattern is described. Anomaly detection could identify novel attacks; however, it leads to a higher amount of false positives. This approach requires heavy human contribution to upgrade signature repository and standard profiles. This is a time-consuming and expensive procedure [3]. The upgrading speed is slower when compared to the speed of new intrusion. Novel attack discovery needs defenders to be on-guard, however, this is impossible for automatically interfaced system. Few types of automated defense method are needed for preventing this attack. Automated signature generation and attack detection schemes support intrusion detection systems (IDS) to report and capture this attack. No single approach could assist in resolving this issue. Integration of methods–like signature generation algorithm, honeypots, IDS, analysis, and tracking–is required.

Network Intrusion Detection System (NIDS) was rapidly advanced in industry and academia responding to the growing cyberattacks against commercial enterprises and governments worldwide. The yearly cost of cybercrime is rising endlessly [4]. The more disturbing cybercrimes are resulting from denial of services, web-based attacks, and malicious insiders. Organizations could lose the intellectual property with this malevolent software crept into the network that might result in disruption to a country's critical national framework. Organization deploys antivirus software, firewall, and NIDS for securing computer systems from unauthorized accessing [5]. One of the attentive areas to solve cyberattacks rapidly is to distinguish the attack method earlier from the system utilizing NIDS. The NIDS is developed for detecting malevolent activity includes distributed denial of service (DDoS), virus, and worm attacks. The crucial factor for NIDS is reliability abnormality, detection speed, and accuracy. To fulfill the requirement of an IDS, the researcher has discovered the likelihood of utilizing machine learning (ML) and deep learning (DL) methods [6]. The two technique comes under the class of artificial intelligence (AI) and aims at learning effective data from the big data. This technique has received much recognition in the fields of network security [7], in the past few years because of the development of graphics processor units (GPU). The above two methods are effective tools in learning important features from the network traffics and predicting the normal and abnormal events on the basis of learned patterns [8]. The ML-based IDS heavily based on feature engineering for learning important data from the network traffics. Meanwhile, DL-based IDS don't depend on feature engineering and are good at learning complicated features automatically from the raw information because of their deep framework.

Vinayakumar et al. [9] define how consecutive data modelling is a related process in Cybersecurity. Sequence is temporal features implicitly or explicitly. The recurrent neural network (RNN) method is a set of artificial neural network (ANN) that has seemed as a principle, powerful method for learning dynamic temporal behavior in a random length of largescale sequence data. Moreover, stacked RNN (S-RNN) has the possibility of quickly learning complicated temporal behavior, involving sparse representation. Agarwal et al. [10] introduced a certain factor that makes complex for an IDS to detect and monitor web-based attacks. Also, the study presents a complete review of the current detection

system developed exclusively for observing web traffics. Moreover, recognize different dimensions to compare the IDS from distinct perceptions based on the functionality and design. Also, we presented a conceptual architecture of web-based IDS with a prevention method for offering systematic guidelines for the system performance.

Zhou et al. [11] present an IDS method and it is depending on the ensemble learning and feature selection methods. Initially, a heuristic method named correlation based feature selection (CFS)-bat algorithm (BA) is presented for reduction dimension that chooses optimum subset on the basis of correlations among the features. Next, present an ensemble model which integrates C4.5, random forest (RF), and Forest using Penalizing Attribute (Forest PA) algorithm. Akashdeep et al. [12] developed a smart technique that implements feature ranking based on the data correlation and gain. Then, reduction feature is performed by integrating rank attained from data correlation and gain with a method for identifying useless and useful characteristics. This reduction feature is later given to an feed forward neural network (FFNN) model for testing and training on KDD99 datasets.

Jin et al. [13] designed an IDS called SwiftIDS, i.e., able to analyse huge traffic information in higher-speed network at an appropriate time and keep acceptable recognition performance. SwiftIDS accomplishes this aim by two techniques. One method is that light gradient boosting machine (LightGBM) is adapted as the IDS for handling the huge data traffics. Li et al. [14] present effective DL methods such as autoencoder (AE)-IDS based random forest (RF) technique. This approach created the training set with feature grouping and FS. When the training process gets completed, the method could forecast the fallouts with AE that significantly decreases the recognition time and efficiently enhanced the predictive performance.

This study presented a novel automated outlier detection technique for cybersecurity in higher education institutions (HEI), named AOD-CSHEI technique. The AOD-CSHEI technique originally executes data pre-processing in two stages namely data conversion and class labelling. Also, the Adaptive Synthetic (ADASYN) is exploited for the removal of outliers in the data. Further, the sparrow search algorithm (SSA) with DNN model is used for classifying the data into the existence or absence of intrusions in the HEIs network. Lastly, the SSA is utilized to effectually adjust the hyper parameter of the DNN. To demonstrate the improved outcomes of the AOD-CSHEI technique, a wide ranging experimental analysis is carried out using three benchmark datasets.

The remaining sections of the paper is organized as follows. Section 2 elaborates the proposed model, Section 3 offers the performance validation, and Section 4 draws the conclusion.

2 The Proposed AOD-CSHEI Technique

This study has presented a new AOD-CSHEI technique to identify the presence of intrusions or attacks in the HEIs and the overall process is given in Fig. 1. At the initial stage, the input data is pre-processed in two stages namely data conversion and class labelling. The AOD-CSHEI technique performs different subprocesses namely pre-processing, ADASYN based outlier detection, DNN based classification, and SSA based hyperparameter tuning. In this work, the SSA with DNN model is used for the classification of data into the existence or absence of intrusions in the HEIs network and the SSA is utilized to effectually adjust the hyper parameters of the DNN model.

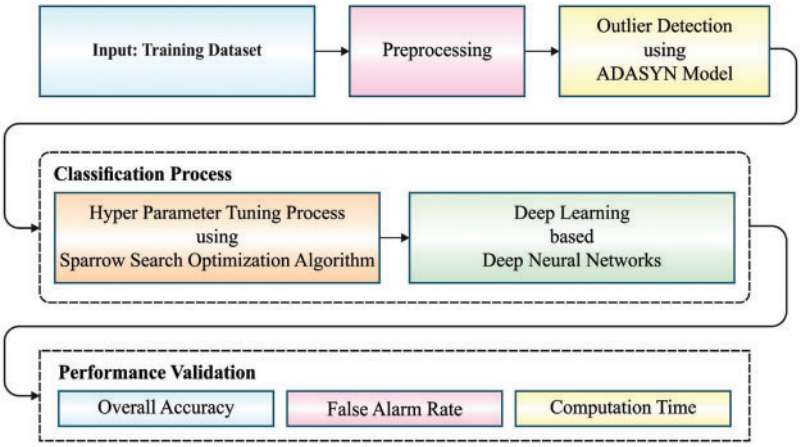

Figure 1: Overall working process of AOD-CSHEI technique

2.1 ADASYN Based Outlier Detection

During the removal of outlier's process, the ADASYN technique receives the pre-processed data as input to eradicate the outliers that exist in it. The fundamental concept of ADASYN technique is to describe the weight distribution of minority sample by determining the degree of learning difficulty of minority sample [15]. For binary classification problems, the dataset D_{tr} of m samples are formulated by $\{x_i, y_i\}$, in which $i = 1, \ldots, m, x_i$ indicates a sample of n-dimension feature space X, and y_i represent the label of sample $x_i, y_i \in Y = \{-1, 1\}$. The amount of majority sample represents m_l, and the amount of minority sample represent m_s. Once d_{th} is 1, it implies that it could be accepted when the amount of samples in distinct classes is equivalent. $\beta \in [0, 1]$ indicates a variable utilized to set the balanced degree of synthetic data set afterward creating sample. When $\beta = 1$, the dataset to generate a new sample would be balanced completely [16], i.e., the amount of sample in distinct classes is equal. K denotes the parameter to find KNN. For the generated sample set S returned by the approach, it would be fused with the original dataset D_{tr} into a novel dataset as a training set. This approach creates further novel instances in the area wherein learning is complex for minority sample that could efficiently reinforce the model learning of minority sample therefore enhancing the model recognition rate of minority sample prediction.

2.2 DNN Based Classification Model

At this stage, the DNN model gets executed to determine the presence of intrusions or attacks in the HEIs. The DNN is a network system i.e., depending upon DL approach. This technique is extensively applied in the image classification, computational biology, and signal prediction fields due to its benefits namely ease of understanding and simple structure. The internal architecture of the DNN comprises input, output, and hidden layers; each layer is fully connected. The input layer has m neuron, as well as w and b, denote the weight and bias, correspondingly [17]. The gradient backpropagation method is employed for updating parameters in the DNN. This parameter includes bias b and weight w of all the connection layers. There might be an unavoidable error between the output and the input sample label at the time of network training. Once the DNN method begins to train, few initialized network parameter needs to be fixed namely network model parameter (the amount of neurons from the hidden layers, the amount of neurons from the input layer, the amount

of neurons in the output layer, and the activation function), epoch, momentum, batch size, initial learning rate.

2.3 SSA Based Hyperparameter Tuning Process

For boosting the efficacy of the DNN, the SSA is applied to properly tune the hyper parameter of the DNN. In general, sparrow is the type of bird i.e., more common one since it tends to relate with group and survives more near to us. For experimental purpose, virtual sparrow is utilized for searching food source. The position of the sparrow is determined as follows:

$$X = \begin{bmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,d} \\ \chi_{2,1} & \chi_{2,2} & \cdots & \chi_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ \chi_{n,1} & \chi_{n,2} & \cdots & \chi_{n,d} \end{bmatrix}, \tag{1}$$

In which n indicates the amount of sparrows and d denotes the dimensional of parameter that must be tuned as follows:

$$F_X = \begin{bmatrix} f([x_{1,1} & x_{1,1} & \cdots & \cdots & x_{1,d}]) \\ f([x_{1,1} & x_{2,2} & \cdots & \cdots & x_2, d]) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f([x_{n,1} & x_{n,2} & \cdots & \cdots & x_{n,d}]) \end{bmatrix} \tag{2}$$

While the values existing in all the rows of F_x determines the fitness value of each individual. In SSA, the producer with optimum fitness value has the importance of attained food in the search method [18]. Also, the producer's sparrow takes responsibility for guiding the motion of the entire population and searching for food.

$$x_{i,j}^{t+1} = \{if\, R_2 < STif\ R \geq ST, \tag{3}$$

$$x_{i,j}^{t+1} = \begin{cases} X_{i,j}^t \cdot \exp\left(\dfrac{-i}{\alpha \cdot iter\_ \max}\right) & if\ R_2 < ST \\ X_{i,j}^t + Q.L & if\ R_2 \geq ST \end{cases} \tag{4}$$

In the equation, t denotes the existing iteration, $j = 1, 2, \ldots, d$. $\chi_{i,j}^t$ determines the value of *jth* parameter of *ith* sparrow. As well, *iter*_ max is a constant with various rounds. $\alpha \in (0, 1]$ denotes arbitrary value R_2 ($R_2 \in [0, 1]$) and ST ($ST \in [0.5, 1.0]$) determine the alarm values and the safety thresholds along with, O denoting a random value following the standard distribution and L represents a matrix of $1 \times d$ where all the elements within 1. Fig. 2 illustrates the flowchart of SSA.

1. When $R_2 < ST$, it shows the absenteeism of predator and the producer enters to a search process
2. When $R_2 = ST$, it shows that few sparrows have found the predator, and all the sparrows should fly to a safe place at a fast speed.

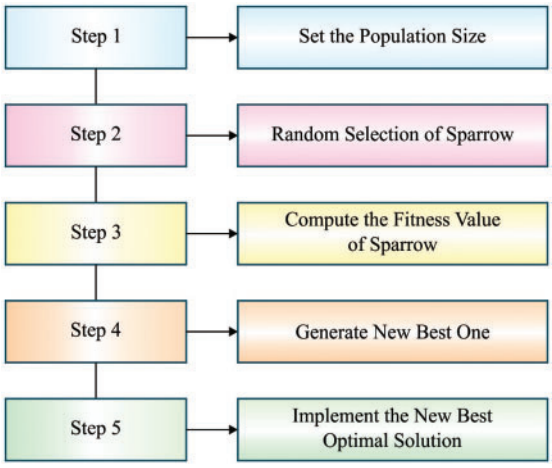

Figure 2: Flowchart of SSA

In the event of scrounger, it is essential for enforcing the rules (1) and (2). After winning the battle, they obtain producer food instantaneously; otherwise, they persevere to achieve the rules (1) and (2):

$$X_{i,j}^{t+1} = \begin{cases} Q \cdot \exp\left(\dfrac{X_{Worst-X_{i,j}^{t}}^{r}}{i^2}\right) & if\ i > n/2 \\ X_P^{t+1} + \left|X_{i,j}^{t} - X_P^{t+1}\right| A^{+} \cdot L & otherwise \end{cases} \tag{5}$$

In the equation, X_P denotes the optimal location reached by producer, X_{worst} characterizes the existing global worst position, A describes a matrix of $1 \times d$ where all the elements within 1 or -1, and $A^{+} = A^{T}(AA^{T})^{-1}$. if $i > n/2$, it can be suggested that the *ith* scrounger with the worst fitness values is more possible that hungry. At the simulation time, the sparrow is considered as the one that is danger aware in ten to twenty percent of the overall population. The initial location of the sparrow is made randomly in the population. According to the rules, it is arithmetically determined by:

$$X_{ij}^{t+1} = \begin{cases} X_{best}^{t} + \beta \cdot \left|X_{ij}^{t} - X_{best}^{t}\right| & if\ f_i > f_g \\ \chi_{ij}^{t} + K \cdot \left(\dfrac{\left|X_{ij}^{t} - X_{worst}^{t}\right|}{(f_i - f_w) + \varepsilon}\right) & if\ f_i = f_g' \end{cases} \tag{6}$$

In which X_{best} indicates the existing global optimal position, β denotes the step size control variable, is a standard distribution of arbitrary numbers with a variance of 1and mean values of 0. $K \in [-1, 1]$ indicates an arbitrary value. Now f_i indicates the fitness values of the existing sparrow f_g and f_w shows the existing global optimum and worse fitness values, respectively ε denote the smaller constant utilized for eliminating the zero-division-error. When $f_i > f_g$, it is represented that the sparrow existing at the edge of swarm, X_{best} describes the location of the middle of the population and is secured around it. $f_i = f_g$ shows that the sparrow in the center of population is aware of the risks and moves closer to another sparrow and K describe the path of the sparrow motion.

OBL is a powerful mechanism utilized for optimization to increase the convergence speed of distinct metaheuristic approaches [19]. The efficient model of the OBL includes the validation of the existing population in the similar round to describe the optimum candidate for given problems. The idea of OBL was applied efficiently in and the concept of opposite value is needed to be determined for describing OBL.

3 Experimental Validation

In this section, the experimental result analysis of the AOD-CSHEI methodology takes place using three benchmark dataset [20]. A comparative analysis is made with decision tree (DT), logistic regression (LR), Naïve Bayesian (NB), ANN, support vector machines (SVM), Adaboost, and LightGBM techniques.

Tab. 1 provides a detailed comparative study of the AOD-CSHEI technique with existing techniques on the test NSL-KDD data set. Fig. 3 offers the accuracy analysis of the AOD-CSHEI technique and existing techniques on the testing and training of NSL-KDD datasets.

Table 1: Result analysis of AOD-CSHEI technique on NSL-KDD dataset

Methods	Training set			Testing SET		
	Accuracy	FAR	Time (min)	Accuracy	FAR	Time (min)
Decision tree	0.9382	0.0890	09.37	0.8105	0.1237	1.47
Logistic regression	0.9380	0.0640	30.15	0.7832	0.1476	2.20
Naive bayesian	0.8166	0.0480	23.23	0.7656	0.1560	2.15
ANN	0.9226	0.0387	16.17	0.7741	0.1421	8.05
SVM	0.9904	0.0650	127.03	0.6952	0.1298	14.85
Adaboost	0.9478	0.0264	49.00	0.8921	0.0978	6.27
LightGBM	0.9889	0.0223	03.35	0.8979	0.0913	0.88
AOD-CSHEI	0.9936	0.0610	03.04	0.9152	0.0324	0.67

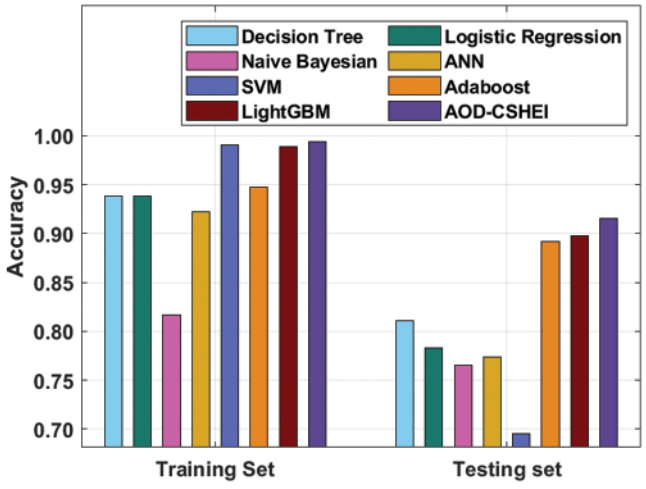

Figure 3: Accuracy analysis of AOD-CSHEI technique on NSL-KDD dataset

The outcomes illustrated that the NB model has shown ineffectual outcomes with the least values of accuracy. At the same time, the ANN, DT, and LR models have obtained slightly improved values of accuracy. Followed by, the Adaboost model has resulted in moderately increased accuracy values. Though the LightGBM and SVM techniques have reached reasonable accuracy values, the presented AOD-CSHEI technique has accomplished maximum training and testing accuracy of 0.9936 and 0.9152 respectively.

Next, the training time (TRT) and testing time (TST) analysis of the AOD-CSHEI approach take place on NSL-KDD dataset has been demonstrated in Fig. 4. The figure reported that the SVM method has showcased worse outcomes with the maximum values of TRT and TST. In line with, the Adaboost model has obtained slightly reduced TRT and TST. Followed by, the LR, NB, and ANN models have accomplished somewhat decreased values of TRT and TST. Although the DT and LightGBM models have resulted in reasonable values of TRT and TST, the presented AOD-CSHEI technique has reached to effective outcome with the lower TRT and TST values of 3.04 min and 0.67 min respectively.

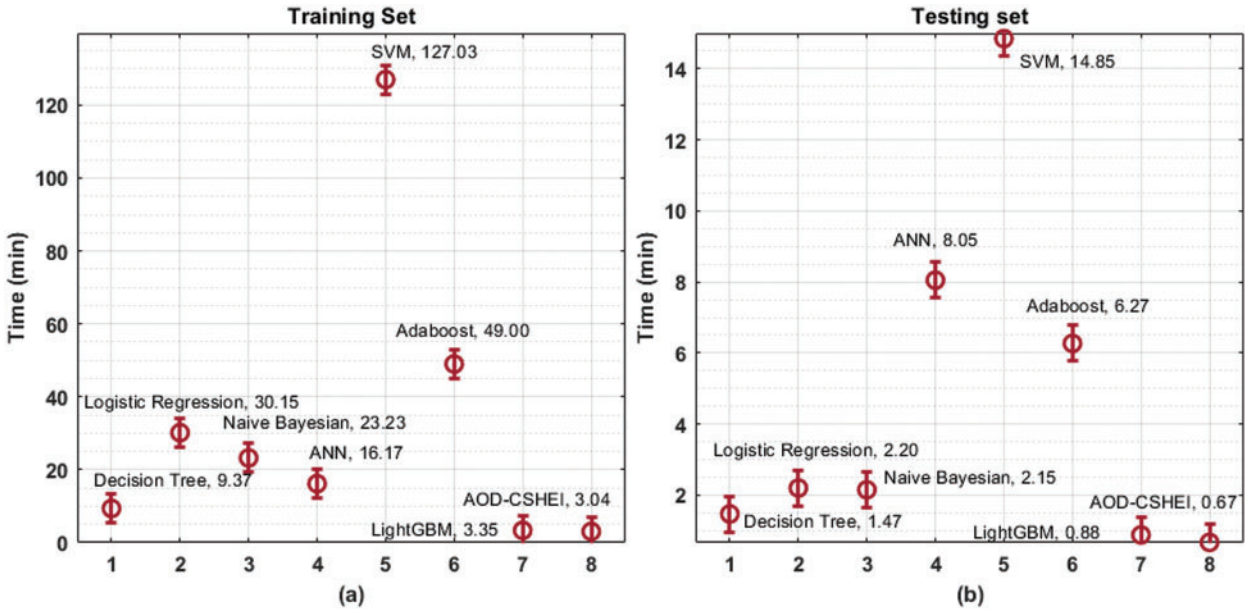

Figure 4: Time analysis of AOD-CSHEI technique on NSL-KDD dataset

Fig. 5 demonstrates the ROC analysis of the AOD-CSHEI methodology on NSL-KDD dataset. The figure exposed that the AOD-CSHEI technique has reached enhanced outcome with the minimum ROC of 99.9714.

Tab. 2 offers a detailed comparative study of the AOD-CSHEI technique with existing techniques on the test UNSW-NB15 dataset. Fig. 6 provides the accuracy analysis of the AOD-CSHEI approach and existing methods on the training and testing set of UNSW-NB15 datasets. The results demonstrated that the NB system has exhibited ineffectual outcomes with the least values of accuracy. At the same time, the ANN, DT, and LR approaches have reached somewhat higher values of accuracy. Then, the Adaboost model has resulted in moderately increased accuracy values. Afterward, the LightGBM and SVM technique has reached reasonable accuracy values, the projected AOD-CSHEI technique has accomplished maximum training and testing accuracy of 0.8918 and 0.8852 correspondingly.

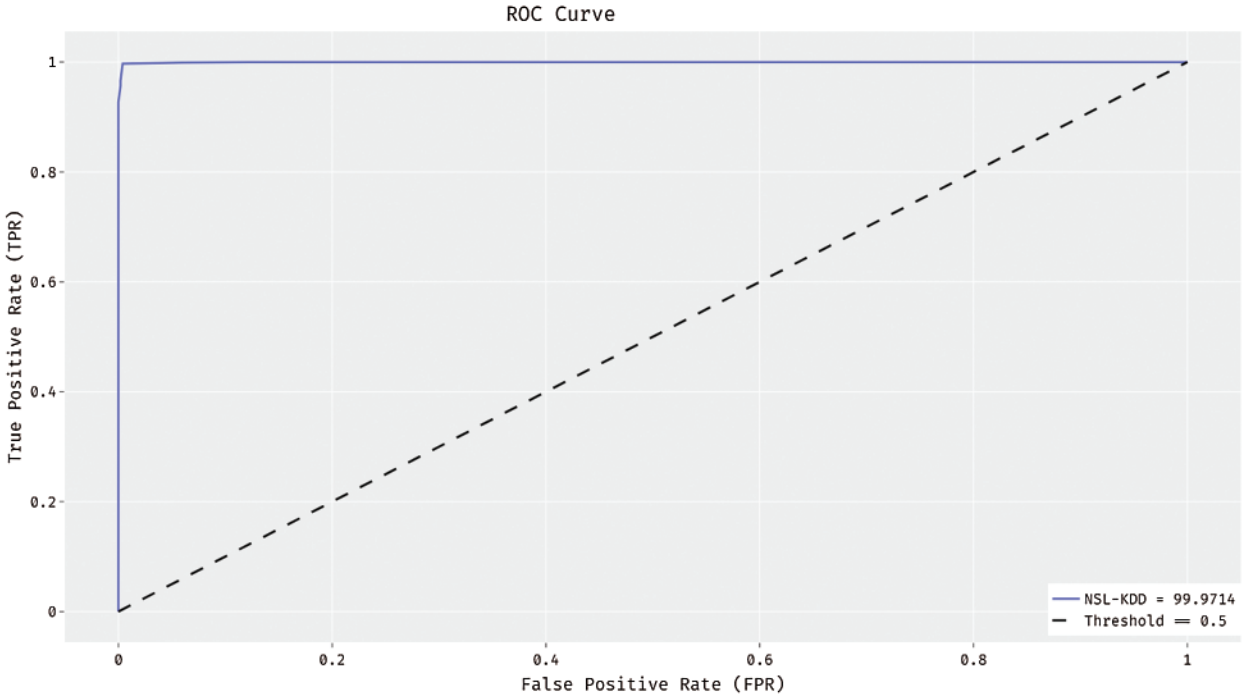

Figure 5: ROC analysis of AOD-CSHEI technique on NSL-KDD dataset

Table 2: Result analysis of AOD-CSHEI technique on UNSW-NB15 dataset

Method	Training set			Testing set		
	Accuracy	FAR	Time (min)	Accuracy	FAR	Time (min)
Decision tree	0.8556	0.1578	12.57	0.7571	0.1834	1.57
Logistic regression	0.8315	0.1848	34.85	0.7165	0.2341	2.62
Naive bayesian	0.8207	0.1856	26.50	0.5604	0.3100	2.48
ANN	0.8134	0.2113	128.15	0.7021	0.2453	15.17
SVM	0.8587	0.1764	82.15	0.6721	0.2242	6.63
Adaboost	0.8652	0.1423	4.15	0.8367	0.1943	1.13
LightGBM	0.8711	0.1342	1.05	0.8398	0.1878	0.47
AOD-CSHEI	0.8918	0.1267	0.54	0.8852	0.1298	0.36

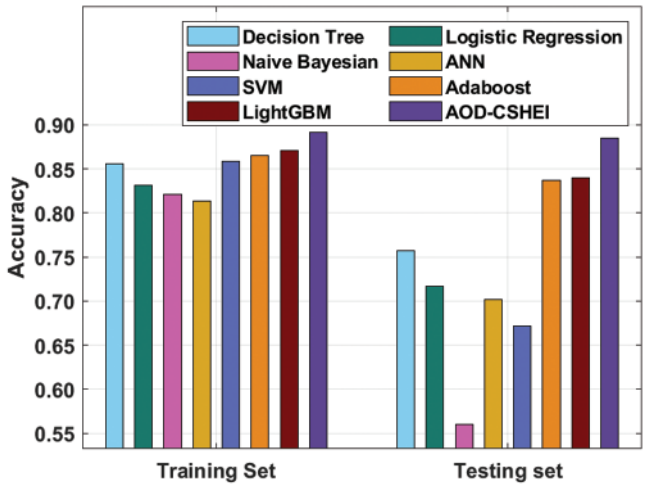

Figure 6: Accuracy analysis of AOD-CSHEI technique on UNSW-NB15 dataset

Next, the TRT and TST analysis of the AOD-CSHEI technique take place on UNSW-NB15 dataset is exhibited in Fig. 7. The figure obvious that the SVM algorithm has illustrated least outcome with the superior values of TRT and TST. Likewise, the Adaboost system has obtained slightly decreased TRT and TST. Followed by, the LR, NB, and ANN models have accomplished somewhat lower values of TRT and TST. But, the DT and LightGBM methodologies have resulted in reasonable values of TRT and TST, the presented AOD-CSHEI technique has reached to effectual outcome with the lower TRT and TST values of 0.54 min and 0.36 min correspondingly.

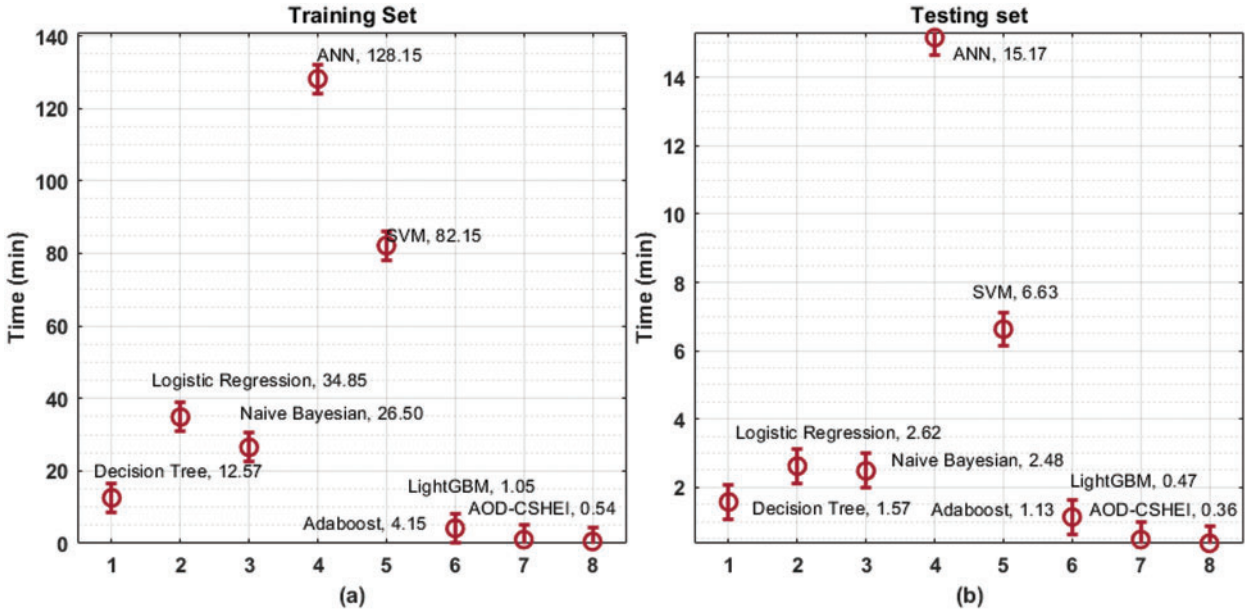

Figure 7: Time analysis of AOD-CSHEI technique on UNSW-NB15 dataset

Fig. 8 showcases the Receiver operating characteristic (ROC) curve analysis of the AOD-CSHEI technique on UNSW-NB15 dataset. The figure exposed that the AOD-CSHEI approach has attained improved outcomes with the reduced ROC of 96.7291.

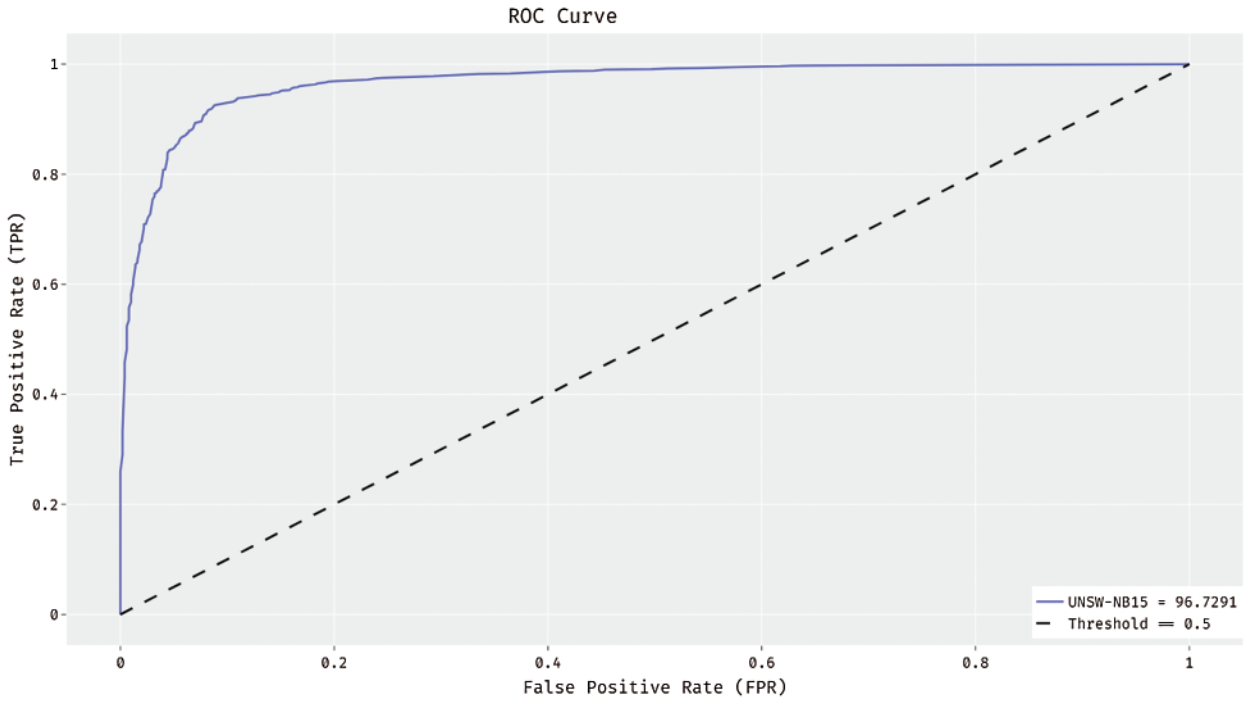

Figure 8: ROC analysis of AOD-CSHEI technique on UNSW-NB15 dataset

Tab. 3 gives a detailed comparative study of the AOD-CSHEI method with existing techniques on the test CICIDS2017 dataset. Fig. 9 offers the accuracy analysis of the AOD-CSHEI technique and existing techniques on the training and testing set of CICIDS2017 dataset. The outcomes demonstrated that the NB technique has revealed ineffectual outcomes with the least values of accuracy. Simultaneously, the ANN, DT, and LR models have obtained slightly increased values of accuracy. Similarly, the Adaboost approach has resulted in moderately enhanced accuracy values. Though the LightGBM and SVM techniques have reached reasonable accuracy values, the presented AOD-CSHEI technique has accomplished maximum training and testing accuracy of 0.9997 and 0.9991 correspondingly.

Table 3: Result analysis of AOD-CSHEI technique on CICIDS2017 dataset

Methods	Training set			Testing set		
	Accuracy	FAR	Time (min)	Accuracy	FAR	Time (min)
Decision tree	0.9987	0.0007	20.52	0.9962	0.0023	1.03
Logistic regression	0.9429	0.0298	22.30	0.9255	0.0564	1.72

(Continued)

Table 3: Continued

Methods	Training set			Testing set		
	Accuracy	FAR	Time (min)	Accuracy	FAR	Time (min)
Naive bayesian	0.9401	0.0022	5.57	0.9390	0.0021	2.43
ANN	0.9947	0.0017	67.10	0.9946	0.0017	12.02
SVM	0.8146	0.1799	83.90	0.8152	0.1792	2.40
Adaboost	0.9946	0.0031	37.67	0.9946	0.0030	0.80
LightGBM	0.9993	0.0003	3.30	0.9986	0.0008	0.20
AOD-CSHEI	0.9997	0.0002	2.56	0.9991	0.0004	0.14

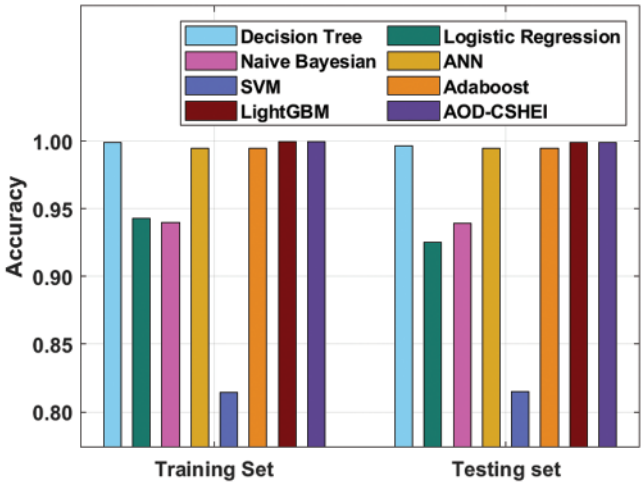

Figure 9: Accuracy analysis of AOD-CSHEI technique on CICIDS2017 dataset

Afterward, the TRT and TST analysis of the AOD-CSHEI technique take place on CICIDS2017 dataset is depicted in Fig. 10. The figure revealed that the SVM model has showcased worse outcomes with the maximum values of TRT and TST. Along with that, the Adaboost system has obtained slightly reduced TRT and TST. After that, the LR, NB, and ANN models have accomplished somewhat decreased values of TRT and TST. Although the DT and LightGBM models have resulted in reasonable values of TRT and TST, the presented AOD-CSHEI methodology has gained to effective outcome with the lower TRT and TST values of 2.56 min and 0.14 min correspondingly.

Fig. 11 exhibits the ROC analysis of the AOD-CSHEI approach on CICIDS2017 dataset. The figure exposed that the AOD-CSHEI methodologies have attained improved outcome with the lower ROC of 99.9904. The above mentioned result analysis reported the supremacy of the AOD-CSHEI technique over the recent approaches.

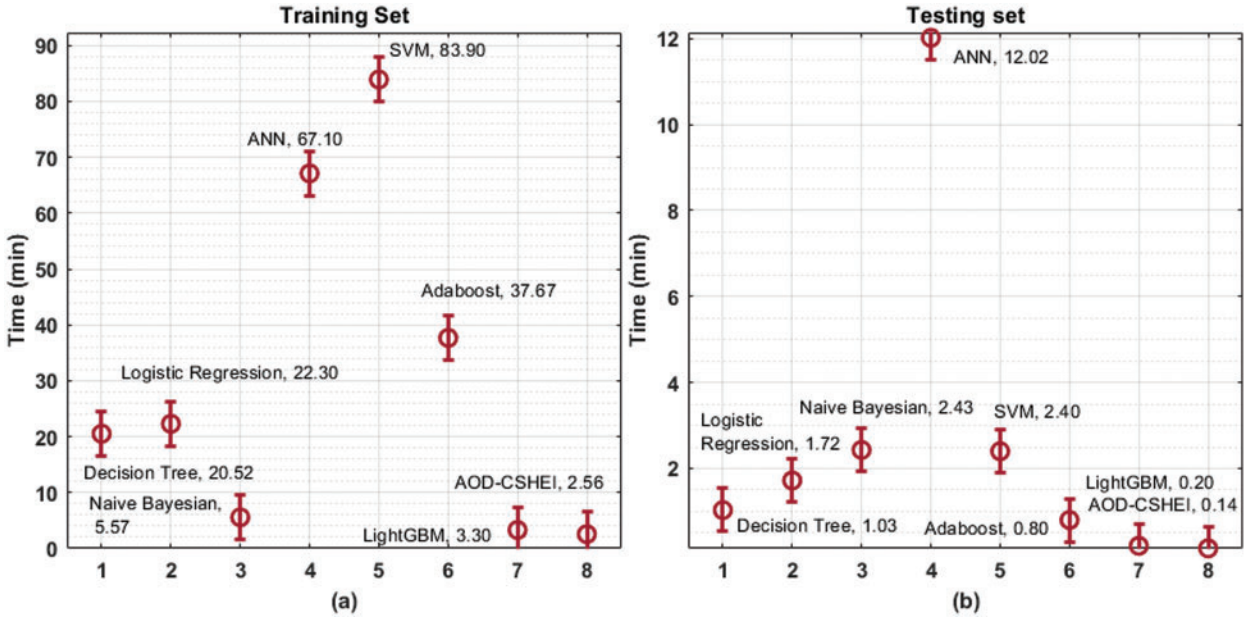

Figure 10: Time analysis of AOD-CSHEI technique on CICIDS2017 dataset

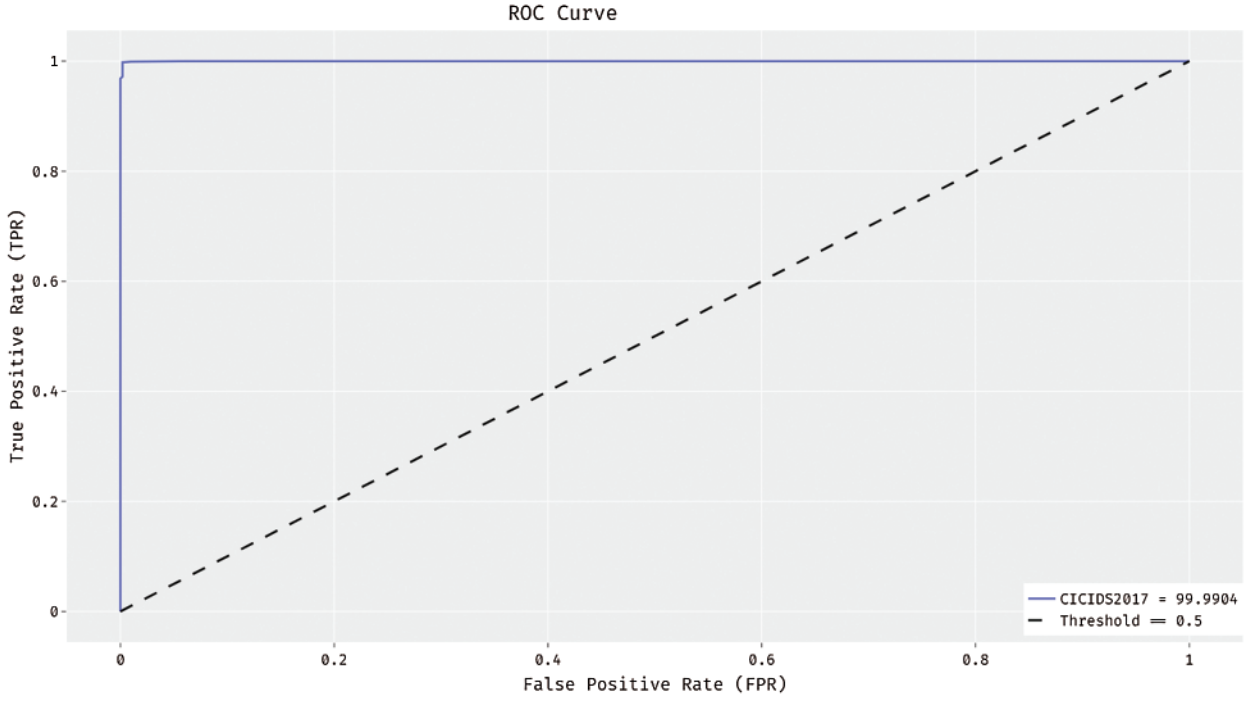

Figure 11: ROC analysis of AOD-CSHEI technique on CICIDS2017 dataset

4 Conclusion

This study has presented a new AOD-CSHEI technique to identify the presence of intrusions or attacks in the HEIs. The AOD-CSHEI technique performs different subprocesses namely preprocessing, ADASYN based outlier detection, DNN based classification, and SSA based hyperparameter tuning. In this work, the SSA with DNN model is used for the classification of data into the existence or absence of intrusions in the HEIs network and the SSA is utilized to effectually adjust the hyper parameters of the DNN model. In order to showcase the enhanced efficacy of the AOD-CSHEI technique, a set of simulations take place on three benchmark datasets and the results reported the enhanced efficiency of the AOD-CSHEI technique over its compared methods. Therefore, the AOD-CSHEI technique has been utilized as an effective tool for cybersecurity in HEIs. In the future, the AOD-CSHEI technique can be placed in the online learning process of HEIs.

Acknowledgement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (IFPRC-154-611-2020) and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: This project was supported financially by Institution Fund projects under grant no. (IFPRC-154-611-2020).

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

References

[1] C. E. Bondoc and T. G. Malawit, "Cybersecurity for higher education institutions: Adopting regulatory framework," *Global Journal of Engineering and Technology Advance*, vol. 2, no. 3, pp. 016–021, 2020.

[2] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, pp. 39, 2021.

[3] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten *et al.,* "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences*, vol. 10, no. 10, pp. 3660, 2020.

[4] E. Kim and R. Beuran, "On designing a cybersecurity educational program for higher education," in *Proc. of the 10th Int. Conf. on Education Technology and Computers -ICETC '18*, Tokyo, Japan, pp. 195–200, 2018.

[5] C.-W. Liu, P. Huang and H. C. Lucas, "Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institution," *Journal of Management Information Systems*, vol. 37, no. 3, pp. 758–787, 2020, https://doi.org/10.2139/ssrn.2850178.

[6] T. Crick, J. H. Davenport, A. Irons, S. Pearce and T. Prickett, "Maintaining the focus on cybersecurity in UK higher education," *ITNOW*, vol. 61, no. 4, pp. 46–47, 2019.

[7] M. Y. Alghamdi and Y. A. Younis, "The use of computer games for teaching and learning cybersecurity in higher education institutions," *Journal of Engineering Research*, vol. 9, no. 3A, pp. 143–152, 2021.

[8] F. B. Schneider, "Cybersecurity education in universities," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 3–4, 2013.

[9] R. Vinayakumar, K. P. Soman and P. Poornachandran, "Evaluation of recurrent neural network and its variants for intrusion detection system (IDS)," *International Journal of Information System Modeling and Design*, vol. 8, no. 3, pp. 43–63, 2017.

[10] N. Agarwal and S. Z. Hussain, "A closer look at intrusion detection system for web applications," *Security and Communication Networks*, vol. 2018, pp. 1–27, 2018.

[11] Y. Zhou, G. Cheng, S. Jiang and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, pp. 107247, 2020.

[12] I. Manzoor and N. Kumar, "A feature reduced intrusion detection system using ANN classifier," *Expert Systems with Applications*, vol. 88, pp. 249–257, 2017.
[13] D. Jin, Y. Lu, J. Qin, Z. Cheng and Z. Mao, "SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism," *Computers & Security*, vol. 97, pp. 101984, 2020.
[14] X. Li, W. Chen, Q. Zhang and L. Wu, "Building auto-encoder intrusion detection system based on random forest feature selection," *Computers & Security*, vol. 95, pp. 101851, 2020.
[15] A. Alhudhaif, "A novel multi-class imbalanced EEG signals classification based on the adaptive synthetic sampling (ADASYN) approach," *PeerJ Computer Science*, vol. 7, pp. e523, 2021.
[16] A. Amin, S. Anwar A. Adnan, M. Nawaz, N. Howard *et al.*, "Comparing oversampling techniques to handle the class imbalance problem: A customer churn prediction case study," *IEEE Access*, vol. 4, pp. 7940–7957, 2016.
[17] Z. Zhu, X. Cui, K. Zhang, B. Ai, B. Shi *et al.,* "DNN-Based seabed classification using differently weighted MBES multifeatures," *Marine Geology*, vol. 438, pp. 106519, 2021.
[18] J. Xue and B. Shen, "A novel swarm intelligence optimization approach: Sparrow search algorithm," *Systems Science & Control Engineering*, vol. 8, no. 1, pp. 22–34, 2020.
[19] J. Adaikalaraj and T. Vengattaraman, "An efficient load scheduling technique using oppositional sparrow search algorithm for cloud computing environment," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 423–432, 2021.
[20] J. Liu, Y. Gao and F. Hu, "A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM," *Computers & Security*, vol. 106, pp. 102289, 2021.