Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026405
Article

Tech Science Press

Enhanced Artificial Intelligence-based Cybersecurity Intrusion Detection for Higher Education Institutions

Abdullah S. AL-Malaise AL-Ghamdi[1], Mahmoud Ragab[2,3,4,*] and Maha Farouk S. Sabir[1]

[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
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa
Received: 24 December 2021; Accepted: 09 February 2022

Abstract: As higher education institutions (HEIs) go online, several benefits are attained, and also it is vulnerable to several kinds of attacks. To accomplish security, this paper presents artificial intelligence based cybersecurity intrusion detection models to accomplish security. The incorporation of the strategies into business is a tendency among several distinct industries, comprising education, have recognized as game changer. Consequently, the HEIs are highly related to the requirement and knowledge of the learner, making the education procedure highly effective. Thus, artificial intelligence (AI) and machine learning (ML) models have shown significant interest in HEIs. This study designs a novel Artificial Intelligence based Cybersecurity Intrusion Detection Model for Higher Education Institutions named AICID-HEI technique. The goal of the AICID-HEI technique is to determine the occurrence of distinct kinds of intrusions in higher education institutes. The AICID-HEI technique encompasses min-max normalization approach to preprocess the data. Besides, the AICID-HEI technique involves the design of improved differential evolution algorithm based feature selection (IDEA-FS) technique is applied to choose the feature subsets. Moreover, the bidirectional long short-term memory (BiLSTM) model is utilized for the detection and classification of intrusions in the network. Furthermore, the Adam optimizer is applied for hyperparameter tuning to properly adjust the hyperparameters in higher educational institutions. In order to validate the experimental results of the proposed AICID-HEI technique, the simulation results of the AICID-HEI technique take place by the use of benchmark dataset. The experimental results reported the betterment of the AICID-HEI technique over the other methods interms of different measures.

Keywords: Higher education institutions; deep learning; machine learning; cybersecurity; intrusion detection

1 Introduction

Owing to the benefits provided by the Internet, business has become more open to supporting Internet driven enterprises like extranet collaboration, customer care, and e-commerce. Academic institution is considered resource limited and thus lot of times is needed to have this resource distributed among the students, lecturers, part time staff, and permanent. Additionally, students include postgraduate, Diplomas, and undergraduate students at distinct stages of education [1]. Likewise, full-time and part time lecturers need distinct network access stages. Several internet websites like pornographic and those that offer immediate solutions to online examination might need to be restricted or controlled. This will enhance bandwidth utilization and network security [2]. Many times, Students become so intrusive to explore all the areas of the network, and therefore it was necessary to defend network with crucial data, and part time staff needn't be trusted with this network resource. This emphasizes the requirement for a proper scheme to identify illegal accessing to this resource on quantified section beforehand experiencing severe damage. The organization is struggling to preserve availability, confidentiality, and integrity of the network resource and various technologies have been applied for guarding against network intrusions [3]. Fig. 1 illustrates the different modules contained in cybersecurity.

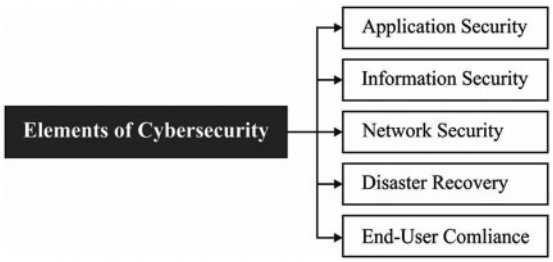

Figure 1: Different components involved in cybersecurity

Intrusion prevention systems (IPS) techniques work by surveilling system action and network traffics for the sign of malicious activities namely intrusion [4]. Mostly, IPS technique depends on signature detection technique which consults a dataset of well-known attack flags and patterns. Once the IPS identifies the matching, it chooses an automatic response from a collection of choices, ranging from alerting an administrator and logging the activity to manually blocking the traffics to preventing network intrusion. In a standard IPS positioning, the organization place devoted IPS network devices in line with the external internet access. This needs a device which is able to keep up with the scale of the institution network traffics [5]. Then, the device checks all the network packets when it blocks and passes suspected activity beforehand it accesses the network. This technique provides automated, rapid responses to security threats on campus networks. That move the event response posture from the reactive method utilized while examining a suspicious event to a proactive method which blocks the incidents from taking place primarily.

Machine learning (ML) and Artificial intelligence (AI) development help individuals exceed classical computers to surpass and simulate human intelligence. The advancement of this technology has considerably modified the educational system, providing students a collaborative learning environment and further knowledge in the HEI with greater implications for the upcoming days [6]. Mostly, reputable higher education institution has realized that ML and AI represent the future and present in education and the world advanced evolution. This technology provides advanced and interactive education knowledge to the student [7]. The result is remarkable: 65% of university in the

America supports AI- and ML-enabled learning. Furthermore, this system provides essential support to lecturers and teachers in the schools, facilitating and improving learning in different manners [8]. Kumar has proven that AI and ML are enhancing and efficient security of the institutions, providing an accessible, peaceful, and flexible computing platform for the study and developing skills amongst students [9], and collaborative learning environments in the HEI reinforce the significance of ML and AI to increase customized learning.

This study designs a novel Artificial Intelligence based Cybersecurity Intrusion Detection Model for Higher Education Institutions named AICID-HEI technique. The AICID-HEI technique encompasses min-max normalization approach to pre-process the data. In addition, the AICID-HEI technique involves the design of improved differential evolution based feature selection (IDEA-FS) technique is applied to choose the feature subsets. Followed by, the bidirectional long short term memory (BiLSTM) model is utilized for the detection and classification of intrusions in the network. Finally, the Adam optimizer is applied for hyperparameter tuning to properly adjust the hyperparameters in higher educational institutions. In order to validate the experimental results of the proposed AICID-HEI technique, the simulation results of the AICID-HEI technique take place by the use of benchmark dataset.

2 Related Works

DeCusatis et al. [10] introduced the implementation and design of a cyber-security framework for a Linux community public cloud assisting research and education. The method integrates packet authentication and transport layer access control gateway for blocking fingerprints of key network resources. Stimulation outcomes are provided for the connected data centres in New York. They demonstrate that our technique is capable of blocking Denial of Service (DoS) attacks and network scanners, and offer geo-location attribution based syslog classification.

Aggrey [11] adapt an intrusion detection system (IDS) for academic institutions to prevent network intrusion and provide early detection. The concept is to offer a combined scheme which reduces the weakness of the intrusion prevention technique. They determine IDS, discuss the various IDS architecture, types, compare distinct IDSs, and investigate an efficient execution approach. Othman et al. [12] present Spark-Chi-support vector machine (SVM) method for detecting intrusions. In this method, we employed ChiSqSelector for selecting features and constructed an IDS by utilizing SVM classifiers on Apache Spark Big Data. They utilized KDD99 for training and testing the models. In this work, we presented a comparison among Chi-logistic regression (LR) and Chi-SVM classifiers.

Yahia et al. [13] examined the various kinds of network intrusion data sets and highlight the fact that students could simply generate a network intrusion data set i.e., illustrative of the network. Intrusion is in form of network signature or anomaly; the student could not grasp each type but they must have the capability of detecting malicious packets with this network. Gao et al. [14] take benchmark dataset as the object of research, analyzed the existing problems and latest progress in the fields of IDS, and presented an adoptive ensemble learning model. By altering the amount of trained information and setting up various decision trees (DTs), we constructed a MultiTree approach. For improving the entire detection effects, we select many base classifications and developed an ensemble adoptive voting method.

In Mishra et al. [15], a comprehensive analysis and investigation of different ML methods were conducted to find the reason for problems related to different ML methods in intrusion activity detection. Attack mapping and classification of the attack feature are given to all the attacks. Problems

that are associated with lower-frequency attack detection using network attack data set are considered and feasible methodologies are recommended for development.

3 The Proposed Model

This study has designed an effective AICID-HEI technique is to determine the occurrence of distinct kinds of intrusions in higher education institutes. The AICID-HEI technique encompasses min-max normalization based pre-processing, IDEA-FS based election of features, BiLSTM based classification, and Adam optimizer based hyperparameter tuning. The choice of IDEA-FS and Adam optimizer assist to enhance the intrusion detection performance in higher educational institutions.

3.1 Data Pre-Processing

Primarily, the input data is transformed into a meaningful format by the use of min-max normalization approach. It is generally utilized for reducing the diversifying scaling of the dimensionality. The normalization process converts the data in a particular range by performing the linear conversion on the input data. The dimensionality of the data can be transformed in the interval of [0, 1] by the use of min-max normalization. It carries out the conversion process using Eq. (6):

$$t = \frac{v - \min_d}{\max_d - \min_d}(tran\_\max_d - tran\_\min_d) + tran\_\min_d \tag{1}$$

where t indicates transformed data v in dimension d, implies the actual lower value and $\max_d$ denotes the actual higher value of the dimension d. Likewise, $tran\_\min_d$ defines the converted lower value and $tran\_\max_d$ indicates the converted higher value of the dimension d.

3.2 Design of IDEA-FS Technique

During the feature selection process, the normalized data is fed into the IDEA-FS technique and derive a useful subset of features. DEA technique is assumed as population based search method that is primary established by Storn et al. [16].

During this phase of the current analysis, a 3 phases altering method was established utilizing the DE approach for resolving an optimized issue. For implementing this task, a particular amount of solution vectors were arbitrarily initialized afterward upgraded iteratively utilizing genetic operators (mutation as well as crossover) and selective operators. A primary step, the mutation operators are executed utilizing 3 distinct arbitrarily chosen solution vectors (represented as r_1, r_2, and r_3 vectors) in the DE population. Afterward, the variance amongst 2 vectors (r_2 and r_3) multiplied by scaling factor (F) has added to the primary vector (r_1). Therefore, all the target solutions X_i^G is changed as to mutant solution vector y_i^{G+1} as follows.

$$V_i^{G+1} = X_{r_1}^G(t) + F * (X_{r_2}^G - X_{r_3}^G), r_1 \neq r_2 \neq r_3 \neq i \tag{2}$$

In the secondary phase, the crossover operator was implemented for calculating a trial vector u_i^{G+1} it is implemented by integrating the destination solution vector with mutated vector dependent upon the subsequent technique.

$$u_{ij}^{G+1} = \begin{cases} v_{ij}^{G+1}, \ (\text{rand}(j) \leq CR) \ or \ j = r \ and \ n(i) \\ \chi_{ij}^{G}, \ (rand\ (j) > CR) and \ j \neq r \ and \ n(i) \end{cases} \tag{3}$$

where $j = 1, 2, \ldots, D$, $rand(j) \in [0, 1]$ denotes the j^{th} estimation of uniform arbitrary generator number. CR indicates the crossover probability that is an arbitrary vector range in [0–1]. $r \ and \ n(i) \in$

$\{1, 2, \ldots, D\}$ signifies the arbitrary value that makes sure u_i^{G+1} obtains one or more elements in $v_i^{G+1,}$ else no novel parent vector was created, and so the population remains unchanging. Fig. 2 illustrates the flowchart of DE technique.

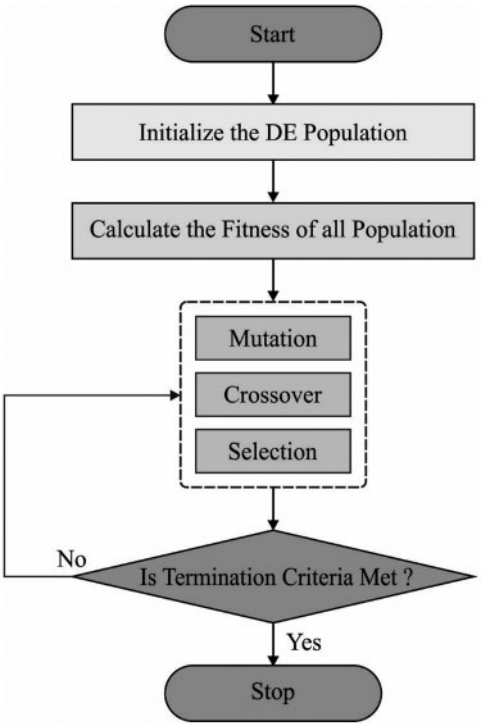

Figure 2: Flowchart of differential evolution

Lastly, in selective sections if and only if the trial vectors u_i^{G+1} produces an optimum FF value related to x_i^G, then u_i^{G+1} is fixed to x_i^{G+1}. Else, the old vector x_i^G has reserved. The selective method is as follows [17].

$$x_i^{G+1} = \begin{cases} u_i^{G+1} & (f(u_i^{G+1}) < f(x_i^G)) \\ x_i^G & (f(u_i^{G+1}) \geq f(x_i^G)) \end{cases} \tag{4}$$

During the IDEA, the Cauchy mutation operators are utilized that typical DEA of enhancements from solution diversity. Its purpose is for enhancing the exploration capability and solution diversity of raw DEA from the previous phases of operation with the combination of incorporate Cauchy mutation operators. Also, the Cauchy distribution was executed to perform Cauchy variation on solution that doesn't converge from *c is* following rounds. The basic method is that its influence stuck with local optimum and so, an exterior association was needed and so the search procedure moved from the direction of exploration procedure. During this case, all dimensions an arbitrary parameter of Cauchy distribution, the density function is signified as follows:

$$f_c(x) = \frac{\sigma}{[\pi(\sigma^2 + x^2)]}, -inf < x < +inf, \tag{5}$$

where $\sigma = 1$ indicates the traditional Cauchy distribution.

The FS technique is represented as N sized vectors where N refers to the feature counts. At this point, all place of vector is assumed the values as *zero* or one where *zero* implies the feature that is

unselective and one refers to the selective features. Based on the above-mentioned, the fitness function (FF) is to define solution in this state crated to obtain a balance among 2 purposes:

$$fitness = \alpha \Delta_R(D) + \beta \frac{|Y|}{|T|} \tag{6}$$

$\Delta_R(D)$ stands for the classifying error rate. $|Y|$ denotes the size of subsets that this technique selects and $|T|$ whole amount of features contained in the present datasets. α determines the parameter $\in [0, 1]$ relating to the weight of error rate of classification correspondingly however $\beta = 1 - \alpha$ refers the importance of reducing feature.

3.3 Hyperparameter Tuned BiLSTM Based Classification Model

At the time of data classification, the features are passed into the BiLSTM model to carry out the classification process. The long short term memory (LSTM) network is a kind of recurrent neural network (RNN) primarily structured for solving the vanishing gradient issue of RNNs if concerning long orders [18]. The LSTM network structure has of layer of LSTM unit afterward a typical feedforward network. In a general viewpoint, an LSTM unit functions as follows: assume x_t be the present input at time t, the resultant of input gate as:

$$i_t = \sigma(W_i^x x_t + W_i^h h_{t-1} + b_i), \tag{7}$$

where W_i^x and W_i^h implies the weight matrices, h_{t-1} represents the preceding hidden state of units, and b_i refers the bias vector. The function $\sigma(x) \in (0, 1)$ has sigmoid function utilized to gate.

Likewise, the resultant of forget gate f_t has estimated as:

$$f_t = \sigma(W_f^x x_t + W_f^h h_{t-1} + b_f). \tag{8}$$

Eventually, the resultants of output gate o_t and cell state c_t are as follows:

$$c_t = i_t \odot \tanh(W_c^x x_t + W_c^h h_{t-1} + b_c) + c_{t-1}, \tag{9}$$

$$o_t = \sigma(W_o^x x_t + W_o^h h_{t-1} + b_o), \tag{10}$$

$$h_t = o_t \odot \tanh(c_t), \tag{11}$$

where $\odot$ refers the Hadamard product. The BiLSTM has 2 parallel LSTM layers such as forward and backward directions. As the input was treated twice, BiLSTM remove further data in the input. Therefore, an enhancing contextual data for making optimum forecasts than LSTM. So, BiLSTMs current has faster convergence and accuracy than LSTM. The BiLSTM structure containing 2 LSTM layers, maintains past as well as future context at whenever of order [19]. The output of all LSTMs was integrated based on the subsequent formula:

$$y_t = W_{\overrightarrow{h}y} \overrightarrow{h_t} + W_{\overleftarrow{h}y} \overleftarrow{h_t} + b_y \tag{12}$$

where $\overrightarrow{h_t}$ *and* $\overleftarrow{h_t}$ refers the outcomes of forward as well as backward LSTMs.

For optimally altering the hyperparameters of the BiLSTM model, the Adam optimizer can be utilized and thereby boost the classification outcomes.

Adam is another widely utilized technique that alters the rate of learning adaptive to all the parameters. The Adam is a group of distinct gradient optimized techniques. Besides is an exponentially decaying average of past squared gradient calculated namely Adadelta, along with Adam gets an

exponentially decaying average of past gradients that is same as Momentum.

$$M_t = \beta_1 M_{t-1} + (1 - \beta_1) g_t, \tag{13}$$

$$G_t = \beta_2 G_{t-1} + (1 - \beta_2) g_t \odot g_t, \tag{14}$$

where β_1 and β_2 implies the decay rate that is suggested to follow the default value. M_t and G_t are determined for estimating the mean of past gradients (a primary moment) and uncentered difference of past gradients (the secondary moment) correspondingly [20]. Since the decay rates generally cause any bias issue, it can be essential to perform the bias-correction work.

$$\begin{aligned} \hat{M} &= \frac{M_t}{1 - \beta_1^t}, \\ \hat{G}_t &= \frac{G_t}{1 - \beta_2^t}. \end{aligned} \tag{15}$$

So, the upgrade value of Adam was determined as:

$$\Delta\theta_t = -\frac{\alpha}{\sqrt{\hat{G} + \varepsilon}} \hat{M}_t. \tag{16}$$

The gradient part of $\triangle\theta_t$ also is determined as:

$$g_t^{'} = \frac{1}{\sqrt{\hat{G}_t + \varepsilon}} \hat{M}_t, \tag{17}$$

$$\begin{aligned} \triangle\theta_t &= -\alpha \left(\frac{1}{\sqrt{\hat{G}_t + \varepsilon}} \hat{M}_t \right) \\ &= -\alpha g_t^{'}. \end{aligned} \tag{18}$$

In Eq. (16), it could be established that every function was dependent upon past gradient of present parameter that has no connection to rate of learning. Therefore, Adam is an optimum efficiency with the support of learning rate techniques.

4 Performance Validation

The simulation analysis of the AICID-HEI technique takes place using the KDDCup99 dataset, which contains a set of 41 attributes where 39 among them are numerical records and rest of them are symbolic records. The dataset comprises two major classes namely normal and anomaly. Besides, the anomaly class includes four kinds of attacks namely DoS, R2l, Probe, and U2r attacks. The best cost analysis of the IDEA-FS technique with recent approaches is carried out in Tab. 1 and Fig. 3. The IDEA-FS technique has chosen the feature subset of (1, 5, 6, 7, 9, 11, 13, 15, 16, 19, 26, 28, 31, 37, 40). The experimental values proved that the ant colony optimization (ACO)-FS, butterfly optimization algorithm (BOA)-FS, and particle swarm optimization (PSO)-FS techniques have reached to higher best cost (BC) of 0.0008754, 0.0009467, and 0.0009865 respectively.

Table 1: Best cost analysis of IDEA-FS with other FS techniques

Methods	Best cost
IDEA-FS	0.0006532
ACO-FS	0.0008754
BOA-FS	0.0009467
PSO-FS	0.0009865

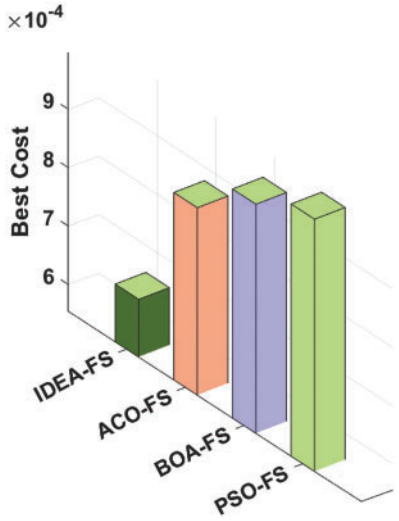

Figure 3: Best cost analysis of AICID-HEI technique

The intrusion detection results obtained by the AICID-HEI technique under various types of attacks are provided in Tab. 2 and Figs. 4–5. The experimental values reported that the AICID-HEI technique has identified all the class labels effectively.

Table 2: Result analysis of proposed model

Attacks	Sensitivity	Specificity	Accuracy	F-Measure	Kappa
Dos	99.020	99.300	98.540	97.480	97.300
R2l	99.080	99.760	99.100	99.870	98.580
Probe	99.100	99.410	99.020	98.750	98.350
U2r	98.480	99.480	99.050	98.570	98.920
Normal	99.390	99.750	99.380	99.440	99.240
Average	99.014	99.540	99.018	98.822	98.478

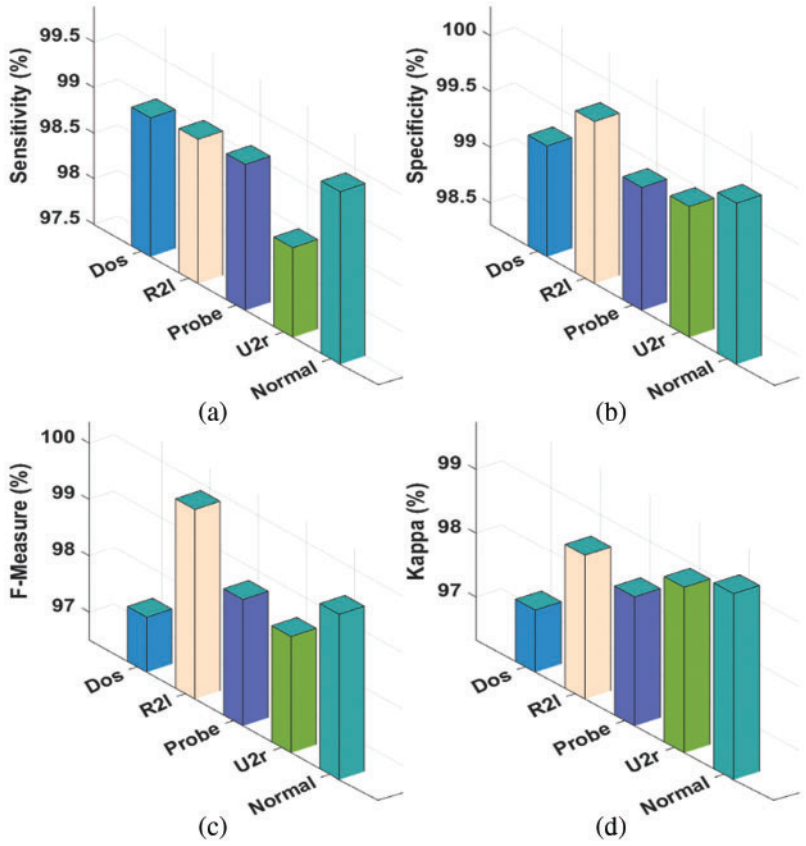

Figure 4: Result analysis of AICID-HEI technique with different measures

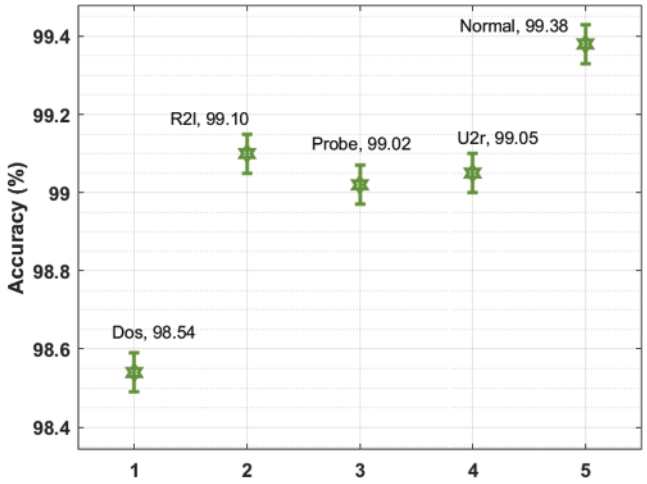

Figure 5: Accuracy analysis of AICID-HEI technique with distinct attacks

For instance, under DoS attack, the AICID-HEI technique has attained $sens_y$, $spec_y$, $accu_y$, $F_{measure}$, and kappa of 99.020%, 99.300%, 98.540%, 97.480%, and 97.300% respectively. Besides, under Probe attack, the AICID-HEI approach has achieved $sens_y$, $spec_y$, $accu_y$, $F_{measure}$, and kappa of 99.100%,

99.410%, 99.020%, 98.750%, and 98.350% correspondingly. In addition, under Normal attack, the AICID-HEI methodology has reached $sens_y$, $spec_y$, $accu_y$, $F_{measure}$, and kappa of 99.390%, 99.750%, 99.380%, 99.440%, and 99.240% correspondingly. Average result analysis of the AICID-HEI technique under all kinds of attacks. The experimental results reported the betterment of the AICID-HEI technique with average $sens_y$, $spec_y$, $accu_y$, $F_{measure}$, and kappa of 99.014%, 99.540%, 99.018%, 98.822%, and 98.478% respectively.

Fig. 6 illustrates the accuracy analysis of the AICID-HEI technique on the test dataset. The results outperformed that the AICID-HEI system has accomplished higher performance with superior training and validation accuracy. It can be stated noticed that the AICID-HEI technique has gained improved validation accuracy over the training accuracy.

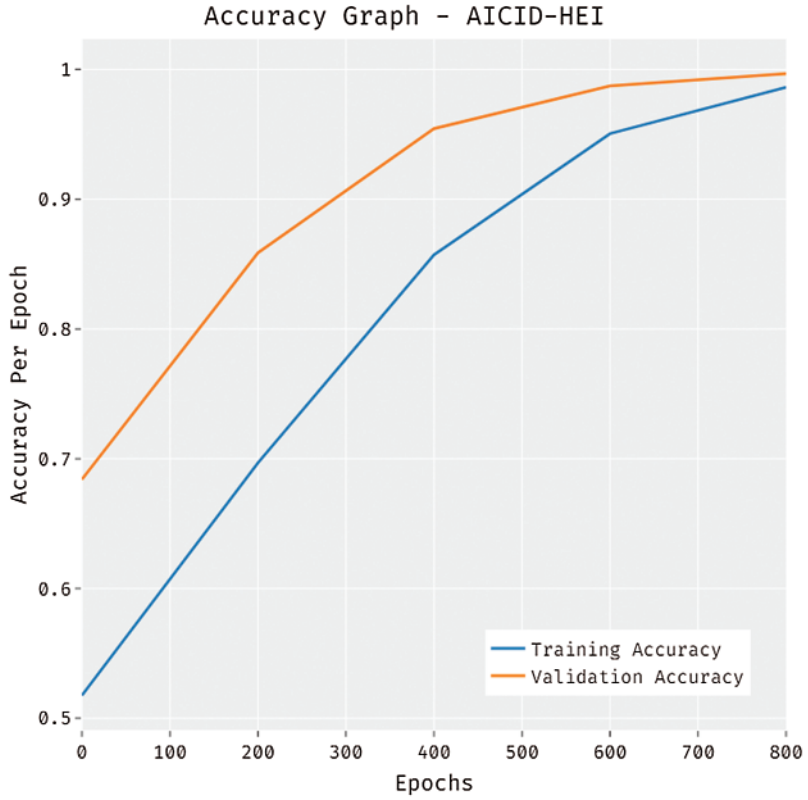

Figure 6: Accuracy graph analysis of AICID-HEI technique

Fig. 7 showcases the loss analysis of the AICID-HEI approach on the test dataset. The outcomes established that the AICID-HEI technique has resulted in a proficient outcome with the reduced training and validation loss. It can be clear that the AICID-HEI technique has offered reduced validation loss over the training loss.

The detailed comparative study of the AICID-HEI technique with recent methods takes place in Tab. 3 and Fig. 8 [21,22]. The experimental results stated that the RBF Network and Random (RAND) Forest models have obtained lower intrusion detection performance. At the same time, the Random Tree and Decision Tree models have attained slightly increased intrusion detection outcomes. In line with, the logistic regression (LOGR) technique has accomplished somewhat acceptable intrusion detection outcomes. However, the AICID-HEI technique has outperformed the other methods with

the increased $sens_y$, $spec_y$, $accu_y$, $F_{measure}$, and kappa of 99.014%, 99.540%, 99.018%, 98.822%, and 98.478% respectively. From the above mentioned tables and figures, it is ensured that the AICID-HEI technique has resulted in effective classification performance and accomplishes security.

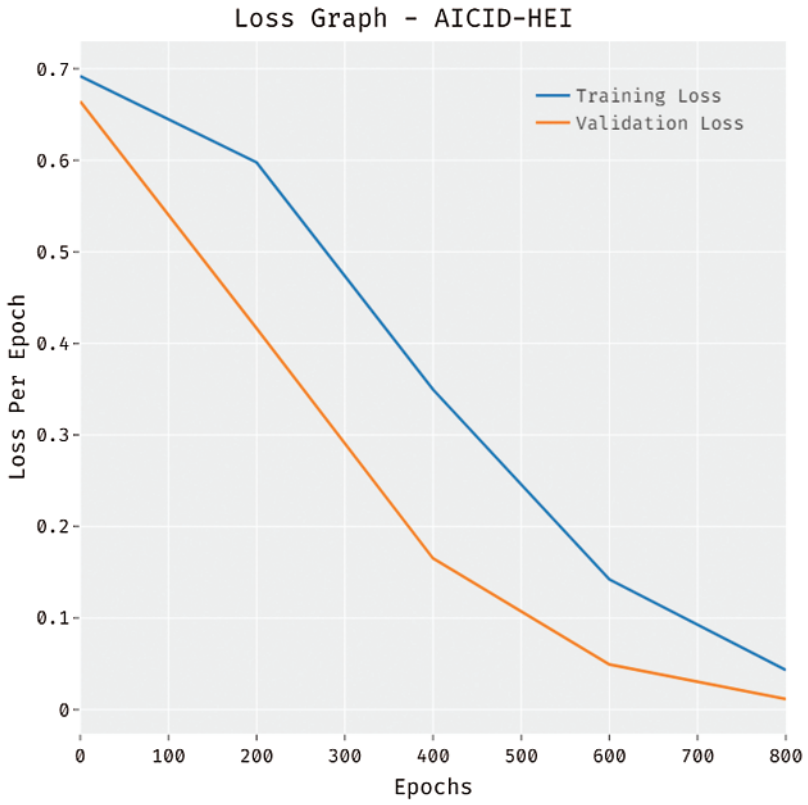

Figure 7: Loss graph analysis of AICID-HEI technique

Table 3: Performance analysis of various methods with proposed AICID-HEI model

Methods	Sensitivity	Specificity	Accuracy	F-score	Kappa
AICID-HEI	99.01	99.54	99.01	98.82	98.47
RBFNetwork	93.40	92.38	92.93	93.38	85.79
LOGR	97.26	96.92	97.10	97.29	94.19
RAND. forest	92.39	93.83	93.04	93.58	85.99
RAND. tree	95.68	95.39	95.55	95.84	91.06
Decision tree	95.68	95.37	95.53	95.83	91.03

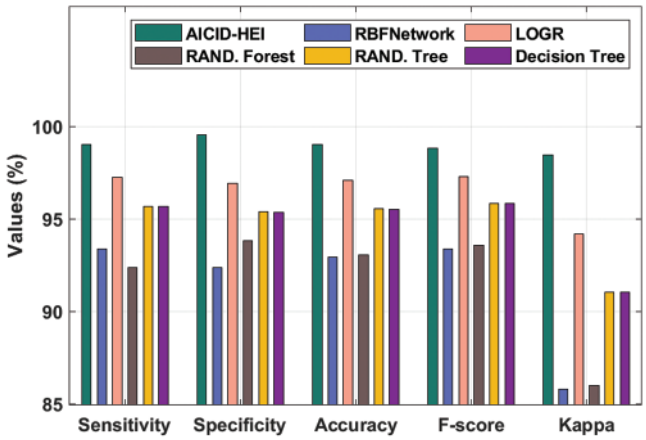

Figure 8: Comparative analysis of AICID-HEI technique with existing approaches

5 Conclusion

This study has designed an effective AICID-HEI technique is to determine the occurrence of distinct kinds of intrusions in higher education institutes. The AICID-HEI technique encompasses min-max normalization based pre-processing, IDEA-FS based election of features, BiLSTM based classification, and Adam optimizer based hyperparameter tuning. The choice of IDEA-FS and Adam optimizer assist to enhance the intrusion detection performance in higher educational institutions. In order to validate the experimental results of the proposed AICID-HEI technique, the simulation results of the AICID-HEI technique take place by the use of benchmark dataset. The experimental results reported the betterment of the AICID-HEI technique over the other methods interms of different measures. As a part of future extensions, clustering techniques can be included to boost the detection rate.

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] V. Kuleto, M. Ilić, M. Dumangiu, M. Ranković, O. M. D. Martins *et al.,* "Exploring opportunities and challenges of artificial intelligence and machine learning in higher education institutions," *Sustainability*, vol. 13, no. 18, pp. 10424, 2021.

[2] S. Liu, Y. Chen, H. Huang, L. Xiao and X. Hei, "Towards smart educational recommendations with reinforcement learning in classroom," in *2018 IEEE Int. Conf. on Teaching, Assessment, and Learning for Engineering (TALE)*, Wollongong, NSW, pp. 1079–1084, 2018.

[3] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
[4] S. Kholmuminov, S. Kholmuminov and R. E. Wright, "Resource dependence theory analysis of higher education institutions in Uzbekistan," *Higher Education*, vol. 77, no. 1, pp. 59–79, 2019.
[5] A. Aldhalemi, F. Abidy and A. Kadhim, "The statistical evaluation of e-exams in higher education institutions during COVID-19 pandemic: A case of Iraq," *Webology*, vol. 18, no. 5, pp. 654–671, 2021.
[6] P. J. Ramísio, L. M. C. Pinto, N. Gouveia, H. Costa and D. Arezes, "Sustainability strategy in higher education institutions: Lessons learned from a nine-year case study," *Journal of Cleaner Production*, vol. 222, pp. 300–309, 2019.
[7] J. M. F. Mendoza, A. G. Schmid and A. Azapagic, "Building a business case for implementation of a circular economy in higher education institutions," *Journal of Cleaner Production*, vol. 220, pp. 553–567, 2019.
[8] A. D. R. Fonseca, S. Jorge and C. Nascimento, "The role of internal auditing in promoting accountability in higher education institutions," *Revista de Administração Pública*, vol. 54, no. 2, pp. 243–265, 2020.
[9] C. Liu and K. Jayakar, "The evolution of telecommunications policy-making: Comparative analysis of China and India," *Telecommunications Policy*, vol. 36, no. 1, pp. 13–28, 2012.
[10] C. DeCusatis, P. Liengtiraphan and A. Sager, "Advanced intrusion prevention for geographically dispersed higher education cloud networks," *In Online Engineering & Internet of Things, Lecture Notes in Networks and Systems Book Series (LNNS)*, vol. 22, pp. 132–143, 2018.
[11] O. Aggrey, "*An intrusion detection system for academic institutions*," *Master of Science Thesis*, Makerere University, 2007.
[12] S. M. Othman, F. M. B. Alwi, N. T. Alsohybe and A. Y. A. Hashida, "Intrusion detection model using machine learning algorithm on big data environment," *Journal of Big Data*, vol. 5, no. 1, pp. 34, 2018.
[13] A. Yahia and E. Atwell, "Network intrusion datasets used in network security education," *International Journal of Innovative Trends in Engineering*, vol. 7, no. 3, pp. 43–50, 2018.
[14] X. Gao, C. Shan, C. Hu, Z. Niu and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019.
[15] P. Mishra, V. Varadharajan, U. Tupakula and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 686–728, 2019.
[16] R. Storn and K. Price, "Differential. evolution, differential evolution a simple and efficient heuristic strategy for global optimization over continuous spaces," *Journal of Global Optimization*, vol. 11, pp. 341–359, 1997.
[17] E. Y. Bejarbaneh, A. Bagheri, B. Y. Bejarbaneh, S. Buyamin and S. N. Chegini, "A new adjusting technique for PID type fuzzy logic controller using PSOSCALF optimization algorithm," *Applied Soft Computing*, vol. 85, pp. 105822, 2019.
[18] Y. Yu, X. Si, C. Hu and J. Zhang, "A review of recurrent neural networks: Lstm cells and network architectures," *Neural Computation*, vol. 31, no. 7, pp. 1235–1270, 2019.
[19] T. M. Velu, J. G. A. Cervantes, J. M. C. Duarte, H. R. Gonzalez and J. R. Pinales, "Imaginary finger movements decoding using empirical mode decomposition and a stacked BiLSTM architecture," *Mathematics*, vol. 9, no. 24, pp. 3297, 2021.
[20] C. Zhang, M. Yao, W. Chen, S. Zhang, D. Chen *et al.,* "Gradient descent optimization in deep learning model training based on multistage and method combination strategy," *Security and Communication Networks*, vol. 2021, pp. 1–15, 2021.
[21] B. V. Kumar and S. Mohan, "A novel feature selection with fuzzy deep neural network for attack detection in big data environment," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 3, pp. 539–550, 2021.
[22] M. Ragab, A. M. K. Abdel Aal, A. O. Jifri and N. F. Omran, "Enhancement of predicting students performance model using ensemble approaches and educational data mining techniques," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–9, 2021.