International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 67-72
Journal homepage: http://iieta.org/journals/ijsse

Hybrid BiLSTM-SVM Intrusion Detection with Decision-Based Flow Ranking

Asraa A. Abd Al-Ameer[1*], Alaa Akram Huby[2]

[1] Department of Information Technology, University of Kerbala, Karbala 56001, Iraq
[2] Department of Aircraft Engineering, University of Warith Al-Anbiyaa, Karbala 56001, Iraq

Corresponding Author Email: israa.abdalhussein@uokerbala.edu.iq

https://doi.org/10.18280/ijsse.150107

Received: 20 November 2024
Revised: 28 December 2024
Accepted: 15 January 2025
Available online: 31 January 2025

Keywords:
network, network security, artificial intelligence, machine learning, deep learning, information ranking, intrusion detection system

ABSTRACT

Intrusion Detection Systems (IDS) are important in facing the development of cyber threats such as Distributed Denial of Service (DDoS), phishing, and malware attacks, so, their promulgating is important. Bidirectional Long Short-Term Memory (BiLSTM) with Support Vector Machines (SVM) has been integrated and proposed as a hybrid model in this paper to improve detection accuracy and threat response. The proposed system steps include comprehensive data preprocessing, feature extraction using BiLSTM, and classification with SVM, and all these using and leveraging the UNSWNB15 dataset. Deep learning takes advantage of BiLSTM's ability and traditional machine learning leverage from SVM's efficiency so this integration captures temporal patterns through BiLSTM and manages high-dimensional data through SVM. Experimental findings showed that the proposed system is accurately proficient in distinguishing between normal and attack traffic, achieving high levels of accuracy values, such as precision 95%, recall 94%, and F1-scores 95%, where the accuracy value reaches 99%. Besides, to improve the efficiency of threat management, SVM's decision function scores have been used to employ a ranking technique by the proposed system. Therefore, this research highlights the hybrid model value in enhancing IDS performance.

1. INTRODUCTION

The cyber-attacks complexity and their recurrence have increased which leads to meaningful threats to organizational security and data integrity [1]. To deal with these threats, traditional IDS was used to provide an intelligent and powerful detection mechanisms [2, 3]. To increase IDS capabilities, the technologies of Machine Learning (ML) and Deep Learning (DL) [4] have been used to provide greater effectiveness and accuracy in performance [5]. The proposed hybrid model for IDS combines BiLSTM networks with SVM to combine the capabilities of both DL and traditional ML models. The UNSW-NB15 dataset [6] provide various normal and attack scenarios [7] which have been used to examine the performance of the proposed system. The main objectives of this research paper are, first, developing a hybrid IDS model to enhance the detection of attacks in network traffic flows, where the hybrid model integrates BiLSTM for feature extraction and SVM for classification. Second, to deal in a prioritized manner with high-confidence threats, a ranking system based on the SVM's decision scores has been used. Third, using the UNSW-NB15 dataset and making tests on it to evaluate the proposed system efficacy and distinguish its ability to distinguish between benign and malicious network traffic.

2. RELATED WORK

Hybrid models are one of the promising approaches to addressing the modern network security through enhancing IDS. These models play a vital role in combating cosmopolitan cyber threats. A hybrid model incorporating XGBoost and CNN for feature extraction, paired with LSTM for classification, was utilized by Shi et al. [8]. It achieved a test accuracy of 94.41%, with experimental results implying a high detection rate and strong accuracy alongside a relatively low False Acceptance Rate (FAR). A hybrid KCLSTM model has been used by Lv and Ding [9], it improves intrusion detection by combining K-means clustering with CNN and LSTM, where the NSL-KDD dataset has been used to evaluate the proposed hybrid categorization model, and the experimental results show that the model can detect anomalous events successfully and with high accuracy of 93.3%, a F1 score of 93.7%, and a DR of 93.2% for both anomalous and normal events. Thus, it achieves higher accuracy, detection rate, and F1-score compared to traditional methods. Random Forest, Gradient Boosting, and Multi-Layer Perceptron classifiers have been combined by Shi et al. [10], affecting high accuracy (0.9998), pivotal for effective intrusion detection and degrading false negatives. Al-Ameer et al. [11] have used multi-deep learning models based on federated learning to provide intelligent intrusion detection system in software-defined networks which provide a preserving data privacy and achieved highly effective method for attack detection, where arrived to impressive accuracy of 95.68%. AlHaddad et al. [12] proposed a hybrid deep learning model integrates Convolutional Neural Networks (CNN) with Recurrent Gated Unit (GRU) algorithms to improve detection capabilities by detect Distributed Denial-of-Service (DDoS) attacks on the communication infrastructure Smart Grids. Through experimental simulations, their approach proved a high accuracy rate of 99.86%, which refers to its capability in protecting Smart Grid communication from DDoS threats. All the previously mentioned related works used different ML and DL ways to detect attacks, while the proposed work has used a BiLSTM model, SVM with RBF, and Ranking method to get network flows possibility of being attacks, it tested on UNSWNB15 dataset and got accurate results.

3. BACKGROUND

In network security architecture, IDS plays a crucial role which is responsible for detecting malicious activities and policy violations. Signature-Based and Anomaly-Based are the two categories of IDS [13]. Signature-based technique used predefined patterns to detect known threats, whereas anomaly-based methods identify diversions from normal behavior, making them effective in spotting novel or previously unseen attacks [14].

3.1 Machine learning in IDS

Many ML techniques have been used to provide IDS [15]. These techniques enable the systems to be better at adapting to emerging threats and make them more advanced. Decision Trees, SVM, Random Forests, and Neural Networks, are some of the popular ML algorithms used in IDS they are very impactful in classification tasks where they learn patterns from traffic data and enable the difference between benign and malicious traffic [16].

3.2 Deep learning in IDS

Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are DL methods considered one of the important competencies for capturing temporal dependencies in sequential data. RNN and LSTM neural networks are a branch of ML [17]. BiLSTM is utilized in this paper to process the data in both forward and backward directions in a way that provides a better comprehension of the context [13].

3.3 Hybrid models

Traditional ML and DL techniques can combine to leverage their strengths to create a hybrid model. For instance, when making an extraction for a feature by DL model and then following it with a traditional ML classifier leads to enhanced performance for the hybrid model [18]. This model enables the DL to capture the representations of the complex feature while handling in an efficient way the managing of classification tasks by ML classifiers, even in high-dimensional data presence [19].

4. METHODOLOGY

To improve the performance of IDS, steps integrating the BiLSTM network and SVM classifier have been used. The diagram of the proposed work is displayed in Figure 1.

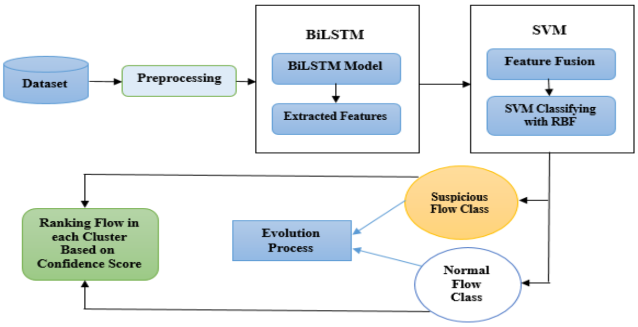


Figure 1. Proposed hybrid BiLSTM-SVM intrusion detection system

4.1 Data preprocessing and feature extraction

The network traffic dataset is preprocessed to form it in a way to is suitable for model training, which includes:

- handling missing values
- encoding categorical data
- and normalization for the raw data

A BiLSTM network is utilized on the preprocessed network traffic data to excerpt temporal features. It captures patterns in both forward and backward directions, improving its ability to identify complex relationships within network flows. The BiLSTM model is compiled using the Adam optimizer and binary cross-entropy loss, making it suitable for binary classification tasks. Adam optimizer ensures good BiLSTM model training, especially with the data's high-dimensional nature while binary cross-entropy loss provides a suitable matric to distinguish between normal and attack traffic and improve the model's performance.

To avoid overfitting, early stopping is employed by examining the validation loss. The output consists of a set of deep, learned features that capture sequential patterns and temporal dependencies within the network traffic flows.

4.2 Feature fusion

The original scaled features have been combined with the features extracted by the BiLSTM, creating a comprehensive feature set that integrates temporal insights from the BiLSTM with the original feature information.

4.3 Classification with SVM

An SVM with a Radial Basis Function (RBF) kernel is used to classify the fused features into attack and normal categories. SVMs are selected for their effective performance in high-dimensional spaces and their robustness against overfitting.

4.4 Ranking mechanism

A ranking mechanism is applied based on the SVM's confidence using decision function scores. Flows predicted as attacks are ranked in descending order of their decision scores, while normal flows are ranked in ascending order, reflecting lower decision scores. The ranking leverages the SVM's decision function denoted as Eq. (1):

$$f(x) = w^T x + b \tag{1}$$

The function f(x) denotes the decision function of the SVM for a specific input vector x, which establishes the classification of x based on its location in relation to the decision boundary. The vector w consists of weights that represent the coefficients assigned to each feature within the input vector x. The input feature vector x refers to the instance that requires classification, while b represents the bias term, a scalar quantity that adjusts the position of the decision boundary (hyperplane) along the feature axes without changing its orientation.

A positive f(x) refers to a prediction of class 1 (attack), while a negative f(x) indicates a prediction of class 0 (normal). During the ranking process, attack flows (Class 1) are sorted in descending order of f(x) to prioritize those with the highest confidence of being attacks. Conversely, normal flows (Class 0) are sorted in ascending order of f(x), giving priority to those with the highest confidence of being normal.

5. EXPERIMENTS AND RESULTS

This section provides a detailed evaluation of the suggested hybrid IDS framework efficacy in identifying abnormalities networks. The evaluation is conducted using the UNSW-NB15 dataset.

5.1 Dataset preprocessing

UNSW-NB15, with 50,000 flow samples chosen for computational feasibility. It has been pre-processed before being passed to the learning model for training. The pre-processing procedure includes cleaning, transformation, and normalization of the raw data.

5.1.1 Data cleaning

In the proposed system, samples with missing data have been managed by simply disregarding them entirely.

5.1.2 Data transformation

One-hot encoding [16] has been applied for machine learning to convert categorical features (e.g., service) into numerical form. This method transforms each category into a separate binary column, ensuring that no unintended ordinal relationships are introduced between categories. It enables algorithms to process categorical data more effectively, improving model performance while saving the integrity of the original categories.

5.1.3 Data normalization

To normalize numerical features [20], standard scaling was applied. This method standardizes the data by removing the mean and scaling it to unit variance, safeguard that each numerical feature contributes equally to the model's learning process. The following formula Eq. (2). defines the transformation:

$$x_{scaled} = \frac{x - \mu}{\sigma} \tag{2}$$

where, x represents the original feature value, μ is the mean of the feature across the training dataset, and σ is the standard deviation of the feature across the training dataset.

5.2 Applicability of the proposed model

The proposed model incorporates several advanced techniques to handle network traffic classification effectively. Data transformation through one-hot encoding ensures categorical features are properly converted into numerical values. Feature extraction leverages a BiLSTM model to capture temporal dependencies in the data, while a dense layer reduces dimensionality for efficient processing. The features extracted from the BiLSTM model are then fused with the original scaled features, combining both temporal and static information to form a more comprehensive feature set. Classification is achieved using an SVM with an RBF kernel, which provides robust binary classification between attack and normal flows. To further enhance its utility, a ranking mechanism is implemented based on the SVM's decision function scores, prioritizing network flows by their possibility of being malicious. This approach makes the model applicable for real-time security applications in intrusion detection systems.

5.3 Classification performance evaluation

The efficacy of the proposed strategy has been illustrated through a table that presents a confusion matrix. A binary confusion matrix is shown in Figure 2.

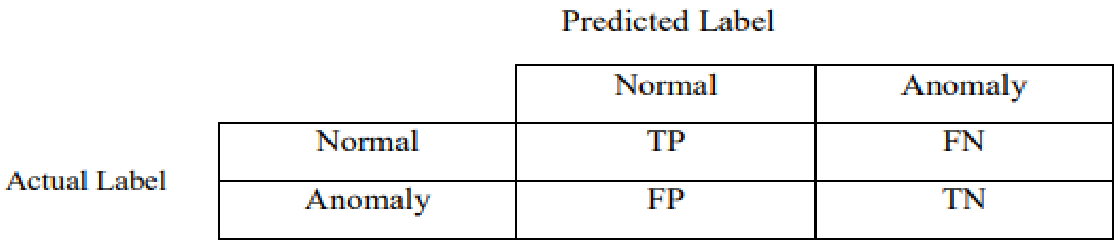
The chosen performance metrics for the recommended system include F1-score, recall, accuracy, and precision [21]. Accuracy is defined as the ratio of correctly identified instances within the complete traffic trace. It is determined by dividing the total number of packets that are accurately and inaccurately classified by the proposed system by the number of packets that are correctly identified as either normal or an attack. This calculation is represented in Eq. (3).

$$Accuracy = \frac{number\ of\ true\ classifications}{total\ number\ of\ classifications} = \frac{TP+TN}{TP+FP+TN+FN} \tag{3}$$

The UNSW-NB15 dataset has been utilized to evaluate the suggested system's classification performance. The proposed system hyperparameters are batch local size B which is set to 64, and local epoch numbers are set to 20. The SVM classifier trained on fused features achieved impressive performance metrics, as detailed below in Table 1 and Figure 3 The confusion matrix for the training and testing data, illustrating the binary classification of Normal and Attack, is presented in Figure 4.

Table 1. Model evaluation results of applying hybrid model for the UNSW-NB15 dataset

Accuracy	Precision	Recall	F1-Score
99%	95.58%	94.42%	95%



		Predicted Label	
		Normal	Anomaly
Actual Label	Normal	TP	FN
	Anomaly	FP	TN

Figure 2. A binary confusion matrix

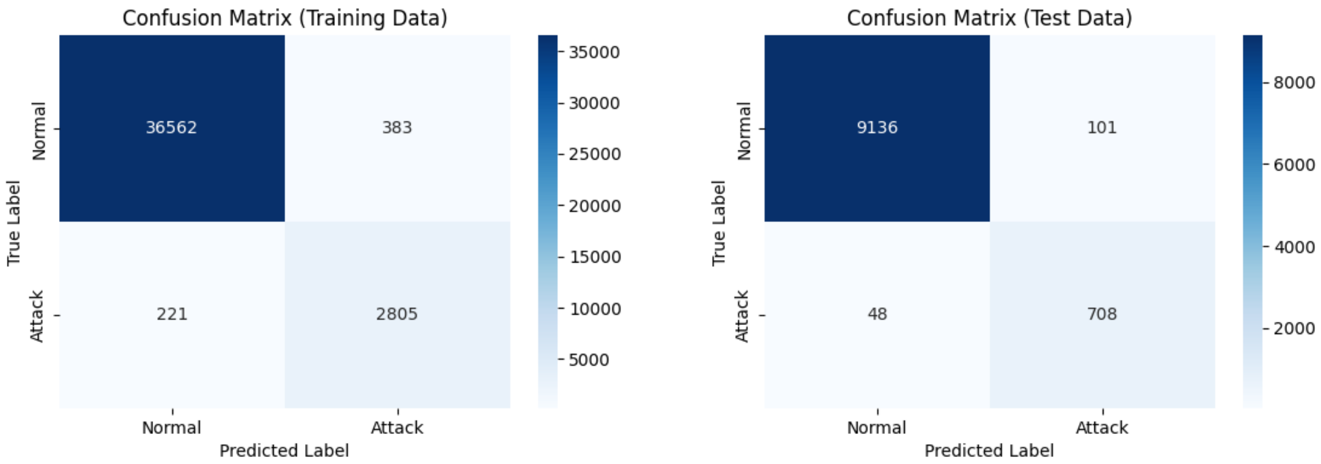


Figure 3. Confusion matrix (train and test data) - SVM model on fused features

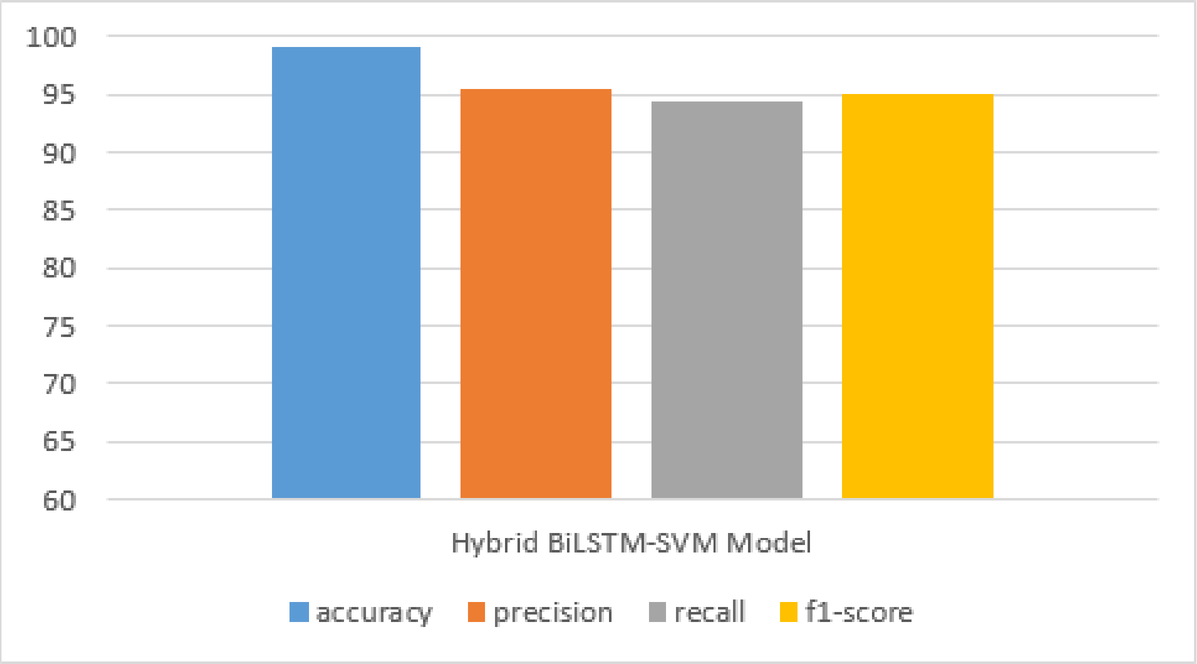


Figure 4. The suggested system's detection performance across UNSW-NB15 dataset

The ranking mechanism effectively prioritized flows based on the SVM's confidence scores. Table 2 and Table 3 show the top-ranked attack / normal flows with some of its features. The attack flows refer to the top-ranked attacks that have the highest positive decision scores, indicating strong confidence in their classification as attacks, and the normal flows refer to the top-ranked normal that have the most negative decision scores, signifying high confidence in their classification as normal traffic. The term 'Probability Attack/ Normal SVM' denotes the calibrated likelihood that a specific data sample is classified as belonging to the normal / attack. This probability is obtained through Platt scaling applied to the decision function of the SVM model.

The proposed system underwent evaluation with a dataset divided into 80% for training the model and 20% for testing purposes, showcasing robust capabilities in differentiating between malicious and normal network traffic. This hybrid architecture capitalizes on the advantages of both BiLSTM and SVM: BiLSTM adeptly identifies temporal patterns within network data, whereas the SVM classifier administers the high-dimensional fused feature space. Additionally, the integration of a ranking mechanism significantly enhances the system by prioritizing the most suspicious flows, thereby facilitating a prompt and targeted response to threats.

Table 2. Top 5 ranked attack flows

Traffic Id.	True Label	Predicted Label SVM	Probability Attack SVM	Decision Score SVM	Rank
4757	1	1	0.999997	2.645678	1
3260	1	1	0.999997	2.595339	2
2757	1	1	0.999996	2.558665	3
2213	1	1	0.999995	2.53106	4
4753	1	1	0.999988	2.358013	5

Table 3. Top 5 ranked normal flows

Traffic Id.	True Label	Predicted Label SVM	Probability Normal SVM	Decision Score SVM	Rank
2672	0	0	0.999995	-4.22846	1
5883	0	0	0.999995	-4.22634	2
7841	0	0	0.999995	-4.22592	3
391	0	0	0.999994	-4.18792	4
27520	0	0	0.999994	-4.1828	5

6. CONCLUSION

This study presents a hybrid IDS that combines BiLSTM networks with SVM to identify and prioritize malicious network traffic. Utilizing the UNSW-NB15 dataset, the system performs data preprocessing, feature extraction, and fusion, with classification and ranking determined by SVM decision scores. This approach improves detection accuracy and enables a prioritized response to threats, focusing on the most significant attacks. The model shows high performance across essential metrics, confirming its capability to differentiate between normal and malicious traffic. Some of the future works are applying an advanced technique of feature selection, using other benchmark datasets to test the hybrid model, and improving the ranking system by using for example anomaly frequency.

REFERENCES

[1] Safitra, M.F., Lubis, M., Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18): 13369. https://doi.org/10.3390/su151813369

[2] Khan, M.A., Kim, Y. (2021). Deep learning-Based hybrid intelligent intrusion detection system. Computers, Materials & Continua, 68(1): 671-687. https://doi.org/10.32604/cmc.2021.015647

[3] Abd Al-Ameer, A.A., Bhaya, W.S. (2023). Federated learning security mechanisms for protecting sensitive data. Bulletin of Electrical Engineering and Informatics, 12(4): 2421-2427. https://doi.org/10.11591/eei.v12i4.4751

[4] Huby, A.A., Sagban, R., Alubady, R. (2022). Oil spill detection based on machine learning and deep learning: A review. In 2022 5th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, pp. 85-90. https://doi.org/10.1109/IICETA54559.2022.9888651

[5] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6: 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950

[6] Moustafa, N., Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, pp. 1-6. https://doi.org/10.1109/MilCIS.2015.7348942

[7] Abd Al-Ameer, A.A., Bhaya, W.S. (2023). Enhanced intrusion detection in software-defined networks through federated learning and deep learning. Ingenierie des Systemes d'Information, 28(5): 1213-1220. https://doi.org/10.18280/isi.280509

[8] Shi, Z., Hu, Y., Mo, G., Wu, J. (2022). Attention-Based CNN-LSTM and XGBoost hybrid model for stock prediction. arXiv Preprint arXiv: 2204.02623, 14(8): 1-7. https://doi.org/10.48550/arXiv.2204.02623

[9] Lv, H., Ding, Y. (2024). A hybrid intrusion detection system with K-means and CNN+LSTM. EAI Endorsed Transactions on Scalable Information Systems, 11(6): 1-12. https://doi.org/10.4108/eetsis.5667

[10] Shi, C., Do, X.A., Huck, N. (2017). Deep neural networks, gradient-boosted trees, random forests: Statistical arbitrage on the S&P 500. European Journal of Operational Research, 259(2): 689-702. https://doi.org/10.1016/j.ejor.2016.10.031

[11] Al-Ameer, A., Asraa, A., Bhaya, W.S. (2023). Intelligent intrusion detection based on multi-Model federated learning for software defined network. International Journal of Safety and Security Engineering, 13(6): 1135-1141. https://doi.org/10.18280/ijsse.130617

[12] AlHaddad, U., Basuhail, A., Khemakhem, M., Eassa, F.E., Jambi, K. (2023). Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. Sensors, 23(17): 7464. https://doi.org/10.3390/s23177464

[13] Mohammed, M.S., Talib, H.A. (2024). Using machine learning algorithms in intrusion detection systems: A review. Tikrit Journal of Pure Science, 29(3): 63-74. https://doi.org/10.25130/tjps.v29i3.1553

[14] Gjorgjievska Perusheska, M., Dimitrova, V. (2023). Application of machine learning in intrusion detection systems. In Science and Information Conference. Cham: Springer Nature Switzerland. Springer, Cham, pp.1288-1308. https://doi.org/10.1007/978-3-031-37717-4_86

[15] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175-1191. https://doi.org/10.1145/3133956.3133982

[16] Saranya, T., Sridevi, S., Deisy, C., Chung, T.D., Khan, M.A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science, 171: 1251-1260. https://doi.org/10.1016/j.procs.2020.04.133

[17] Ashiku, L., Dagli, C. (2021). Network intrusion detection system using deep learning. Procedia Computer Science, 185: 239-247. https://doi.org/10.1016/j.procs.2021.05.025

[18] Maseno, E.M., Wang, Z., Xing, H. (2022). A systematic review on hybrid intrusion detection system. Security and Communication Networks, 2022(1): 9663052. https://doi.org/10.1155/2022/9663052

[19] Cahyo, A.N., Sari, A.K., Riasetiawan, M. (2020). Comparison of hybrid intrusion detection system. In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, pp. 92-97. https://doi.org/10.1109/ICITEE49829.2020.9271727

[20] Eliazar, I., Metzler, R., Reuveni, S. (2018). Universal max-min and min-max statistics. arXiv e-Prints.

[21] Hassoun, M.H. (1995). Fundamentals of Artificial Neural Networks. The MIT Press.