

Three layer hybrid learning to improve intrusion detection system performance

Ruki Harwahyu¹, Fajar Henri Erasmus Ndolu¹, Marlinda Vasty Overbeek²

¹Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia

²Department of Informatics, Faculty of Engineering and Informatics, Universitas Multimedia Nusantara, Tangerang, Indonesia

Article Info

Article history:

Received May 21, 2023

Revised Sep 24, 2023

Accepted Nov 4, 2023

Keywords:

CSE-CIC-IDS2018

Hybrid learning

Intrusion detection system

Long short-term memory

Random forest

ABSTRACT

In imbalanced network traffic, malicious cyberattacks can be hidden in a large amount of normal traffic, making it difficult for intrusion detection systems (IDS) to detect them. Therefore, anomaly-based IDS with machine learning is the solution. However, a single machine learning cannot accurately detect all types of attacks. Therefore, a hybrid model that combines long short-term memory (LSTM) and random forest (RF) in three layers is proposed. Building the hybrid model starts with Nearmiss-2 class balancing, which reduces normal samples without increasing minority samples. Then, feature selection is performed using chi-square and RF. Next, hyperparameter tuning is performed to obtain the optimal model. In the first and second layers, LSTM and RF are used for binary classification to detect normal data and attack data. While the third layer model uses RF for multiclass classification. The hybrid model verified using the CSE-CIC-IDS2018 dataset, showed better performance compared to the single algorithm. For multiclass classification, the hybrid model achieved 99.76% accuracy, 99.76% precision, 99.76% recall, and 99.75% F1-score.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ruki Harwahyu

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia

Kampus Baru Depok, Jawa Barat, 16424, Indonesia

Email: ruki.h@ui.ac.id

1. INTRODUCTION

With the rapid development of information technology, cyber attacks are increasing and becoming a special concern. The use of antivirus and firewalls has been widely implemented, but in reality networks are still being attacked, causing global losses of up to \$6 trillion in 2021, and is estimated to increase to \$10.5 trillion in 2025 [1]. The spread of cyber attacks even extends to the wireless sensor network (WSN), which causes the need for an intrusion detection system [2], [3]. Intrusion detection systems (IDS) are divided into two types based on attack detection, namely signature-based methods and anomaly-based methods [4]. In this research, an anomaly-based IDS was used even though it produced a high false alarm rate [4]. Anomaly-based IDS is more effective in detecting cyber attacks on network traffic [5] and has been widely accepted among the IDS research community [6].

A number of studies have been conducted in the domain of intrusion anomaly detection in network traffic, including the use of single machine learning, deep learning, and ensemble learning. Kotpalliwar and Wajgi [7] achieved 89.85% accuracy using KDDCUP99 dataset with a single support vector machine (SVM). Hota and Shrivastava [8], used several decision tree algorithms on the NSL-KDD dataset and obtained the highest accuracy of 99.68% with C4.5. In [9], k-nearest neighbor (KNN) was used on KDDCUP99 dataset to detect unknown attacks, and achieved 75% accuracy. An accuracy rate of less than 90% in detecting

unknown attacks poses a risk, as attacks continue to evolve and produce different patterns. However, all three studies still use outdated datasets and do not reflect the current characteristics of network traffic.

Besides traditional algorithms, some researchers have used deep learning and ensemble learning methods. Yoo *et al.* [10], using a convolution neural network (CNN) with the discretization preprocessing method on the NSL-KDD and CSE-CIC-IDS2018 datasets, produced an accuracy of 85% for NSL-KDD and 98% for the CSE-CIC-IDS2018 dataset. Alzughabi and El Khediri [11] used a deep neural network (DNN) and metaheuristic optimization algorithm on the CSE-CIC-IDS2018 dataset, achieving 98.41% accuracy for multiclass classification with a multi-layer perceptron (MLP) model using the backpropagation (BP) method. Lin *et al.* [12] utilized long short-term memory (LSTM) with attention mechanism (AM) on the CSE-CIC-IDS2018 dataset, resulting in an average accuracy of 96.2%. Mezina *et al.* [13] proposed three models for intrusion classification using u-shaped network (U-Net), temporal convolutional network (TCN) and a combination of TCN and LSTM. The highest accuracy was obtained with TCN-LSTM of 97.77% on the CSE-CIC-IDS2018 dataset. Meanwhile, in KDDCUP99, the highest accuracy was obtained with U-NET at 93.03%. Kunang *et al.* [14] proposed a pretraining approach with a deep autoencoder (PTDAE) combined with a DNN, obtaining an accuracy of 83.33% on the NSL-KDD dataset and an accuracy of 95.79% on the CSE-CIC-IDS2018 dataset. Fitni and Ramli [15] applied ensemble learning on the CSE-CIC-IDS2018 dataset. Gradient boosting, logistic regression, and decision trees were used in an ensemble model with 23 selected features, resulting in a high average score for the binary class, reaching 98.8% accuracy. From all the research that has been carried out, both using deep learning and ensemble learning have achieved high accuracy. However, there are difficulties in detecting types of attacks with minority samples on the NSL-KDD and CSE-CIC-IDS 2018 datasets.

From previous research, there are several problems. First, many still use a single machine learning, leading to ineffectiveness in identifying all types of attacks [16]. Some algorithms are effective in detecting certain types of attacks, but less effective in detecting other types of attacks [17]. Secondly, class imbalance in the dataset was shown to affect detection accuracy. Attack types with minority samples have lower detection accuracy [16]. Third, Features that are relevant for a certain type of attacks may not be necessary for other attacks due to differences in attack behavior [18]. Fourth, most studies still use the outdated KDDCUP99 and NSL-KDD datasets. KDDCUP99 has a significant degree of redundancy [19], while NSL-KDD does not represent current network traffic, due to the lack of public datasets, and is only simulated [20].

To overcome this, hybrid learning was proposed which combines two algorithms because it can detect various types of attacks [17] and was proven to be effective in reducing bias due to imbalance [21]. Hybrid learning consists of three layers that combine LSTM and random forest (RF). In addition, the nearmiss-2 undersampling method is used to overcome class imbalance. Relevant feature selection is also implemented to improve performance, time efficiency, and reduce computational costs [22]. Feature selection is applied and evaluated using the chi-square and RF methods to determine the best feature combination at each layer. Furthermore, to obtain the optimal model, hyperparameter tuning is performed with random grid search. Finally, the CSE-CIC-IDS2018 dataset is used which is the latest dataset, created in 2018 [23].

From the evaluation results, the proposed three layer hybrid model effectively detects attacks that have minority samples. However, this three layer hybrid model has difficulty detecting infiltration that has a pattern similar to the benign class. This three layer hybrid model shows superior overall performance compared to single machine learning, deep learning, and ensemble learning from previous studies.

2. METHOD

The research involves several steps as shown in Figure 1 data processing, under sampling to address class imbalance, data split for training and testing data, feature selection to identify relevant attributes, hyperparameter tuning for optimal performance, and finally, hybrid model building. The three layer model is then evaluated with the performance metrics accuracy, precision, recall and F1-score. Through this comprehensive approach, a robust and reliable IDS is developed to detect potential security threats.

2.1. Dataset

The CSE-CIC-IDS2018 dataset is a collaborative project between Communications Security Institution (CSE) and Canadian Institute for Cybersecurity (CIC) created in 2018, consisting of 16 million data with two main categories 83% normal traffic data and 17% representing attack traffic data [23]. The dataset is divided into ten files, nine files contain 79 features and one file contains 83 features. Table 1 shows the class distribution by attack category where infiltration and web attacks are the lowest sampled attack categories having only 0.9975% and 0.0057% of the whole dataset respectively.

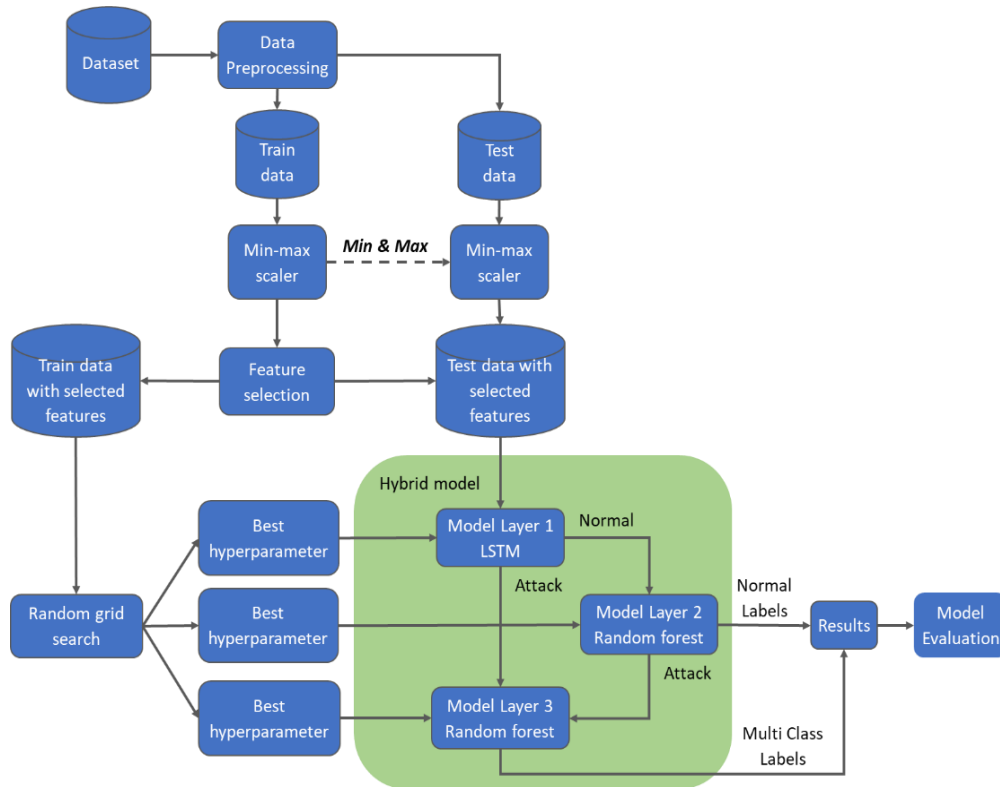


Figure 1. Research methodology

Table 1. Distribution of normal and attack class in network traffic distribution on CSE-CIC-IDS2018 dataset

Category	Class	Distribution (%)	Number of samples
Benign	Benign	83.070014%	13484708
DDoS	DDoS attack HOIC, DDoS attacks LOIC HTTP, DDoS attack LOIC UDP	7.786222%	1263933
DoS	DoS attacks SlowHTTPTest, DoS attacks GoldenEye, DoS attack Hulk, DoS attacks Slowloris	4.030692%	654300
Brute Force	FTP Brute force, SSH Brute force	2.346765%	380949
Bot	Bot	1.763026%	286191
Infiltration	Infiltration	0.997564%	161934
Web attacks	Brute force Web, Brute force XSS, SQL Injection	0.005717%	928
Total			16232943

2.2. Data preprocessing and sampling data

During this preprocessing stage, ten datasets were merged, duplicate headers were removed and timestemp features were converted to unix time. Features with NaN of more than 50% were removed, while data samples were removed on features that had NaN values of less than 50%. In addition, features that have no value variation and one of the two features that have similar value distribution are removed. After the preprocessing stage, from the initial 83 features, 20 features and 33,4072 data samples were removed, leaving 63 features with 1,589,8871 samples. To achieve class balance, the nearmiss-2 undersampling approach was used. NearMiss-2 has better performance than nearmiss-1 and nearmiss-3 [24]. Class balancing is performed with two ratios of 2:1, and 3:1 between normal and attack data. In addition, a scenario without class balancing was also considered. Then the dataset was divided into 80% training data and 20% testing data. To equalize the feature values into the same range data normalization was applied with the minmax scaler, scaling the features in the range [0,1]. Table 2 shows the comparison between normal and attack classes on each dataset.

2.3. Feature selection

Feature selection uses two chi-square [25] methods and RF [26] to identify important features for binary and multiclass target vectors. In determining feature importance, a cumulative score is calculated in relation to the target vector. A score percentage limit of 95% or 99% is applied. Features with a remaining

score percentage of 5% or 1% were eliminated, as they were considered less relevant. There were 8 feature combinations in each dataset and a total of 24 feature combinations were generated from the datasets (ratio 2:1, 3:1 and 4.79:1). This step plays an important role in identifying the most informative features at each layer thus contributing to the development of an effective and accurate hybrid model for intrusion detection as a whole.

Table 2. Comparison of normal class and attack class

Under Sampling	Ratio	Total sample	
		Benign	Attack
Nearmiss-2	2:1	5488800	2744400
Nearmiss-2	3:1	8233200	2744400
None	4.79:1	13154471	2744400

2.4. Hyperparameter tuning

Hyperparameter tuning is done by random grid search to save computational time and cost [27]. Random grid search selects a specific combination of hyperparameter values, then optimized by 5-fold cross validation. Hyperparameter tuning is performed on only a few hyperparameters to avoid expensive computational costs. Tables 3 and 4 show the range of hyperparameter values used for LSTM and RF, while other hyperparameters are set to default values from the scikit-learn library. Hyperparameter tuning was performed at each layer using 8 combinations of features on each dataset with ratios of 2:1, 3:1, and 4.79:1, resulting in a total of 72 combinations of hyperparameter values across the three datasets. From these combinations, the hyperparameter value that achieved the highest F1-score was selected for each layer. As a result, 12 hyperparameter combinations were identified, as shown in Table 5.

Table 3. Hyperparameter values LSTM for layer 1

Hyperparameter	Value
Hidden layer	16,32,48,64
Learning rate	0.0001,0.0005,0.001,0.005, 0.01,0.05,0.1
Dropout	0.1,0.2,0.3,0.4,0.5
Epoch	10, 20, 30, 40
Batch size	256, 512, 1024, 2048

Table 4. Hyperparameter values RF for layer 2 and layer 3

Hyperparameter	Value
Estimators	10,15,20,25,25,30,35,40,45,50
Max features	5,9,12,15,18
Max depth	None,5,10,15,20,25,30,35
Min samples split	2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Min samples leaf	2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Table 5. Best combination of hyperparameters from hyperparameter tuning

Dataset	Classification	Feature selection (method-vector target-score)	Total features	Best hyperparameter
Ratio 2:1 (nearmis-2)	Layer 1 LSTM	RF-Binary class-99%	50	unit: 64, learning_rate: 0.01, epochs: 30, dropout : 0.1, batch_size: 512
	Layer 2 RF	RF-Multi class-95%	37	n_estimators : 40, min_samples_split : 20, min_samples_leaf : 16, max_features : 15, max_depth : 15
	Layer 3 RF	RF-Binary class-99%	50	n_estimators: 25, min_samples_split: 4, min_samples_leaf: 3, max_features: 15, max_depth: 30
Ratio 3:1 (nearmis-2)	Layer 1 LSTM	Chi square-Binary kelas-99%	36	unit: 64, learning_rate: 0.01, epochs: 40, dropout: 0.2, batch_size: 512
	Layer 2 RF	RF-Multi class-95%	38	n_estimators: 50, min_samples_split: 17, min_samples_leaf: 10, max_features: 15, max_depth: 15
	Layer 3 RF	Chi square-Multi class-99%	46	n_estimators: 15, min_samples_split: 17, min_samples_leaf: 2, max_features: 15, max_depth: 30
Ratio 4.79:1 (None)	Layer 1 LSTM	Chi square-Binary class-99%	35	unit: 48, learning_rate: 0.1, epochs: 40, dropout: 0.1, batch_size: 1024
	Layer 2 RF	Chi square-Multi class-99%	37	n_estimators: 25, min_samples_split: 19, min_samples_leaf: 12, max_features: 15, max_depth: 20
	Layer 3 RF	Chi square-Binary class-99%	35	n_estimators: 35, min_samples_split: 3, min_samples_leaf: 2, max_features: 15, max_depth: 35

2.5. Three layer hybrid model algorithm

The use of LSTM in the first layer is because it has good performance in processing time-correlated data sequences such as network traffic and can remember the characteristics of previous network traffic [12]. In addition, LSTM is effective in detecting normal data. However, it has difficulty detecting minority classes such as infiltration and web attacks (Brute Force Web, Brute Force XSS, SQL Injection), as the results of previous studies [10]–[15]. Therefore, it is used in the first layer classified in binary with the aim of detecting normal data so as to reduce false positives (FPR). While RF effectively detects various types of attacks, especially attacks with a minority number of samples on unbalanced datasets and reduces the risk of overfitting [28]. Random forest is implemented in the second and third layers. In the second layer, RF reclassifies the normal data from first layer, aiming to detect malicious traffic that may be hidden among the normal data. Meanwhile, in the third layer, RF reclassifies attack data from the first and second layers to classify the type of attack in a multiclass manner and identify the type of attack more specifically.

The development of this three layer hybrid model is based on the selection of the best features and hyperparameters obtained in the previous step. The first layer classifies the data into two categories: benign (normal data) or attacks (attack data). If the data is classified as benign, it will be reclassified in the second layer into two more categories, namely benign or attacks. If the data is classified as benign, it becomes the final output. However, if the data is classified as attacks, it will be reclassified in the third layer. The third layer reclassifies data that has been classified as attacks from the first and second layers to determine a more specific class, be it "benign" or one of the other 14 types of attacks as in Table 1. Thus, this three layer hybrid model provides more useful results regarding the type of attacks detected.

3. RESULTS AND DISCUSSION

3.1. Experimental environment

The proposed three layer hybrid model is implemented with python 3.10, Jupyter lab 6.4.5, as well as Scikit-learn 1.0.2 and TensorFlow 2.8.0 libraries in windows 10 environment. Hardware includes AMD Ryzen 5 3400G CPU, 32 GB DDR4 memory. The steps taken include data preprocessing, feature selection, data splitting, hyperparameter tuning, model development and evaluation.

3.2. Model evaluation

The development of a three layer hybrid model was performed at each layer using three different datasets with ratios of 2:1, 3:1, and 4.79:1. A total of 12 models were built to form three hybrid models. The three layer hybrid model of multiclass classification is evaluated and the results are compared with the single LSTM and RF algorithms, as well as previous research. Based on the multiclass classification evaluation, the three layer hybrid model with a 3:1 ratio dataset showed better performance than the single LSTM and RF algorithms. The three layer hybrid model with a 3:1 ratio dataset uses 36 features in the first layer, 38 features in the second layer, and 46 features in the third layer. The selection of different relevant features at each layer improves IDS performance because the model is more dynamic in predicting attacks at each layer. Table 6 shows the comparison of the results with other developed models.

Table 6. Comparison of evaluation results of each algorithm

Algorithm	Ratio dataset	Feature selection (total features)	Multi-class classification (%)				Time (sec)	
			Accuracy	Precision	Recall	F1-score	Train	Test
RF	Ratio 4.79:1	None (63)	99.1893	99.0964	99.1893	99.1309	1107.95	20.44
RF	Ratio 4.79:1	Chi square (37)	99.2794	99.2099	99.2794	99.2351	1605.97	21.84
RF	Ratio 4.79:1	RF (47)	99.2053	99.1238	99.2054	99.1550	1837.51	27.85
LSTM	Ratio 4.79:1	None (63)	99.0785	98.9922	99.0785	98.7671	4079.36	120.80
LSTM	Ratio 4.79:1	RF (47)	99.0751	98.9830	99.0751	98.7609	8347.05	147.72
LSTM	Ratio 4.79:1	Chi square (37)	99.0713	98.9625	99.0713	98.7628	7548.48	159.82
Three layer hybrid learning (LSTM + RF)	Ratio 2:1	Layer 1 RF (50) Layer 2 RF (37) Layer 3 RF (50)	99.6812	99.6772	99.6812	99.6704	2653.4	41.8
Three layer hybrid learning (LSTM + RF)	Ratio 3:1	Layer 1 Chi square (36) Layer 2 RF (38) Layer 3 Chi square (46)	99.7618	99.7584	99.7618	99.7539	4147.3	53.99
Three layer hybrid learning (LSTM + RF)	Ratio 4.79:1	Layer 1 Chi square (35) Layer 2 Chi square (37) Layer 3 Chi square (35)	99.5033	99.4633	99.5033	99.4563	4698.7	92.04

The three layer hybrid model with a dataset ratio of 3:1 shows outstanding performance with the average multiclass classification evaluation results achieving 99.76% accuracy, 99.76% precision, 99.76%

recall, and 99.75% F1-score. Especially, the model is able to predict perfectly for a large number of attack types, as evidenced by 7 out of 15 classes having a recall value of 100%. Based on the misclassification analysis in Table 7, SQL Injection has the highest misclassification percentage of 23.53%. This is due to the small sample size of SQL Injection of only 87 samples or about 0.00054% of the entire dataset. Infiltration is the second highest attack type based on misclassification of 14.58%. Out of 4,619 misclassified infiltration samples, 4,619 of them were misclassified as benign. In addition, of the 593 misclassified benign samples, 590 were misclassified as infiltration. This suggests that some infiltration classes and benign classes have similar patterns, making it difficult for the model to differentiate between them.

Table 7. Evaluation of three-layer hybrid model and misclassification in multi-class classification

Category	Class	Precision	Recall	F1-score	Samples	Misclassification	
						Total	Percentage (%)
Benign	Benign	0.997194	0.99964	0.998415	1646640	593	0.036013
DDos	ddos_attack_hoic	1	1	1	137202	0	0
	ddos_attacks_loic_http	0.999974	0.999965	0.99997	115238	4	0.003471
Dos	ddos_attack_loic_udp	1	1	1	346	0	0
	dos_attacks_hulk	1	1	1	92382	0	0
	dos_attacks_slowhttptest	1	1	1	27978	0	0
	dos_attacks_goldeneye	1	1	1	8302	0	0
	dos_attacks_slowloris	1	0.999545	0.999772	2198	1	0.045496
Brute force	ftp_bruteforce	0.999974	1	0.999987	38671	0	0
	ssh_bruteforce	1	0.999947	0.999973	37518	2	0.005331
Bot	bot	1	1	1	57187	0	0
Infiltration	infiltration	0.97866	0.854184	0.912196	31677	4619	14.581558
Web attacks	brute_force__web	0.974138	0.957627	0.965812	118	5	4.237288
	brute_force__xss	1	0.956522	0.977778	46	2	4.347826
	sql_injection	0.928571	0.764706	0.83871	17	4	23.529412
Accuracy					2195520	5230	
Weighted avg		0.997584	0.997618	0.997539	2195520		

3.3. Comparison analysis

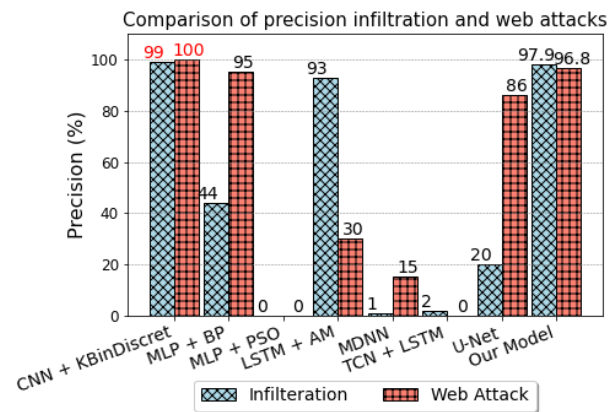
This section compares the performance of the proposed hybrid model with previous studies, as shown in Table 8. The results show that the proposed model achieves excellent performance, excelling in all attack categories. In particular, it achieves F1-scores of 91.22% for the infiltration category and 92.74% for the web attack category, which shows the reliability of the three layer hybrid model in detecting different types of attacks, even on classes with minority samples, much better than all previous research methods.

Table 8. Comparison of evaluation results of multiclass classification on the CSE-CIC-IDS2018

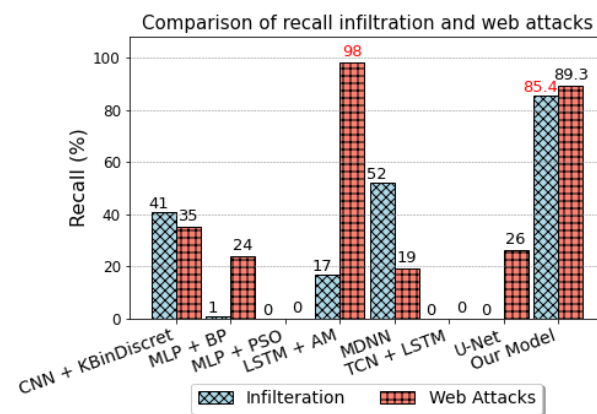
Method	Multi-class classification (%)			
	Accuracy	Precision	Recall	F1-score
CNN + KBinDiscretizer [10]	98	98	98	98
MLP + BP [11]	98.41	99.55	98.85	99.20
MLP + Particle swarm optimization (PSO) [11]	95.32	98.97	96.27	97.60
LSTM + AM [12]	96.1995	96	96	93
TCN [13]	97.53	97.89	97.25	97.22
TCN + LSTM [13]	97.77	97.94	97.53	97.73
U-Net [13]	94.65	94.88	94.55	94.71
Deep auto encoder (DAE) + DNN [14]	95.79	95.38	95.79	95.11
Three layer hybrid learning LSTM + RF with Ratio 3 : 1 (Our Model)	99.7618	99.7584	99.7618	99.7539

There are two models from previous research that have good performance in detecting attacks with minority classes, namely CNN+KBinDiscretizer and LSTM+AM. In Figure 2(a) The CNN+KBinDiscretizer model has a very high precision rate for infiltration at 99% and web attacks at 100%. However, the main drawback of this model is the low recall for both categories at only 41% for infiltration and 35% for web attacks. This means the model has difficulty detecting a large number of attacks from the class of infiltration and web attacks. Meanwhile, in Figure 2(b) the LSTM+AM model has a high recall, reaching 98% for the web attacks category. This shows the model's ability to detect most attacks from the web attacks category. However, it has a very low precision of only 30%, indicating a tendency to misclassify other categories as web attacks. On the other hand, LSTM+AM has a low recall for the infiltration category, at only 17%, indicating that the model tends to mispredict most infiltration attacks. However, it has a precision of 93% which indicates low misclassification of other categories as infiltration attacks.

Meanwhile, the proposed three layer hybrid learning LSTM+RF achieves high precision for infiltration at 97.86% and web attacks at 96.76%. In addition, the model has a high recall for both classes, which is 85.42% for infiltration, and 89.3% for web attacks. These results show that the three layer hybrid model is more effective in detecting most attacks from the infiltration and web attacks categories, and reduces the risk of misprediction of other categories into both categories.



(a)



(b)

Figure 2. Comparison of results (a) precision and (b) recall on infiltration and web attacks between methods

4. CONCLUSION

A three layer hybrid algorithm, which combines LSTM and RF, has shown potential to improve performance and reduce false detection (false positives and false negatives) in intrusion detection systems. The three layer hybrid model achieved impressive results, especially with a data set ratio of 3:1. The evaluation of multiclass classification showed average accuracy, precision, recall and F1-score above 99%. This demonstrates the effectiveness of the model in detecting multiple classes of network traffic. The overall success of the three layer hybrid model was shown to reduce false positive and false negative and was able to detect attacks with a minority number of samples, thus outperforming the single algorithm approach and previous research using various methods on CSE-CIC-IDS2018. The three layer hybrid learning approach promises a solution to improve intrusion detection performance in dynamic network traffic.




REFERENCES

- [1] S. Morgan, "Cybercrime to cost the world \$10.5 trillion annually by 2025," *Cybercrime Magazine*, 2020. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (accessed Feb. 03, 2022).
- [2] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, "Improving the resilience of wireless sensor networks against security threats: a survey and open research issues," *International Journal of Technology*, vol. 9, no. 4, Jul. 2018, doi: 10.14716/ijtech.v9i4.1526.
- [3] C. Day, "Intrusion prevention and detection systems," in *Managing Information Security*, Elsevier, 2013, pp. 119–142.
- [4] H.-J. Liao, C.-H. R. 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, Jan. 2013, doi: 10.1016/j.jnca.2012.09.004.





- [5] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Machine learning towards intelligent systems: applications, challenges, and opportunities," *Artificial Intelligence Review*, vol. 54, no. 5, pp. 3299–3348, Jun. 2021, doi: 10.1007/s10462-020-09948-w.
- [6] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: a systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018, doi: 10.1109/ACCESS.2018.2872784.
- [7] M. V. Kotpallivar and R. Wajgi, "Classification of attacks using support vector machine (SVM) on KDDCUP'99 IDS database," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, Apr. 2015, pp. 987–990, doi: 10.1109/CSNT.2015.185.
- [8] H. Hota and A. K. Shrivastava, "Decision tree techniques applied on NSL-KDD data and its comparison with various feature selection techniques," in *Advanced Computing, Networking and Informatics-Volume 1: Advanced Computing and Informatics Proceedings of the Second International Conference on Advanced Computing, Networking and Informatics (ICACNI)*, 2014, pp. 205–211.
- [9] Y. Liao and V. R. Vemuri, "Use of k-nearest neighbor classifier for intrusion detection," *Computers and Security*, vol. 21, no. 5, pp. 439–448, Oct. 2002, doi: 10.1016/S0167-4048(02)00514-X.
- [10] J. Yoo, B. Min, S. Kim, D. Shin, and D. Shin, "Study on network intrusion detection method using discrete pre-processing method and convolution neural network," *IEEE Access*, vol. 9, pp. 142348–142361, 2021, doi: 10.1109/ACCESS.2021.3120839.
- [11] S. Alzughairi and S. El Khediri, "A cloud intrusion detection systems based on DNN using backpropagation and PSO on the CSE-CIC-IDS2018 dataset," *Applied Sciences*, vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042276.
- [12] P. Lin, K. Ye, and C.-Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," in *Cloud Computing CLOUD 2019*, Springer International Publishing, 2019, pp. 161–176.
- [13] A. Mezina, R. Burget, and C. M. Travieso-Gonzalez, "Network anomaly detection with temporal convolutional network and U-Net model," *IEEE Access*, vol. 9, pp. 143608–143622, 2021, doi: 10.1109/ACCESS.2021.3121998.
- [14] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprpto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," *Journal of Information Security and Applications*, vol. 58, May 2021, doi: 10.1016/j.jisa.2021.102804.
- [15] Q. R. S. Fitri and K. Ramli, "Implementation of ensemble learning and feature selection for performance improvements in anomaly-based intrusion detection systems," in *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, Jul. 2020, pp. 118–124, doi: 10.1109/IAICT50021.2020.9172014.
- [16] P. Mishra, V. Varadarajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.
- [17] H. Yao, Q. Wang, L. Wang, P. Zhang, M. Li, and Y. Liu, "An intrusion detection framework based on hybrid multi-level data mining," *International Journal of Parallel Programming*, vol. 47, no. 4, pp. 740–758, 2019, doi: 10.1007/s10766-017-0537-7.
- [18] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.
- [19] M. Tavallaei, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6, doi: 10.1109/CISDA.2009.5356528.
- [20] A. Devarakonda, N. Sharma, P. Saha, and S. Ramya, "Network intrusion detection: a comparative study of four classifiers using the NSL-KDD and KDD'99 datasets," *Journal of Physics: Conference Series*, vol. 2161, no. 1, Jan. 2022, doi: 10.1088/1742-6596/2161/1/012043.
- [21] L. Li, Y. Yu, S. Bai, Y. Hou, and X. Chen, "An effective two-step intrusion detection approach based on binary classification and k-NN," *IEEE Access*, vol. 6, pp. 12060–12073, 2018, doi: 10.1109/ACCESS.2017.2787719.
- [22] S.-H. Kang and K. J. Kim, "A feature selection approach to find optimal feature subsets for the network intrusion detection system," *Cluster Computing*, vol. 19, no. 1, pp. 325–333, Mar. 2016, doi: 10.1007/s10586-015-0527-8.
- [23] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116, doi: 10.5220/0006639801080116.
- [24] I. Mani and I. Zhang, "kNN approach to unbalanced data distributions: a case study involving information extraction," in *Proceedings of workshop on learning from imbalanced datasets*, 2003, vol. 126, pp. 1–7.
- [25] L. Huan and R. Setiono, "Chi2: feature selection and discretization of numeric attributes," in *Proceedings of 7th IEEE International Conference on Tools with Artificial Intelligence*, 1995, pp. 388–391, doi: 10.1109/TAL.1995.479783.
- [26] J. Rogers and S. Gunn, "Identifying feature relevance using a random forest," in *Subspace, Latent Structure and Feature Selection*, Springer Berlin Heidelberg, 2006, pp. 173–184.
- [27] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," *Journal of Machine Learning Research*, vol. 13, pp. 281–305, 2012.
- [28] A. S. More and D. P. Rana, "Review of random forest classification techniques to resolve data imbalance," in *1st International Conference on Intelligent Systems and Information Management (ICISIM)*, 2017, pp. 72–78, doi: 10.1109/ICISIM.2017.8122151.

BIOGRAPHIES OF AUTHORS







Ruki Harwahu    received the BE degree in computer engineering from Universitas Indonesia (UI), Depok, Indonesia, in 2011. He received the ME degree from UI, and the M.Sc. degree from the National Taiwan University of Science and Technology (NTUST), Taiwan, both in computer and electronic engineering, in 2013. He received Ph.D. degree in electronic and computer engineering from NTUST, in 2018. Currently, he is a lecturer and researcher, as well as head of computer network laboratory in Faculty of Engineering, UI. He serves as a member of the editorial board in two international journals. He is a member of experts for UI GreenMetric World University Rankings since 2018. He has been involved in organizing several international conferences. He received awards from CTCI Foundation Taiwan in 2017 and IEEE Indonesia Section in 2020. His current research interests include computer and communication networks, Internet of Things, and cyber security. He can be contacted at email: ruki.h@ui.ac.id.



Fajar Henri Erasmus Ndolu     currently he is a student of master's degree from Dept. of Electrical Engineering Universitas Indonesia. For research interest, he likes to study cybersecurity, telecommunication, machine learning, internet of things, and network engineering. He can be contacted at email: fajar.henri@ui.ac.id.



Marlinda Vasty Overbeek     currently she is a lecturer in the Department of Informatics Universitas Multimedia Nusantara. Her expertise is in machine learning, natural language processing, and pattern recognition. She can be contacted at email: marlinda.vasty@umn.ac.id.