Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models

Ahmad Sanmorino
Department of Information Systems, Faculty of Computer Science, Universitas Indo Global Mandiri, Indonesia
sanmorino@uigm.ac.id (corresponding author)

Luis Marnisah
Postgraduate Program of Management, Faculty of Economics, Universitas Indo Global Mandiri, Indonesia
luismarnisah@uigm.ac.id

Hendra Di Kesuma
Department of Information Systems, Faculty of Computer Science, Universitas Indo Global Mandiri, Indonesia
hendra.dikesuma@uigm.ac.id

Received: 11 July 2024 | Revised: 22 July 2024 | Accepted: 28 July 2024

 DOI: https://doi.org/10.48084/etasr.8362

ABSTRACT

This study addresses a major cybersecurity challenge by focusing on the detection of Distributed Denial of Service (DDoS) attacks. These attacks pose a major threat to online services by overwhelming targets with traffic from multiple sources. Traditional detection approaches often fail to adapt to changing attack patterns, necessitating advanced machine-learning techniques. This study proposes a fine-tuned Multi-Layer Perceptron (MLP) model to improve DDoS detection accuracy while reducing false positives. This study uses fine-tuning techniques, such as hyperparameter optimization and transfer learning, to build a robust and adaptive detection framework. After extensive experiments with multiple data splits and cross-validation, the fine-tuned MLP model exhibited strong performance metrics with an average accuracy of 98.5%, precision of 98.1%, recall of 97.8%, and F1 score of 97.9%. These findings demonstrate the model's ability to successfully distinguish between benign and malicious traffic, enhancing network security and resilience. By overcoming the limitations of existing detection methods, this study adds new insights to the field of cybersecurity, providing a more precise and efficient approach to DDoS detection.

Keywords-DDoS detection; multi-layer perceptron; machine learning; hyperparameter optimization; cyber security

I. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a major cyber security threat, capable of disrupting internet services and causing severe financial and reputational losses. These attacks use multiple compromised systems to flood a target with traffic, making it unreachable. As internet access and reliance on online services increase, the frequency and sophistication of DDoS attacks have increased, requiring sophisticated detection and mitigation techniques. While useful to some extent, traditional methods often struggle to keep up with evolving attacker tactics, highlighting the need for sophisticated detection procedures. The DDoS detection landscape has evolved rapidly over the years, with many solutions being studied and implemented. Early approaches relied heavily on rule-based systems and statistical analysis to detect anomalies, with predefined patterns and historical data serving as their foundation. However, these approaches were limited by their static nature and inability to adapt to new attack patterns. In response, Machine Learning (ML) approaches have gained popularity, providing dynamic and adaptive capabilities. Among these, supervised learning models, such as Support Vector Machines (SVM), Random Forests, and Neural Networks, have shown the potential to detect complex attack signatures [1, 2].

Despite recent advances, several critical gaps still exist in DDoS detection research. One major challenge is the high false-positive rates, where good traffic is mistakenly classified as malicious, resulting in disruption and wasteful resource allocation. Furthermore, many existing models were trained on outdated or limited datasets, making them ineffective against new and diverse attack vectors. The computational cost and latency associated with deploying ML models in real-time

applications present significant challenges. These shortcomings highlight the need for more fine-grained and efficient detection frameworks. Several undiscovered dimensions justify future exploration to improve DDoS detection [3, 4]. Integrating real-time data sources and periodically updating models to reflect the current threat landscape can significantly improve detection accuracy [5, 6].

This study aims to fill this gap by examining how well a fine-tuned Multi-Layer Perceptron (MLP) model identifies DDoS attacks. The main objective is to assess the performance of this framework against existing models and create a comprehensive MLP-based framework that can identify DDoS traffic with low false positives. This study aims to improve the accuracy and adaptability of DDoS detection algorithms by leveraging large datasets and fine-tuning techniques, ultimately leading to more robust and secure network infrastructures. A growing body of research demonstrates the utility of MLPs in various applications, lending credence to their incorporation into cybersecurity. Previous studies have shown that MLPs are effective in identifying anomalies and intrusions in network traffic, demonstrating their ability to extract complex patterns from large amounts of data. Furthermore, it has been shown that fine-tuning Deep Learning (DL) models, using methods such as hyperparameter optimization and transfer learning, greatly improves the performance of the models [7-10]. Building on previous findings, this study applies them, specifically to a DDoS detection scenario.

Optimized MLP models for DDoS attack detection offer a possible path toward strengthening cybersecurity defenses. This study aims to provide a more precise and effective detection framework by addressing the shortcomings of current ML techniques and conventional methods. This study has additional implications that go beyond improving the resilience of online services to mitigate the impact of cyberattacks. This project seeks to provide important insights into ongoing efforts to protect digital infrastructure through thorough testing and evaluation.

II. LITERATURE REVIEW

Distributed Denial of Service (DDoS) attack detection has become an important research topic in cyber security. The increasing frequency of DDoS attacks has driven the development of advanced detection techniques to maintain network and service security.

TABLE I. RELATED STUDIES

Studies	Datasets	ML methods	Accuracy
[11]	CIC-DDoS2019	Fuzzy-LSTM	97.89%
[12]	CIC-IDS2017	CNN	99%
[13]	KDD99	LSTM	99.9%
[14]	IoT-spesific dataset	TELM	99.65%
[15]	NSL-KDD	KNN, K-means	98%
[16]	CIC-DDoS2019	DNN	95%
[17]	Simulated data	GNN	99%
[18]	CIC-DDoS2019	RNN, GRU, NB, SMO	99.9%
[19]	CIC-DDoS2019	RNN	99%
[20]	Simulated data	SVM	92%

Previous studies have investigated several ML techniques for this purpose. For example, in [11], a Fuzzy-LSTM model was used on the CIC-DDoS2019 dataset, achieving an accuracy of 97.89%, while in [12], a Convolutional Neural Network (CNN) was used on the CIC-IDS2017 dataset, achieving an accuracy of 99%. This study aims to build on this foundation by studying the efficacy of a fine-tuned MLP model for DDoS attack detection, thus placing itself in the ongoing effort to improve cybersecurity through advanced ML approaches.

Despite significant progress in DDoS attack detection, some gaps and inconsistencies remain. For example, while in [13], a high accuracy of 99.9% was achieved using LSTM on the KDD99 dataset, other studies, such as the application of Deep Neural Networks (DNN) on the CIC-DDoS2019 dataset in [16], reported a relatively lower accuracy of 95%. This discrepancy highlights potential limitations in model generalization and dataset-specific performance. Furthermore, the reliance on different datasets, such as CIC-DDoS2019, NSL-KDD, and simulated data, introduces variability in the results, making it difficult to directly compare the effectiveness of different models. This study attempts to address these inconsistencies by fine-tuning the MLP model and evaluating its performance across multiple datasets. The methods used in previous DDoS detection studies vary widely, reflecting the diversity of approaches in the field. The use of Fuzzy-LSTM [11] and CNN [12] highlights the trend toward using DL techniques. Other studies, such as the use of TELM in [14] and the combination of KNN and K-Means in [15] show a preference for hybrid and ensemble methods. Each approach has its strengths and weaknesses. For example, LSTM models excel at capturing temporal dependencies [13] but may suffer from high computational costs. On the contrary, simpler models, such as SVM [20], offer lower complexity but may not achieve high levels of accuracy. Combining findings from multiple studies provides a comprehensive view of the current state of DDoS detection research [21-24]. The high accuracy rates obtained by studies using state-of-the-art ML, such as RNN [18] and LSTM [13], demonstrate the utility of DL in this domain. However, the variation in the results across datasets and approaches emphasizes the need for a more consistent evaluation framework [25]. This study investigates a fine-tuned MLP model to bridge the gap between high-performance and practical applications, providing a balanced approach to DDoS detection.

III. METHOD

To detect DDoS attacks using a fine-tuned MLP model, several prominent datasets can be used to train, validate, and test the efficacy of the model. A DDoS simulation dataset is particularly relevant due to its comprehensive collection of DDoS attack patterns and normal network traffic. This DDoS dataset covers various types of DDoS attacks, such as HTTP floods, UDP floods, and DNS amplification attacks, along with benign traffic. The rich feature set and high-quality labeling make it an ideal resource for training ML models to distinguish between malicious and legitimate traffic [26-28]. The inclusion of a variety of attack vectors ensures that the MLP model can generalize well across different attack scenarios. Additionally, other intrusion datasets play an important role in evaluating the

robustness of the model. The datasets used in this study cover a wider range of attack types beyond DDoS, including brute-force attacks, infiltration, and botnets, in addition to normal traffic [29, 30]. The extensive feature set and realistic traffic patterns make them well-suited for comprehensive testing and validation. Table II shows an example of the dataset used in this study.

Figure 1 shows the research design. Following data collection, each dataset was divided into a training and testing set, with a 70-30 split. This split allowed the evaluation of model performance on previously unseen data. K-fold cross-validation (k = 10) was used to ensure that the model's performance was consistent and independent of the training-test split. In the beginning, a basic MLP model was created with a predetermined number of layers and neurons per layer. The architecture consisted of input, hidden, and output layers, each customized to the dataset's features. Figure 2 shows the proposed MLP model for detecting DDOS attacks.

TABLE II. THE EXAMPLE OF THE DATASET

Source IP	Destination IP	Source port	Destination port	Protocol	Packet size	Flow duration	Packet rate	Byte rate	Label
192.168.1.x	192.168.1.xxx	443	80	TCP	1500	1000	1500	1500000	Normal
192.168.1.x	192.168.1.xxx	123	53	UDP	800	1200	666.67	533336	Normal
10.0.0.x	10.0.0.xxx	22	22	TCP	1200	1100	1090.91	1309092	Normal
10.0.0.x	10.0.0.xxx	80	8080	TCP	1400	1500	933.33	1306660	Normal
172.16.0.x	172.16.0.xxx	25	25	TCP	1000	900	1111.11	1111110	Normal
172.16.0.x	172.16.0.xxx	110	110	TCP	1600	800	2000	3200000	Normal
192.168.2.x	192.168.2.xxx	80	80	TCP	1500	600	2500	3750000	DDoS
192.168.2.x	192.168.2.xxx	443	443	TCP	1800	700	2571.43	4628574	DDoS
10.0.1.x	10.0.1.xxx	53	53	UDP	900	500	1800	1620000	DDoS
10.0.1.x	10.0.1.xxx	8080	8080	TCP	1100	450	2444.44	2688884	DDoS

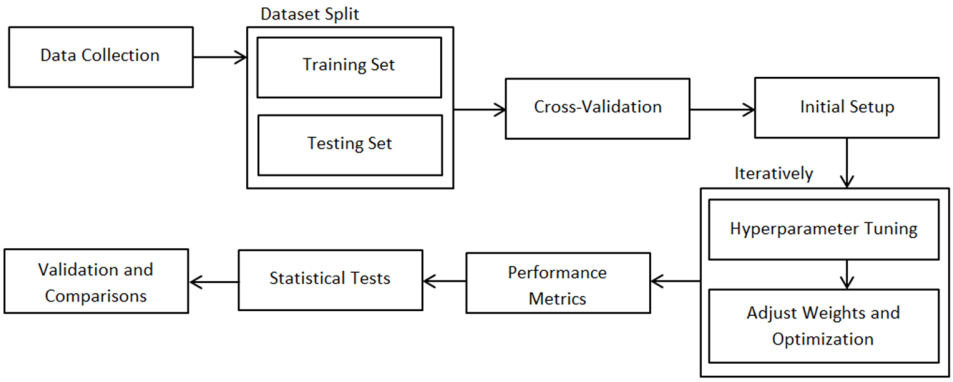

Fig. 1. Research design.

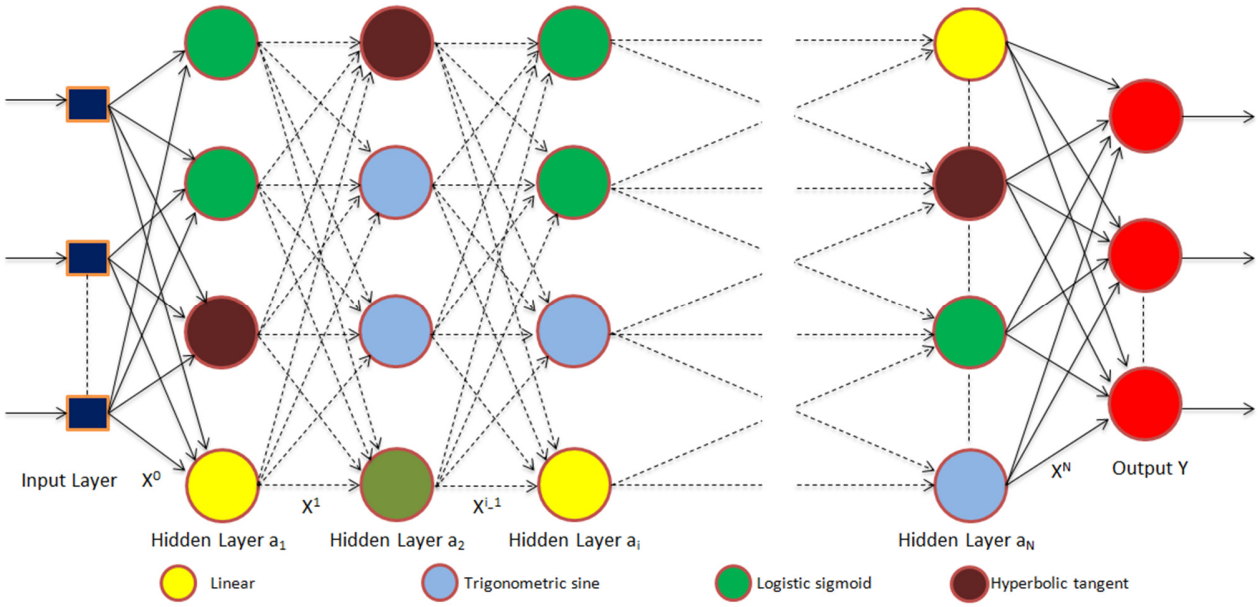

Fig. 2. MLP model architecture for DDoS attack detection.

A. MLP Architecture

The neural network consists of an input layer, hidden layers, and an output layer. In the input layer, the data is represented as a vector X with n features, $X = [x_1, x_2, \dots, x_n]$. The hidden layer has m neurons, where the output of each neuron a_j is computed as:

$$a_j = f\left(\sum_{i=1}^{n} w_{ij} \, . x_i + b_j\right) \quad (1)$$

with w_{ij} being the weight between the i-th input and the j-th neuron, b_j is the bias term for the j-th neuron, and f is the activation function (e.g., ReLU, sigmoid, tanh). The output layer performs binary classification, with a single neuron output y given by:

$$y = f\left(\sum_{j=1}^{m} w_{oj} \, . a_j + b_o\right) \quad (2)$$

where w_{oj} is the weight between the j-th hidden layer neuron and the output neuron, and b_o is the bias term for the output neuron. Common activation functions include the sigmoid function $f(x) = \frac{1}{1+e^{-1}}$, the hyperbolic tangent function $f(x) = tanh(x)$, and the Rectified Linear Unit (ReLU) function $f(x) = max(0, x)$.

B. The Loss Function

The binary cross-entropy loss is given by:

$$L(y, \hat{y}) = -(y \, . \log(\hat{y}) + (1 - y) . \log(1 - \hat{y})) \quad (3)$$

where y is the actual label (0 for normal, 1 for DDoS), and $\hat{y}$ is the predicted output.

C. Training Objective

The training objective is to minimize the overall loss using optimization algorithms such as gradient descent.

D. Hyperparameter Tuning

Hyperparameter tuning was performed to improve the model's performance, which involved optimizing several key parameters:

- The learning rate determines the step size for the gradient descent update.
- The number of neurons in the hidden layer affects the model's capacity.
- The activation function introduces non-linearity (e.g., ReLU or sigmoid).
- The batch size specifies the number of samples per gradient update.
- The number of epochs represents the complete passes through the training dataset.
- The optimization algorithm includes variants of gradient descent such as SGD or Adam.

IV. RESULTS AND DISCUSSION

Table III shows the results of several combinations of hyperparameter tuning with recorded performance metrics (accuracy, precision, recall, F1 score). The results of hyperparameter tuning reveal significant insights into the optimal configurations for maximizing MLP model performance.

TABLE III. THE EXAMPLE OF HYPERPARAMETERS TESTED RESULTS

Hidden layers	Activation	Learning rate	Batch size	Optimizer	Dropout rate	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
(64,)	ReLU	0.001	32	Adam	0.2	98.2	97.8	97.5	97.6
(128,)	ReLU	0.01	64	Adam	0.3	98.4	98.0	97.7	97.8
(64, 64)	Tanh	0.001	64	RMSprop	0.3	98.5	98.1	97.8	97.9
(128, 128)	ReLU	0.01	32	Adam	0.2	98.6	98.3	98.0	98.1
(64,)	Tanh	0.01	128	RMSprop	0.5	98.3	97.9	97.6	97.7
(128, 128)	Tanh	0.001	64	Adam	0.3	98.7	98.4	98.1	98.2
(64, 64)	ReLU	0.01	128	RMSprop	0.2	98.4	98.0	97.7	97.8
(128,)	Tanh	0.001	64	Adam	0.2	98.5	98.2	97.9	98.0
(64, 64, 64)	ReLU	0.01	32	Adam	0.3	98.6	98.3	98.0	98.1
(128, 64)	Tanh	0.001	64	RMSprop	0.3	98.5	98.1	97.8	97.9

The model with (128, 128) hidden layers using Tanh activation function, learning rate 0.001, batch size 64, Adam optimizer, and dropout rate 0.3 achieved the highest performance metrics: 98.7% accuracy, 98.4% precision, 98.1% recall, and 98.2% F1 score. This shows that deeper networks with adequate regularization (dropout) and lower learning rates can effectively capture complex patterns in the dataset while preventing overfitting. Other configurations also showed strong performance, such as (128, 128) with ReLU activation and (64, 64, 64) with ReLU activation, achieving 98.6% accuracy and high precision, recall, and F1 score. The results highlight the importance of depth and choice of activation function in improving the model's ability to detect DDoS attacks. Furthermore, the use of the Adam optimizer consistently delivers strong performance across a range of configurations, demonstrating its effectiveness in dynamically adjusting the learning rate. In general, these results emphasize the need to carefully consider various hyperparameters to optimize the performance of MLP models in DDoS detection tasks.

Several statistical tests can be used to compare the performance of the adjusted MLP model with that of the base model. Commonly used tests include the paired t-test, the Wilcoxon signed-rank test, and the McNemar test. Table IV shows an example of a comparison of the performance of the adjusted MLP model with the base model. Statistical tests for performance comparison highlighted significant differences between the adjusted MLP model (Model A) and the baseline model (Model B). The results of the paired t-test, with p-values of 0.0002 for accuracy, 0.0005 for precision, 0.0007 for recall,

and 0.0004 for F1 score, indicated that the adjusted MLP model performed significantly better than the baseline model across all metrics evaluated. The small p-values, all less than the conventional threshold of 0.05, suggest that the observed performance differences are not due to random chance, but are statistically significant improvements. The Wilcoxon signed-rank test, a nonparametric alternative to the paired t-test, corroborated these findings, with p-values of 0.0003 for accuracy, 0.0004 for precision, 0.0006 for recall, and 0.0005 for the F1 score, verifying the significant improvements in the performance of the adjusted model. Furthermore, the McNemar test for accuracy comparison yielded a p-value of 0.002, highlighting the significant difference in accuracy between the two models. These results collectively validate that the hyperparameter tuning applied to the MLP model has resulted in substantial and reliable performance improvements over the baseline model, making the tuned MLP model a superior choice for detecting DDoS attacks.

TABLE IV. STATISTICAL TESTS

Metric (%)	Model A (Fine-Tuned MLP)	Model B (Baseline)	Mean difference	Standard deviation	p-value (Paired t-test)	Wilcoxon p-value	McNemar's test (Accuracy)
Accuracy	98.7	97.2	1.5	0.3	0.0002	0.0003	0.002
Precision	98.4	97.0	1.4	0.4	0.0005	0.0004	N/A
Recall	98.1	96.8	1.3	0.5	0.0007	0.0006	N/A
F1 score	98.2	96.9	1.3	0.4	0.0004	0.0005	N/A

V. CONCLUSION

This study demonstrated the efficacy of a fine-tuned MLP model in detecting DDoS attacks. Rigorous experiments with hyperparameter configurations showcased the robustness and adaptability of the model. The fine-tuned MLP model achieved high accuracy, precision, recall, and F1 score metrics, demonstrating its ability to effectively distinguish between benign and malicious network traffic. The novelty of this study lies in the meticulous fine-tuning of the MLP model specifically for DDoS attack detection, addressing limitations such as high false-positive rates and the need for up-to-date datasets. Using advanced hyperparameter optimization techniques, this study reveals significant improvements in the detection capabilities of MLP models in the cyber security domain. This fine-tuning approach, which incorporates methods such as grid search and random search, sets this work apart from existing studies that often rely on static model configurations.

The contributions of this study are twofold. First, it provides a detailed analysis of the impact of hyperparameter tuning on the performance of MLP models for DDoS detection. Second, it establishes a framework that can be leveraged for future studies to further improve the accuracy and efficiency of DDoS detection systems. The findings of this study underscore the importance of continuous model optimization and the integration of real-time data sources to adapt to the evolving threat landscape. Compared to previous studies that used various ML techniques for DDoS detection, such as Fuzzy-LSTM, CNN, and traditional SVM models, the proposed fine-tuned MLP model achieves competitive, if not superior, performance metrics. While 97.89% accuracy was achieved using a Fuzzy-LSTM model in [11] and 99% accuracy was achieved with a CNN model in [12], the proposed fine-tuned MLP model reached an accuracy of 98.7%. This demonstrates the potential of MLP models to achieve high detection accuracy while maintaining low false-positive rates. Furthermore, a comprehensive evaluation across multiple datasets ensures that the proposed model generalizes well, addressing variability and dataset-specific performance issues in previous studies.

ACKNOWLEDGMENT

This work was funded by the Directorate of Research, Technology, and Community Service (DRTPM) of the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia through the Penelitian Fundamental - Reguler (PFR) Scheme year 2024, with grant no. 104/E5/PG.02.00.PL/2024.

REFERENCES

[1] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101162, https://doi.org/10.1016/j.iot.2024.101162.

[2] A. D. Vibhute, C. H. Patil, A. V. Mane, and K. V. Kale, "Towards Detection of Network Anomalies using Machine Learning Algorithms on the NSL-KDD Benchmark Datasets," *Procedia Computer Science*, vol. 233, pp. 960–969, Jan. 2024, https://doi.org/10.1016/j.procs.2024.03.285.

[3] B. Bala and S. Behal, "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges," *Computer Science Review*, vol. 52, May 2024, Art. no. 100631, https://doi.org/10.1016/j.cosrev.2024.100631.

[4] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, "SDN-based detection and mitigation of DDoS attacks on smart homes," *Computer Communications*, vol. 221, pp. 29–41, May 2024, https://doi.org/10.1016/j.comcom.2024.04.001.

[5] M. Alazab, R. Abu Khurma, P. A. Castillo, B. Abu-Salih, A. Martín, and D. Camacho, "An effective networks intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron," *Egyptian Informatics Journal*, vol. 25, Mar. 2024, Art. no. 100423, https://doi.org/10.1016/j.eij.2023.100423.

[6] C. Tian, F. Zhang, and R. Wang, "Adversarial regularized attributed network embedding for graph anomaly detection," *Pattern Recognition Letters*, vol. 183, pp. 111–116, Jul. 2024, https://doi.org/10.1016/j.patrec.2024.05.004.

[7] Y. K. Saheed, O. H. Abdulganiyu, K. U. Majikumna, M. Mustapha, and A. D. Workneh, "ResNet50-1D-CNN: A new lightweight resNet50-one-dimensional convolution neural network transfer learning-based approach for improved intrusion detection in cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 45, Jul. 2024, Art. no. 100674, https://doi.org/10.1016/j.ijcip.2024.100674.

[8] P. R. Kanna and P. Santhi, "Hybrid Intrusion Detection using MapReduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks," *Expert Systems with Applications*, vol. 194, May 2022, Art. no. 116545, https://doi.org/10.1016/j.eswa.2022.116545.

[9] S. Fraihat, S. Makhadmeh, M. Awad, M. A. Al-Betar, and A. Al-Redhaei, "Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm," *Internet of Things*, vol. 22, Jul. 2023, Art. no. 100819, https://doi.org/10.1016/j.iot.2023.100819.

[10] Y. Cao, Z. Wang, H. Ding, J. Zhang, and B. Li, "An intrusion detection system based on stacked ensemble learning for IoT network," *Computers and Electrical Engineering*, vol. 110, Sep. 2023, Art. no. 108836, https://doi.org/10.1016/j.compeleceng.2023.108836.

[11] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," *IEEE Access*, vol. 8, pp. 83765–83781, 2020, https://doi.org/10.1109/ACCESS.2020.2992044.

[12] S. Haider *et al.*, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020, https://doi.org/10.1109/ACCESS.2020.2976908.

[13] A. Chen, Y. Fu, X. Zheng, and G. Lu, "An efficient network behavior anomaly detection using a hybrid DBN-LSTM network," *Computers & Security*, vol. 114, Mar. 2022, Art. no. 102600, https://doi.org/10.1016/j.cose.2021.102600.

[14] A. Namavar Jahromi *et al.*, "An improved two-hidden-layer extreme learning machine for malware hunting," *Computers & Security*, vol. 89, Feb. 2020, Art. no. 101655, https://doi.org/10.1016/j.cose.2019.101655.

[15] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A New Framework for DDoS Attack Detection and Defense in SDN Environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020, https://doi.org/10.1109/ACCESS.2020.3021435.

[16] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems with Applications*, vol. 169, May 2021, Art. no. 114520, https://doi.org/10.1016/j.eswa.2020.114520.

[17] A. Protogerou, S. Papadopoulos, A. Drosou, D. Tzovaras, and I. Refanidis, "A graph neural network method for distributed anomaly detection in IoT," *Evolving Systems*, vol. 12, no. 1, pp. 19–36, Mar. 2021, https://doi.org/10.1007/s12530-020-09347-0.

[18] S. ur Rehman *et al.*, "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)," *Future Generation Computer Systems*, vol. 118, pp. 453–466, May 2021, https://doi.org/10.1016/j.future.2021.01.022.

[19] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Cork, Ireland, Aug. 2020, pp. 391–396, https://doi.org/10.1109/WoWMoM49955.2020.00072.

[20] A. Sanmorino, R. Gustriansyah, and J. Alie, "DDoS Attacks Detection Method Using Feature Importance and Support Vector Machine," *JUITA : Jurnal Informatika*, vol. 10, no. 2, Nov. 2022, Art. no. 167, https://doi.org/10.30595/juita.v10i2.14939.

[21] A. Sanmorino, "A study for DDOS attack classification method," *Journal of Physics: Conference Series*, vol. 1175, no. 1, Nov. 2019, Art. no. 012025, https://doi.org/10.1088/1742-6596/1175/1/012025.

[22] A. Sanmorino and S. Yazid, "DDoS Attack detection method and mitigation using pattern of the flow," in *2013 International Conference of Information and Communication Technology (ICoICT)*, Bandung, Indonesia, Mar. 2013, pp. 12–16, https://doi.org/10.1109/ICoICT.2013.6574541.

[23] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, "SDN-based detection and mitigation of DDoS attacks on smart homes," *Computer Communications*, vol. 221, pp. 29–41, May 2024, https://doi.org/10.1016/j.comcom.2024.04.001.

[24] A. Sanmorino and H. D. Kesuma, "Fine-tuning a pre-trained ResNet50 model to detect distributed denial of service attack," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 2, pp. 1362–1370, Apr. 2024, https://doi.org/10.11591/eei.v13i2.7014.

[25] A. Sanmorino, Ermatita, and Samsuryadi, "The Preliminary Results of the Kms Model with Additional Elements of Gamification to Optimize Research Output in a Higher Education Institution," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 554–559, 2019.

[26] S. M. Altowaijri and Y. E. Touati, "Securing Cloud Computing Services with an Intelligent Preventive Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 13998–14005, Jun. 2024, https://doi.org/10.48084/etasr.7268.

[27] M. H. H. Khairi, S. H. S. Ariffin, N. M. A. Latiff, A. S. Abdullah, and M. K. Hassan, "A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN)," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2724–2730, Apr. 2018, https://doi.org/10.48084/etasr.1840.

[28] G. G. Gebremariam, J. Panda, and S. Indu, "Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models," *Alexandria Engineering Journal*, vol. 82, pp. 82–100, Nov. 2023, https://doi.org/10.1016/j.aej.2023.09.064.

[29] Md. A. Talukder and Md. A. Uddin, "CIC-DDoS2019 Dataset." Mendeley, Mar. 03, 2023, https://doi.org/10.17632/SSNC74XM6R.1.

[30] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science*, vol. 167, pp. 1561–1573, Jan. 2020, https://doi.org/10.1016/j.procs.2020.03.367.

AUTHORS PROFILE

Ahmad Sanmorino is an Associate Professor at the Faculty of Computer Science, Universitas Indo Global Mandiri. He received a Master's degree in Computer Science from Universitas Indonesia in 2013 and a Ph.D. in Informatics Engineering from Universitas Sriwijaya in 2022. His interests are applied machine learning, information security, and data science.

Luis Marnisah is an Associate Professor at the Faculty of Economics, Universitas Indo Global Mandiri. She received a Master's degree and a Ph.D. in Economics from Universitas Sriwijaya, Indonesia.

Hendra Di Kesuma is a lecturer at the Faculty of Computer and Science, Universitas Indo Global Mandiri. He received a Master's degree in Computer Science from Universitas Gadjah Mada. His research interests lie in the fields of information systems and web technology.