Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2645~2653
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.10579

Optimization of cyber attack detection model using deep learning algorithm based on convolutional neural network

Hondor Saragih, Jonson Manurung
Informatics, Indonesia Defense University, Bogor, Indonesia

Article Info

Article history:

Received Apr 27, 2025
Revised Mar 25, 2026
Accepted Apr 19, 2026

Keywords:

Convolutional neural network
Cyber attacks
Deep learning
Intrusion detection
Network security

ABSTRACT

The increasing intensity and complexity of cyber threats demand more adaptive intrusion detection mechanisms. Conventional approaches are often limited in capturing complex and non-linear attack patterns in network traffic data. This study develops and evaluates a convolutional neural network (CNN)-based model for multi-class cyberattack detection. The proposed architecture integrates convolutional, pooling, and fully connected layers with rectified linear unit (ReLU) and SoftMax activation functions to improve classification performance. The network security laboratory-knowledge discovery and data mining (NSL-KDD) dataset is used for training and evaluation. Experimental results show that the CNN model achieves 96.34% accuracy and an F1-score of 0.99, outperforming several traditional machine learning methods, including Naïve Bayes (NB), decision tree (DT), support vector machine (SVM), and random forest (RF). The superior performance is attributed to the model's capability to automatically learn and extract meaningful spatial representations from network data without manual feature engineering. These findings demonstrate the effectiveness of deep learning techniques in improving cyberattack detection and contribute to the development of reliable AI-driven network security systems with strong potential for real-world cybersecurity applications and evolving threat mitigation strategies.

Corresponding Author:

Hondor Saragih
Informatics, Indonesia Defense University
Kawasan IPSC Sentul, Sukahati, Citeureup, Bogor, Jawa Barat 16810, Indonesia
Email: hondor.saragih@idu.ac.id

1. INTRODUCTION

The rapid development of information and communication technology (ICT) has driven digital transformation in various sectors, such as government, industry, education, and healthcare [1], [2]. This digitalization not only provides convenience in information exchange and increased operational efficiency, but also raises new challenges in the form of increasingly complex and difficult to detect cybersecurity threats. cyber attacks are no longer simple, but more sophisticated, structured, and adaptive to existing defense systems [3]–[5]. Based on reports from global and national cybersecurity agencies, such as the National Cyber and Crypto Agency (BSSN), there has been a significant increase in the number and intensity of cyberattacks in recent years, including distributed denial of service (DDoS) attacks, malware, ransomware, and exploitation of system vulnerabilities [6], [7]. This condition emphasizes the importance of developing a cyberattack detection system that is reliable, efficient, and capable of responding in real-time to evolving threats. Therefore, the need for artificial intelligence-based approaches, especially deep learning, is becoming increasingly urgent in an effort to anticipate and mitigate cyberattacks more effectively [8]–[10].

Despite various efforts to develop cyberattack detection systems, most existing approaches still rely on conventional signature-based and rule-based methods that have proven ineffective in identifying new attacks, including zero-day attacks and polymorphic attack variants [11]. These limitations lead to increased false positive and false negative rates, which ultimately compromise the effectiveness of the overall network security system. Most detection methods still rely on manual feature extraction processes that are not only time-consuming, but also prone to subjective bias and human error [12], [13]. In the midst of evolving threat dynamics, an approach that is able to recognize attack patterns automatically, adaptively, and accurately is needed. The implementation of deep learning algorithms, especially convolutional neural network (CNN), in the context of cyber attack detection is still not optimal and has not been studied in depth, both in terms of model architecture, computational efficiency, and validity of the detection results [14], [15]. This raises fundamental questions regarding the extent to which CNN can be optimized to be an effective solution in detecting and classifying cyberattacks in real-time and with high precision [15].

Various previous studies have examined the application of artificial intelligence methods in network intrusion detection systems, both through conventional machine learning approaches such as support vector machine (SVM), random forest (RF), and Naïve Bayes (NB) [16], [17], as well as through deep learning algorithms such as recurrent neural network (RNN) [18], autoencoder [19], and long short-term memory (LSTM) [20], [21]. These studies show significant potential in improving accuracy and automatic detection of attack patterns. A number of drawbacks are still found, including limitations in efficiently handling large data volumes, high training time complexity, and sensitivity to class imbalance in the dataset. Previous research results also indicate that most models still rely on manually extracted features, thus limiting the generalizability of the model to new, previously unknown attack types [22]. Several studies suggest the importance of exploring CNN models due to their ability to automatically and consistently extract spatial features, and strengthen the representation of attack patterns from network traffic data [23]–[25]. The application of CNNs in this field is still limited and has not been widely explored in the framework of architectural optimization and performance evaluation based on complex and current attack data. Therefore, this research is geared towards filling the void by offering a more structured and scalable approach.

This research aims to design and optimize a deep learning algorithm-based cyber attack detection model using CNN architecture that is able to identify various attack patterns automatically, accurately, and efficiently. The main focus of this research is to build a model that not only has reliable feature extraction capabilities, but is also able to minimize classification error rates, such as false positives and false negatives, which are common in conventional approaches [12], [26]. To achieve this goal, this research will implement the CNN model on representative benchmark datasets in the network security domain, such as network security laboratory-knowledge discovery and data mining (NSL-KDD) or CICIDS2017, to evaluate the model's performance based on relevant evaluation metrics, including accuracy, precision, recall, and F1-score. In addition, this research also aims to compare the performance of the CNN model with other existing detection methods, so as to gain a more comprehensive understanding of the effectiveness of this approach in the context of modern cyberattack detection. Thus, this research is expected to make a real contribution to the development of cybersecurity systems that are adaptive, intelligent, and ready to be applied in real-world computing environments.

Although the study of deep learning-based cyberattack detection has undergone significant development in recent years, there are a number of research gaps that remain comprehensively unexplored. Previous research has focused on non-convolutional deep learning algorithms such as LSTM and autoencoder [20], [21], while the superior potential of CNN in terms of spatial feature extraction from network data is still relatively underutilized [27]. The proposed approach has not considered specific CNN architecture adjustments to the characteristics of network traffic data, so the performance of the model in detecting different types of attacks tends to vary and be inconsistent. There are limitations in empirical model validation, where evaluations are often only performed on one type of dataset or do not consider complex and dynamic real-world attack scenarios. There is a lack of research that systematically integrates hyperparameter optimization techniques in CNN model development to improve detection performance [28]–[30]. Therefore, this research comes to bridge the gap by offering a CNN-based approach specifically designed for high-precision detection of cyberattacks through optimized architecture and comprehensive evaluation of various types of attacks in realistic scenarios.

This research offers novelty in the form of developing a CNN-based cyber attack detection model with an architecture optimization approach that is specifically tailored to the characteristics of network traffic data. Unlike previous research that tends to use generic CNN structures, this study designs convolution, pooling, and activation layer configurations adaptively to maximize feature extraction capabilities and improve classification accuracy against various types of cyber attacks, including unknown attacks [13], [31], [32]. This research also applies systematic hyperparameter tuning techniques to obtain the best combination of parameters in model training, and validates performance using several representative benchmark datasets that reflect the

complexity of real cyber environments [33]–[35]. The justification for conducting this research is based on the urgent need for an attack detection system that is not only accurate, but also able to adapt to the dynamics of evolving cyber threats. With this approach, it is expected that the research results can provide theoretical contributions in the development of intelligent detection algorithms as well as practical contributions in the implementation of a more effective and efficient network security system.

2. METHOD

Figure 1 shows the research methods used in this study. The research stages began with dataset collection and preprocessing, CNN architecture design, and model optimization. Next, performance evaluation and comparative analysis with classical algorithms were conducted to produce recommendations for the development of a more adaptive cyber attack detection system.

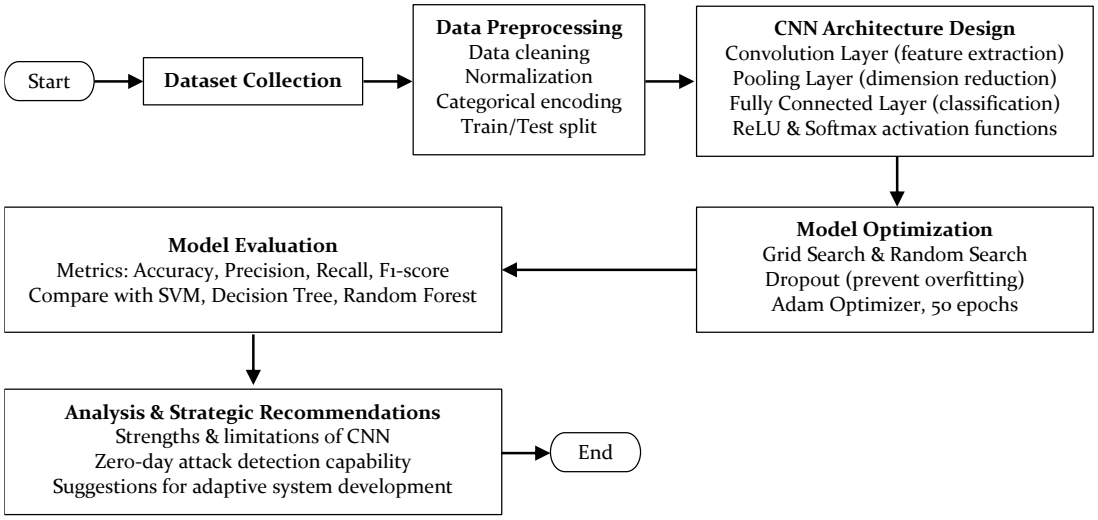

Figure 1. Flowchart of the cyber attack detection research method

This study adopts a quantitative experimental approach by implementing deep learning techniques, particularly a CNN architecture, to enhance the effectiveness of cyberattack detection [36]. The research utilizes two widely recognized public datasets in the field of network security, namely NSL-KDD and CICIDS2017, which encompass a diverse range of both conventional and sophisticated attack types. The research procedure begins with a comprehensive data preprocessing stage, including data cleansing, normalization, encoding of categorical variables, and partitioning of the dataset into training and testing sets. The CNN model is structured with key components such as convolutional layers for feature extraction, pooling layers for dimensionality reduction, and fully connected layers for classification, supported by rectified linear unit (ReLU) and SoftMax activation functions to facilitate multi-class classification.

Model optimization is conducted through hyperparameter tuning using grid search and random search strategies, complemented by the implementation of dropout techniques to reduce the risk of overfitting [37]. The training process employs the Adam optimizer over 50 epochs. Model performance is evaluated using standard metrics, including accuracy, precision, recall, and F1-score. To ensure robustness, the proposed model is compared against several conventional machine learning algorithms, such as SVM, decision tree (DT), and RF. The evaluation outcomes are further analyzed to identify the strengths and limitations of the CNN model in detecting various forms of cyberattacks, including zero-day threats, and to formulate strategic insights for developing more adaptive and accurate intrusion detection systems in future research.

3. RESULTS AND DISCUSSION

The mathematical model of the CNN architecture developed in cyberattack detection research is represented as a composition function of several non-linear transformations of the input data *X*.

$$\hat{y} = f(X;\theta) = f_L \circ f_{L-1} \circ \cdots \circ f_1(X) \quad (1)$$

where: $\hat{y}$ is prediction output (probability of each class), $X \in \mathbb{R}^{mxn}$ is input data (matrix representation of network features), f_i is non-linear transformation at the i-th layer, and θ is a set of parameters that includes weights and biases at all layers:

– Convolution layer

A two-dimensional convolution operation on input X with filter K can be defined:

$$Z_{i,j}^{(l)} = \sum_{m=1}^{M} \sum_{n=1}^{N} K_{m,n}^{(l)} \cdot X_{i+m-1,j+n-1}^{(l-1)} + b^{(l)} \quad (2)$$

where: $Z_{i,j}^{(l)}$ is output value of the neuron at position (i,j) in the l^{th} layer, $K_{m,n}^{(l)} \in \mathbb{R}^{mxn}$ is convolution kernel/filter, $b^{(l)}$ is bias, and $X^{(l-1)}$ is the output of the previous layer.

– ReLU activation function

After convolution, the ReLU activation function is applied.

$$A_{i,j}^{(l)} = ReLU\left(Z_{i,j}^{(l)}\right) = max\left(0, Z_{i,j}^{(l)}\right) \quad (3)$$

– Pooling layer

The max pooling layer is used to reduce the spatial dimension of the feature map:

$$P_{i,j}^{(l)} = max_{(m,n)\in W} A_{\delta \cdot i+m, \delta \cdot j+n}^{(l)} \quad (4)$$

where: W is pooling area, δ is steps (stride), and $P_{i,j}^{(l)}$ is maximum value in the combined region.

– Fully connected layer

The output of the last layer of convolution and pooling is averaged and given to the fully connected layer:

$$h^{(l)} = \sigma\left(W^{(l)} \cdot h^{(l-1)} + b^{(l)}\right) \quad (5)$$

where: $h^{(l)}$ is activation vector at the l^{th} layer, $W^{(l)}$ is weight matrix, $b^{(l)}$ is bias vector, and σ is activation function, e.g., ReLU.

– Output layer-SoftMax

$$\hat{y}_i = \frac{\exp(h_i)}{\sum_{j=1}^{C} \exp(h_j)} \quad (6)$$

where: $\hat{y}_i$ is probability of predicting the i^{th} class, C is number of classes (e.g., attack types), and h_i is logit score before SoftMax.

– Loss function-cross entropy

This model is optimized by minimizing the categorical cross-entropy loss function:

$$\mathcal{L} = -\sum_{i=1}^{C} y_i log(\hat{y}_i) \quad (7)$$

where: $y_i \in \{0,1\}$ is the actual label in the form of one-hot encoding and $\hat{y}_i$ is prediction probability of SoftMax.

4. CONVOLUTIONAL NEURAL NETWORK MODEL TESTING RESULTS

This research aims to build and evaluate a CNN model to automatically detect cyber attacks through multi-class classification. The model is evaluated based on accuracy metrics, confusion matrix, as well as precision, recall, and F1-score values of each class. The CNN model that has been trained and tested shows excellent performance, with a test accuracy rate of: 96.34%. This result indicates that the model was able to correctly classify the majority of the test data, even though the data had not been previously seen during the training process.

The model shows excellent performance in the normal and R2L/U2R classes, with a very low classification error rate. The largest errors occur in the DoS and Probe classes, which may be due to feature similarity or unbalanced data distribution. The classification performance evaluation is shown in the form of a confusion matrix in Table 1.

Table 1. Classification performance evaluation

Actual/predicted class	Normal	DoS	Probe	R2L/U2R
Normal	2,154	5	0	0
DoS	8	2,031	12	4
Probe	0	7	1,889	16
R2L/U2R	0	1	9	2,120

Based on Table 1, the classification model demonstrates a very high level of accuracy across all classes, as indicated by the dominance of values along the main diagonal of the confusion matrix, such as Normal (2,154), DoS (2,031), Probe (1,889), and R2L/U2R (2,120) being correctly predicted. Misclassifications are relatively minimal and mostly occur between classes with similar characteristics, for example several DoS instances incorrectly predicted as Probe (12) and Normal (8), as well as Probe instances misclassified as R2L/U2R (16). The small distribution of errors indicates that the model has strong discriminative capability in distinguishing between normal traffic and various types of attack categories. Further evaluation was conducted by calculating the precision, recall, and F1-score values for each class. The results are presented in Table 2.

Table 2. CNN model classification report

Class	Precision	Recall	F1-score	Sample number
Normal	0.99	1.00	0.99	2,159
DoS	0.99	0.98	0.99	2,055
Probe	0.98	0.98	0.98	1,912
R2L/U2R	0.99	0.99	0.99	2,130
Accuracy	-	-	0.96	8,256
Macro Avg	0.99	0.99	0.99	-
Weighted Avg	0.96	0.96	0.96	-

F1-score values above 0.96 for all classes indicate that the model is balanced in detecting cyberattacks with a high level of precision and sensitivity. To observe the dynamics of model training, we visualized the accuracy and loss values during the training and validation processes, as shown in Figures 2 and 3.

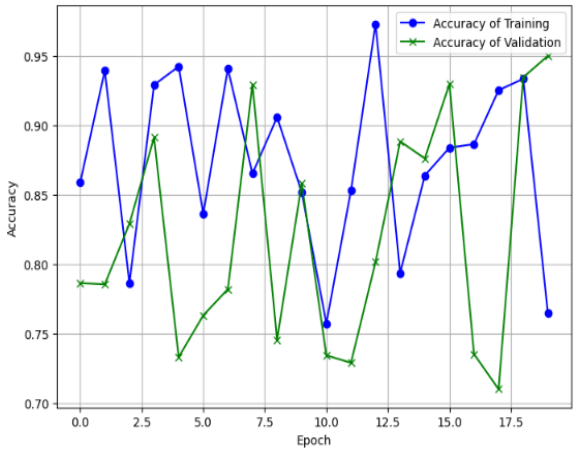

Figure 2. CNN model training and validation accuracy chart

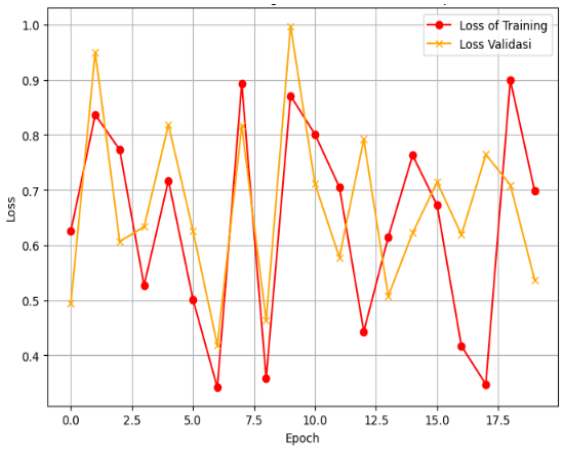

Figure 3. CNN model training and validation loss graph

The consistently increasing accuracy curve and decreasing loss values indicate a stable training process without significant overfitting. This indicates that the model is able to generalize well to the test data. To measure the superiority of the CNN model, a performance comparison was conducted with several conventional models commonly used in cyber attack detection research. The results are presented in Table 3.

Table 3. Comparison of CNN model performance with other models

Models	Accuracy (%)	Precision	Recall	F1-score
CNN (proposed)	96.34	0.99	0.98	0.99
NB	84.12	0.81	0.84	0.82
DT	91.75	0.91	0.92	0.91
SVM (linear)	89.43	0.89	0.88	0.88
RF	94.05	0.94	0.93	0.93

Based on Table 3, the CNN model (proposed) shows the best performance compared to other classification models, with an accuracy of 96.34%, precision of 0.99, recall of 0.98, and F1-score of 0.99. This performance is significantly higher than NB (84.12% accuracy), linear SVM (89.43%), and DT (91.75%), and still superior to RF, which achieved an accuracy of 94.05%. This advantage shows that the CNN model is more consistent in accurately identifying classes with a very low error rate. The CNN model significantly outperforms traditional models in all evaluation metrics, especially in its ability to automatically detect complex attack patterns. CNN's capability to extract spatial features directly from input data without requiring manual feature engineering provides a substantial advantage over conventional machine learning approaches, resulting in higher classification accuracy, precision, recall, and overall F1-score.

In order to gain a more comprehensive understanding of the CNN model's performance in detecting cyberattacks based on multi-class classification, a comparative analysis was conducted against several comparison models commonly used in the cybersecurity domain, namely NB, DT, and SVM with linear kernel and RF. The following line graph visualization is based on four main evaluation metrics, namely accuracy, precision, recall, and F1-score, each of which reflects the model's ability to classify data accurately, consistently, and balanced. The arrangement of the metrics on the horizontal (X) axis allows a comprehensive observation of the relative contribution of each model to each performance indicator. Figure 4 shows that the CNN model consistently achieved the highest scores across all metrics, confirming its superiority in the context of detecting complex, high-volume cyber attacks.

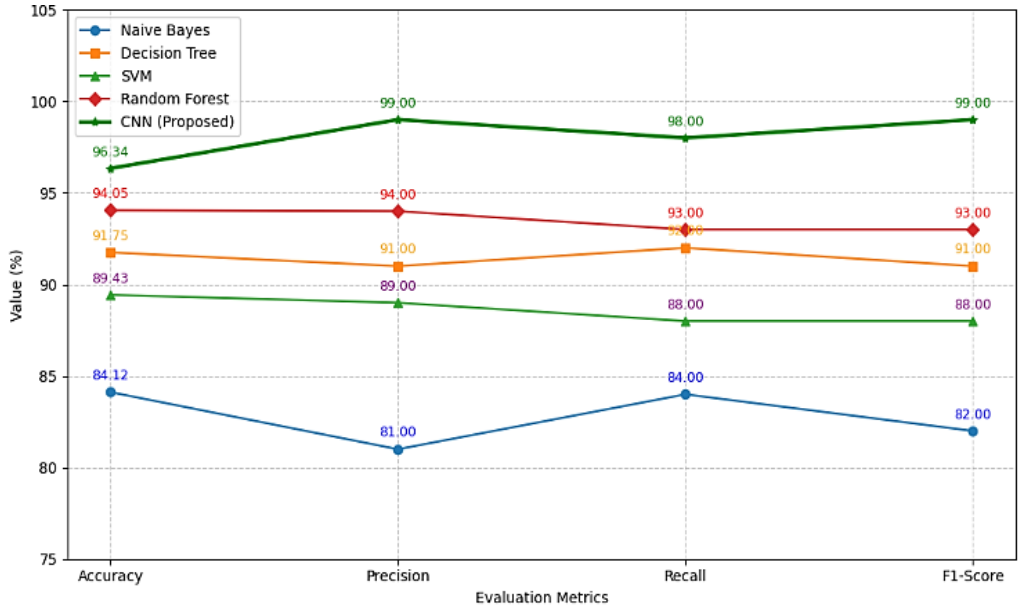

Figure 4. Comparison chart of cyber attack detection model performance

5. DISCUSSION

The results of this study show that the CNN model developed specifically for cyber attack detection is able to outperform various traditional comparison models, such as NB, DT, SVM, and RF. CNN obtained the highest accuracy of 96.34% with F1-score reaching 0.99, indicating the model's excellent generalization ability to cyber attack data in various categories. CNN's superiority in extracting spatial features from network data without the need for manual feature engineering provides added value in the context of complex and dynamic cyber data processing. This shows that deep learning-based approaches are not only relevant, but also crucial in facing modern intrusion detection challenges that require speed, accuracy, and scalability.

The consistently high performance of the CNN model on all evaluation metrics demonstrates the efficiency of the architecture used, especially the convolution and pooling layers that are able to capture attack patterns with an optimal level of representation. Compared to the baseline model, CNN shows significant advantages on high-complexity attack categories, such as R2L and U2R, which are usually difficult to detect by conventional models due to limitations in recognizing hidden sequential or spatial patterns. These findings strengthen the argument that the use of CNNs in cyberattack detection systems can be a strong foundation for the development of adaptive and highly predictive artificial intelligence-based network security systems. Thus, the results of this research not only contribute to the strengthening of scientific literature in the field of cybersecurity, but also open up opportunities for real implementation in the network environment of the industrial and government world.

6. CONCLUSION

This study concludes that the proposed CNN model demonstrates superior performance in multi-class cyberattack detection, achieving an accuracy of 96.34% and an F1-score of 0.99, thereby outperforming conventional models such as NB, DT, SVM, and RF across all evaluation metrics. The effectiveness of the model is primarily attributed to its ability to automatically extract and learn complex spatial patterns from network traffic data without relying on manual feature engineering, resulting in high precision, recall, and overall classification robustness, even for complex attack categories such as R2L and U2R. These findings confirm that deep learning-based approaches, particularly CNN, provide a powerful and scalable solution for modern intrusion detection systems. Nevertheless, future research is recommended to focus on improving computational efficiency and enhancing the model's generalization capability toward unseen and evolving attack patterns by integrating advanced techniques such as transfer learning, data augmentation, and hybrid deep learning architectures, as well as validating the model in real-world and large-scale network environments to ensure its practical applicability and sustainability in dynamic cybersecurity contexts.

ACKNOWLEDGMENTS

The authors express their sincere gratitude to the Faculty of Defense Engineering and Technology at the Republic of Indonesia Defense University, Bogor, Indonesia, for their support. They also extend their appreciation to the anonymous reviewers for their insightful comments and constructive suggestions, which have significantly contributed to the improvement of this work.

FUNDING INFORMATION

The authors state that no financial support or funding was received for the conduct of this research, authorship, and/or publication of this article.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Hondor Saragih	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Jonson Manurung		✓		✓		✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The author declares that there is no conflict of interest regarding the publication of this paper. The author states that there are no known competing financial interests or personal relationships that could have influenced the work reported in this study.

DATA AVAILABILITY

The datasets used in this study are publicly available benchmark datasets in the field of cybersecurity, namely the NSL-KDD and CICIDS2017 datasets. These datasets can be accessed through their respective official repositories for research and academic purposes. The processed data and model implementation used to support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] S. Iyanna, P. Kaur, P. Ractham, S. Talwar, and A. K. M. N. Islam, "Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users?," *Journal of Business Research*, vol. 153, pp. 150–161, Dec. 2022, doi: 10.1016/j.jbusres.2022.08.007.

[2] M. A. M. Hashim, I. Tlemsani, and R. D. Matthews, "A sustainable University: Digital Transformation and Beyond," *Education and Information Technologies*, vol. 27, no. 7, pp. 8961–8996, Aug. 2022, doi: 10.1007/s10639-022-10968-y.

[3] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digital Communications and Networks*, vol. 8, no. 4, pp. 422–435, Aug. 2022, doi: 10.1016/j.dcan.2021.07.006.

[4] W. Duo, M. C. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, May 2022, doi: 10.1109/JAS.2022.105548.

[5] D. Du *et al.*, "A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-physical Power Systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727–743, 2023, doi: 10.35833/MPCE.2021.000604.

[6] A. B. d. Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks*, vol. 222, p. 109553, Feb. 2023, doi: 10.1016/j.comnet.2022.109553.

[7] O. I. Falowo, M. Ozer, C. Li, and J. B. Abdo, "Evolving Malware and DDoS Attacks: Decadal Longitudinal Study," *IEEE Access*, vol. 12, pp. 39221–39237, 2024, doi: 10.1109/ACCESS.2024.3376682.

[8] O. A. Ajala, C. C. Okoye, O. C. Ofodile, C. A. Arinze, and O. D. Daraojimba, "Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time," *Magna Scientia Advanced Research and Reviews*, vol. 10, no. 1, pp. 312–320, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0037.

[9] A. J. Bhuvaneshwari and P. Kaythry, "A Review of Deep Learning Strategies for Enhancing Cybersecurity in Networks," *Journal of Scientific and Industrial Research*, vol. 82, no. 12, pp. 1316–1330, Dec. 2023, doi: 10.56042/jsir.v82i12.1702.

[10] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, p. 102655, Mar. 2021, doi: 10.1016/j.scs.2020.102655.

[11] F. E. Husseini, H. Noura, O. Salman, and A. Chehab, "Advanced Machine Learning Approaches for Zero-Day Attack Detection: A Review," in *Proceedings of the 8th Cyber Security in Networking Conference: AI for Cybersecurity, CSNet 2024*, Dec. 2024, pp. 297–304, doi: 10.1109/CSNet64211.2024.10851751.

[12] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Applied Sciences (Switzerland)*, vol. 11, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/app11041674.

[13] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," *Internet of Things (Netherlands)*, vol. 20, p. 100615, Nov. 2022, doi: 10.1016/j.iot.2022.100615.

[14] M. K. Bhuyan, M. Kamruzzaman, S. I. Nilima, R. Khatoon, and N. Mohammad, "Convolutional Neural Networks Based Detection System for Cyber-attacks in Industrial Control Systems," *Journal of Computer Science and Technology Studies*, vol. 6, no. 3, pp. 86–96, Aug. 2024, doi: 10.32996/jcsts.2024.6.3.9.

[15] Q. A. Al-Haija and S. Zein-Sabatto, "An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks," *Electronics (Switzerland)*, vol. 9, no. 12, pp. 1–26, Dec. 2020, doi: 10.3390/electronics9122152.

[16] P. Vanin *et al.*, "A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning," *Applied Sciences (Switzerland)*, vol. 12, no. 22, p. 11752, Nov. 2022, doi: 10.3390/app122211752.

[17] M. Jawahar, N. K. C. Babu, K. Vani, L. J. Anbarasi, and S. Geetha, "Vision based inspection system for leather surface defect detection using fast convergence particle swarm optimization ensemble classifier approach," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4203–4235, Jan. 2021, doi: 10.1007/s11042-020-09727-3.

[18] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," *Computer Communications*, vol. 199, pp. 113–125, Feb. 2023, doi: 10.1016/j.comcom.2022.12.010.

[19] S. Moraboena, G. Ketepalli, and P. Ragam, "A deep learning approach to network intrusion detection using deep autoencoder," *Revue d'Intelligence Artificielle*, vol. 34, no. 4, pp. 457–463, Sep. 2020, doi: 10.18280/ria.340410.

[20] F. E. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, p. 65, Dec. 2021, doi: 10.1186/s40537-021-00448-4.

[21] S. Shende, "Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security," *International Journal of Engineering Research & Technology*, vol. V9, no. 06, Jul. 2020, doi: 10.17577/ijertv9is061016.

[22] Y. He, G. Meng, K. Chen, X. Hu, and J. He, "Towards Security Threats of Deep Learning Systems: A Survey," *IEEE Transactions on Software Engineering*, vol. 48, no. 5, pp. 1743–1770, May 2022, doi: 10.1109/TSE.2020.3034721.

[23] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," *Vehicular Communications*, vol. 35, p. 100471, Jun. 2022, doi: 10.1016/j.vehcom.2022.100471.

[24] Z. Yang *et al.*, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Computers and Security*, vol. 116, p. 102675, May 2022, doi: 10.1016/j.cose.2022.102675.

[25] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Applied Sciences (Switzerland)*, vol. 12, no. 16, p. 8162, Aug. 2022, doi: 10.3390/app12168162.

[26] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *Journal of Big Data*, vol. 11, no. 1, p. 16, Jan. 2024, doi: 10.1186/s40537-023-00870-w.

[27] M. Suresha, S. Kuppa, and D. S. Raghukumar, "A study on deep learning spatiotemporal models and feature extraction techniques for video understanding," *International Journal of Multimedia Information Retrieval*, vol. 9, no. 2, pp. 81–101, Jun. 2020, doi: 10.1007/s13735-019-00190-x.

[28] M. A. K. Raiaan *et al.*, "A systematic review of hyperparameter optimization techniques in Convolutional Neural Networks," *Decision Analytics Journal*, vol. 11, p. 100470, Jun. 2024, doi: 10.1016/j.dajour.2024.100470.

[29] D. Kilichev and W. Kim, "Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO," *Mathematics*, vol. 11, no. 17, p. 3724, Aug. 2023, doi: 10.3390/math11173724.
[30] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, "Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment," *Network*, vol. 3, no. 4, pp. 538–562, Dec. 2023, doi: 10.3390/network3040024.
[31] J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics (Switzerland)*, vol. 9, no. 6, pp. 1–21, Jun. 2020, doi: 10.3390/electronics9060916.
[32] M. Hussain, C. Cheng, R. Xu, and M. Afzal, "CNN-Fusion: An effective and lightweight phishing detection method based on multi-variant ConvNet," *Information Sciences*, vol. 631, pp. 328–345, Jun. 2023, doi: 10.1016/j.ins.2023.02.039.
[33] H. Bakır and Ö. Ceviz, "Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection," *Arabian Journal for Science and Engineering*, vol. 49, no. 9, pp. 13025–13043, Sep. 2024, doi: 10.1007/s13369-024-08949-z.
[34] A. Alsarhan *et al.*, "Optimizing Cyber Threat Detection in IoT: A Study of Artificial Bee Colony (ABC)-Based Hyperparameter Tuning for Machine Learning," *Technologies*, vol. 12, no. 10, p. 181, Sep. 2024, doi: 10.3390/technologies12100181.
[35] N. Berbiche and J. El Alami, "Enhancing Anomaly-Based Intrusion Detection Systems: A Hybrid Approach Integrating Feature Selection and Bayesian Hyperparameter Optimization," *Ingenierie des Systemes d'Information*, vol. 28, no. 5, pp. 1177–1195, Oct. 2023, doi: 10.18280/isi.280506.
[36] Y. Wang, X. Wang, Q. Ni, W. Yu, and M. Huang, "BCDM: An Early-Stage DDoS Incident Monitoring Mechanism Based on Binary-CNN in IPv6 Network," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5873–5887, Oct. 2024, doi: 10.1109/TNSM.2024.3431701.
[37] M. Subramanian, K. Shanmugavadivel, and P. S. Nandhini, "On fine-tuning deep learning models using transfer learning and hyper-parameters optimization for disease identification in maize leaves," *Neural Computing and Applications*, vol. 34, no. 16, pp. 13951–13968, Aug. 2022, doi: 10.1007/s00521-022-07246-w.

BIOGRAPHIES OF AUTHORS

Hondor Saragih is a lecturer at the Faculty of Defense Engineering and Technology, Republic of Indonesia Defense University, Bogor, Indonesia. He holds a Bachelor's degree in Informatics Engineering from Gunadarma University, Depok, Indonesia. He holds a Master of Science degree in Defense Science from Republic of Indonesia Defense University, Bogor, Indonesia and a Master of Management degree in Information Systems from Gunadarma University, Jakarta, Indonesia. In 2021 he received his Doctorate degree from the Doctor of Management Science Program at the State University of Jakarta, Jakarta, Indonesia. He can be contacted at email: hondor.saragih@idu.ac.id.

Jonson Manurung is a lecturer in the Computer Science Program, Faculty of Defense Engineering and Technology, Universitas Pertahanan Republik Indonesia, Bogor, Indonesia. He is an author who earned his bachelor's degree from the Electrical Engineering Program at the Institut Teknologi Medan, Medan, Indonesia. He completed his master's program in Computer Science at the Universitas Sumatera Utara, Medan, Indonesia, and earned his Ph.D. in Computer Science from the Universitas Sumatera Utara, Medan, Indonesia. His research interests lie in the field of Computer Science. He can be contacted at email: jhonson.geo@gmail.com.