Towards Lightweight Intrusion Identification in SDN-based Industrial Cyber-Physical Systems

Ahmad Zainudin*[†], Rubina Akter[‡], Dong-Seong Kim[§], and Jae-Min Lee[§]
*Department of Electronic Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea
[§]Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea
[‡]ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea
[†]Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia
(zai*, rubinaakter2836, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—Software-defined networks (SDN)-based industrial cyber-physical systems (CPS) enable customizing development opportunities with integrated network interconnection to perform monitoring, measurement, control system, and security tasks. The extensive connectivity and the vast amount of data exchange in the SDN-based industrial CPS environment make it vulnerable to cyberattacks. Furthermore, an SDN controller is a single attractive target for an attack. It is challenging when the SDN controller manages DL-based high-complexity intrusion detection in an IIoT network with low latency requirements to identify and prevent attacks. This study proposes a lightweight intrusion detection model in an SDN-based industrial CPS environment. The proposed model was evaluated using a recent publicly SDN-related cyber-security InSDN dataset. The experimental results show that the proposed model outperforms the state-of-the-art by achieving 98.95% accuracy, 99.00% precision, 98.91% recall, and a 0.164 ms time cost when using the LightGBM feature selection technique.**

***Index Terms*—lightweight IDS, SDN, industrial CPS, feature selection**

I. Introduction

The industrial internet of things (IIoT) is a massively distributed network connecting sensors and actuators to generate tremendous amounts of data with sensing, communication, and computing capabilities. Massive data generated over the networks can be efficiently analyzed, collected, and exchanged in an IIoT environment. IIoT applications have advanced to increase effectiveness and productivity in several sectors, such as manufacturing, healthcare, smart cities, retail, supply chain, automotive, and transportation [1]. IIoT utilizes cyber-physical systems (CPS) to address the complex architecture of physical entities and remotely connect them via cyber-components. CPS enables an integrated network interconnection to perform monitoring, measurement, control system, and security tasks. Therefore, CPS supports integrated computing, physical processing, and intelligent networking capabilities [2].

Industrial CPS requires new specifications related to heterogeneity and flexibility without reducing the quality of service (QoS). Software-defined networks (SDN) provide emerging requirements for heterogeneous entities with different protocols that allow customizing development opportunities [3]. SDN separates the application, control, and data planes. The SDN controller communicates with the application using the north-bound interface and the south-bound interface with network devices in the data plane [4]. SDN provides a framework for a security solution to quickly and precisely identify threats without wearing down IIoT equipment like firewalls, antivirus software, and intrusion detection systems (IDS).

The extensive connectivity and the vast amount of data exchange in the SDN-based industrial CPS environment make it vulnerable to cyberattacks. Furthermore, an SDN controller is a single attractive target for an attack. A distributed denial-of-service (DDoS) attack can disrupt, cause a failure, and restrict the communication channel between the control and the data planes. The dynamic nature of IIoT devices raises security issues such as denial of service (DoS), botnet malware, probe scan, web attacks, and various other kinds of attacks [5] [6].

An IDS platform tries to detect malicious activities in the networks, which is a challenging issue in IIoT networks. Machine learning (ML) and deep learning (DL) have advanced for intrusion detection and classification tasks. However, an SDN controller in SDN-based IIoT networks is a central device that handles all network services such as flow management, network management, network monitoring, intrusion detection, and load balancing services. It is challenging when the SDN controller manages DL-based high-complexity intrusion detection in an IIoT network with low latency requirements. Moreover, IDS must be able to identify attacks as rapidly as feasible and need low computing power to identify and prevent attacks [7] [8]. Moreover, heterogeneous connections lead to a sharp increase in intrusion threats with sophisticated capabilities in IIoT networks. The robustness of the IDS model is a need that cannot be disputed by increasing and more sophisticated cyber-attacks.

The significant contributions of this study are summarized as follows.

- We implemented a feature selection mechanism by leveraging an ML classifier such as extremely randomized trees (Extra Trees), extreme gradient boosting (XGBoost), and a light gradient boosting algorithm (LightGBM) to determine important features. Selected promising features can reduce model complexity and improve intrusion model performance.
- We evaluated the accuracy, precision, recall, loss, ROC score, and time cost of the feature selection strategies' performance. LightGBM was used to reduce feature

978-1-6654-9927-9/22/$31.00 ©2022 IEEE

dimensions while maintaining high accuracy and low computational cost.

- We proposed a lightweight CNN-GRU model to classify the cyber-attacks in SDN-based industrial CPS. This model applied a residual connection to improve training model performance and resolve the gradient vanishing problem. A factorized convolution architecture was exploited to conduct a lightweight model structure.

II. Related Works

Several approaches have been proposed and evaluated using DL-based lightweight intrusion detection models to address limited computing capabilities in the internet of things (IoT) networks. The authors [9] proposed a CNN-based deep neural network intrusion detection model by applying the principal component analysis (PCA) to reduce feature dimensions. Besides, this model was built by exploiting an inverse residual connection, channel shuffle operation, compression, and expansion structure to get low computational cost and effective feature extraction. Applying feature dimensions reducing algorithm will reduce some promising features and effects for model performance. In 5G networks, wireless intrusion detection systems are implemented to combat malicious activities. The authors [10] proposed a deep auto-encoded dense for detecting intrusion in 5G and IoT networks. The model was evaluated with the Argean Wi-Fi intrusion dataset.

The authors [11] implemented a lightweight CNN-LSTM-based intrusion detection for security in IIoT. This model uses the UNSW-NB15 dataset to evaluate the proposed model's performance. This model did not consider the feature selection mechanism, so the model has a high computational cost and is unpracticable for low-latency intrusion detection and prevention applications. The authors [12] evaluated an ML-based SVM for intrusion detection in IoT networks. The proposed model achieved 98.03% accuracy for the CICIDS2017 dataset in the binary classification case. Intrusion detection capability is still not enough for recent cyber-attacks. In recent sophisticated attacks, IDS requires an intrusion classification capability to determine a defense mechanism.

Combining ML/DL with feature selection can reduce the computational cost with improved model performance. The authors [13] performed a decision tree (DT) model with a Pearson's correlation coefficient (PCC) feature selection mechanism to detect malicious traffic in a SCADA-based smart factory. A PCC technique was required to ensure the reduction of over-fitting. The model was evaluated using two public datasets: CIRA-CIC-DoHBrw-2000 and the NSL-KDD dataset. The best accuracy was achieved at 99.2% for intrusion detection cases. The authors [14] applied an ensemble feature selection technique by combining two ensemble algorithms: random forest and AdaBoost, to boost the detection accuracy. This model achieved reduced training time and better accuracy. DDoS detection and classification in B5G networks were performed in [15] using composite multilayer perceptron (MLP) and PCC feature selection techniques. The proposed model was evaluated using the CICDDoS2019 dataset and achieved 99.66% accuracy. The authors [16] exploited ML algorithms: REP Tree, random tree, decision stump, J48 or C4.5, and random forest. The model was evaluated using the CICIDS2017 and CICDDoS2019 datasets and performed with SYN and UDP attacks, at 99.99% and 99.7%, respectively. A lightweight DL-based IDS was implemented by authors [17] for DDoS calssification in SDN-enabled IIoT networks. This approach exploits the ML classifier to choose the potential features. However, this work didn't use an SDN-related dataset to evaluate the proposed model.

III. Intrusion Detection in SDN-based Industrial CPS

Heterogenous connectivity in SDN-based industrial CPS networks is vulnerable to cyber-attacks. Furthermore, the SDN controller is the center of the network flow management, making it susceptible to being distributed by an unauthorized user or malicious network activities. This study proposes a DL-assisted intrusion identification framework with a lightweight architecture model. Fig. 1 shows the overall the proposed model. The SDN network architecture is separated into the application, control, and data planes. These application plane services include flow management, network monitoring, and balancing. The application plane communicates with the control plane through northbound interfaces (NBI). The proposed DL model was implemented in the SDN controller to classify cyber-attacks. The network traffic from the data plane was captured by the SDN controller as the input to the intrusion classification model. The control and data plane are connected using southbound interfaces (SBI). The proposed DL model can classify malicious activities such as DDoS, Probes, DoS, and brute-force-attack (BFA) attacks.

A. Dataset Description, Preprocessing and Feature Selection

This system utilized the SDN-related cyber-security InSDN dataset [5] to evaluate the proposed intrusion classification model. The InSDN dataset enables some cyber-attacks using OpenFlow protocols in the SDN architecture. The InSDN dataset provides some attacks such as DoS, DDoS, web attacks, remote to local (R2L), malware (botnet), probe, and user to root (U2R) attacks. This study considers four types of attacks (DoS, DDoS, Probe, BFA) and benign network activity.

Preprocessing was necessary to ensure excellent data quality before delivering the proposed model with the data features. This stage performs some procedures such as data cleaning and feature data normalization. In the data cleaning process, some non-contributing features (such as ”Timestamp”, ”Flow ID”, ”Src IP”, ”Dst IP”, ”SrcPort”, and ”Dst Port”) were eliminated. Furthermore, based on [5] through OpenFlow calls to the SDN switches, only statistical features may be generated from the SDN controller. In the InSDN dataset, forty-eight features are related to SDN networks and can be used for the feature selection mechanism. To prevent large variations in values across the features, this approach uses MinMax normalization based on Equation 1.

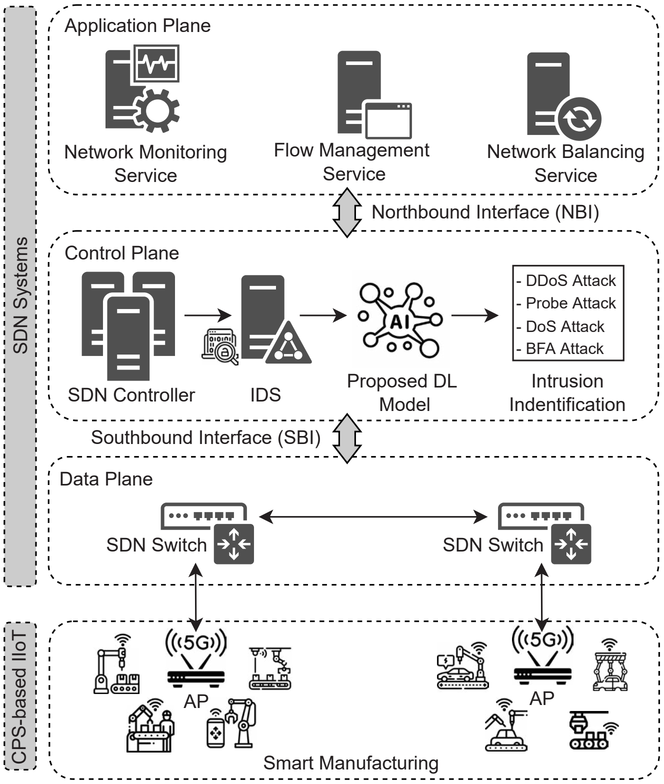


Fig. 1. Intrusion Identification in SDN-based CPS

$$X_n = \frac{X - X_{min}}{X_{max} - X_{min}}, \quad (1)$$

where X_n denotes the normalized data features with values ranging from [0,1]. This approach implemented an ML classifier-based feature selection mechanism (extra trees, xgboost, and lightGBM) to reduce feature dimension and select promising features to reduce model complexity and improve model performance.

B. Lightweight CNN-GRU-based Intrusion Identification

This section presents a lightweight CNN-GRU-based intrusion identification model. The proposed model consists of three main parts: pre-block, depth-wiseConv, and classification modules. The pre-block was conducted by stacked (1×3) and (3×3) convolution with an eight kernel size and ReLU activation. The depth-wiseConv module exploited residual connections to resolve the gradient vanishing problem and implement a factorized convolution architecture to conduct a lightweight model structure. The model utilized the two stacked depth-wiseConv structures for extracting features and the stacked GRU for attack classification.

The feature map pre-block output is directly fed to the depth-wiseConv module. Subsequently, deep feature maps are generated by (1×3) and (3×1) factorized convolution structures for a deep feature calculation. A depth-wise concatenation layer is used to aggregate the deep asynchronous feature maps. The concatenation layer computation is shown below:

TABLE I
PARAMETERS SETTING OF THE PROPOSED MODEL

Parameters	Value
Total Features (SDN-related)	48
Selected Features	30
Number of class	5
Cross Validation	5 k-fold
Activation Function	ReLU
Epoch	50
Batch Size	32
Optimizer	Adam
Learning rate	0.001
Loss Function	Cross-entropy

TABLE II
LIGHTGBM FS PERFORMANCE WITH DIFFERENT NUMBER OF A FEATURE FOR INTRUSION IDENTIFICATION

Number of Feature	Accuracy	Precision	Recall	Loss	Time-cost
10	98.88%	97.91%	97.86%	0.0604	0.302 ms
15	98.92%	98.94%	98.91%	0.0334	0.153 ms
20	98.80%	98.84%	98.76%	0.0406	0.126 ms
25	98.32%	98.36%	98.28%	0.0561	0.157 ms
30	98.98%	98.99%	98.96%	0.0275	0.164 ms

$$\mathcal{F}_{concat} = \mathcal{D}\left(X^{f}_{(1\times3)}\left(X_{(1\times3)}\right), X^{f}_{(3\times1)}\left(X_{(1\times3)}\right)\right), \quad (2)$$

where $\mathcal{D}$ represents the depth-wise concatenation's calculation, $X^{f}_{(1\times3)}$, and $X^{f}_{(3\times1)}$ represent the output of the factorized function for the parallel convolution layer with kernel sizes of (1×3) and (3×1). The $X_{(1\times3)}$ as the input of factorized block denotes the output of convolution layer with kernel size of (1×3). The dimension of concatenation output is reduced by feeding to the max-pooling layer with pool size $(2, 2)$ as follow:

$$\mathcal{F}_{pool} = \mathcal{P}_{(2,2)}\left(\mathcal{F}_{concat}\right). \quad (3)$$

here, $\mathcal{F}_{pool}$ denotes as the output of the max-pooling layer. Subsequently, the reduced feature map is fed to the (1×1) convolution layer and is added to the stacked convolution and pooling layer as a skip connection function. This process is conducted two times, and the last output is fed to the average pooling layer. Two stacked GRU layers with ReLU activation calculate the average pooling output. The output of the GRU layer is fed to the fully-connected and softmax layers to identify the cyber attacks.

Table I presents the proposed model's optimal parameter settings. The model performs excellent results using the following configurations: employed thirty selected subsets, k-fold cross validation of 5, ReLU activation function, mini batch-size of 8, Adam optimizer, a learning rate of 0.001, and applying a cross-entropy loss function.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This section evaluates the ML classifier-based extra-tress, xgboost, and lightGBM feature selection techniques to assist

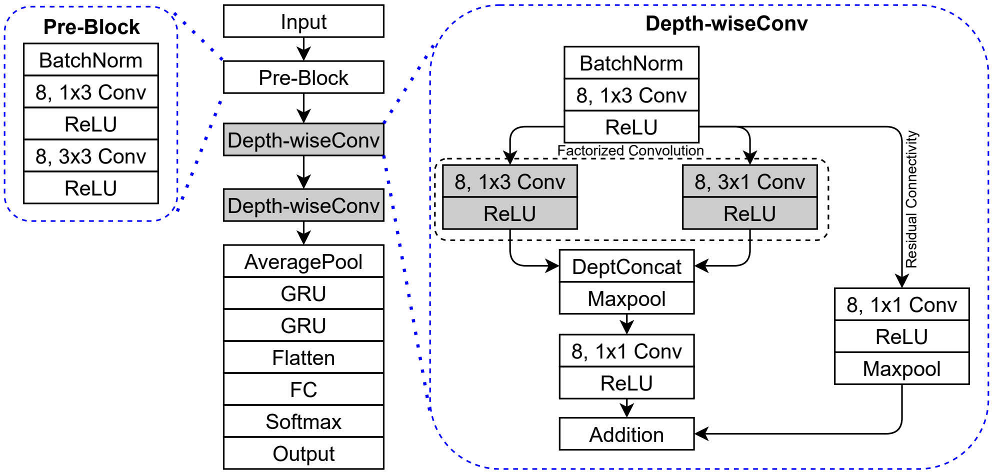
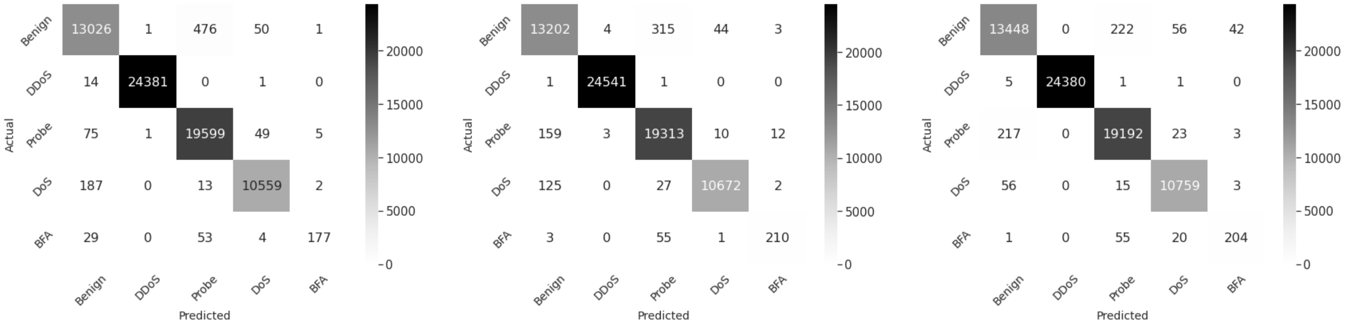


Fig. 2. Lightweight CNN-GRU-based Intrusion Identification Model

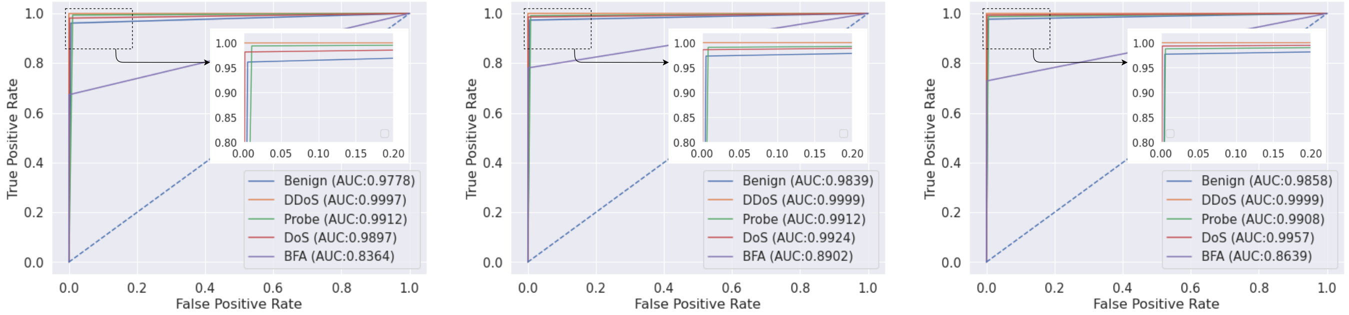
TABLE III
FEATURE SELECTION PERFORMANCE FOR INTRUSION IDENTIFICATION

FS Technique	Cyber Attacks Classification Accuracy					Average Accuracy	Precision	Recall	Loss	Average ROC Score	Time-cost
	Benign	DDoS	Probe	DoS	BFA						
Extra Tree	97.71%	99.99%	97.31%	99.02%	**95.68%**	98.60%	98.62%	98.60%	0.0441	0.9589	0.165 ms
XGBOOST	97.87%	99.97%	97.98%	**99.49%**	92.51%	98.89%	98.92%	98.86%	0.0330	0.9715	0.181 ms
LightGBM	**97.97%**	**100.00%**	**98.50%**	99.08%	80.95%	**98.95%**	**99.00%**	**98.91%**	**0.0318**	**0.9872**	**0.164 ms**



(a) (b) (c)

Fig. 3. Confusion matrix score for some FS techniques: (a) Extra Trees, (b) XGBoost, (c) LightGBM



(a) (b) (c)

Fig. 4. ROC score for some FS techniques: (a) Extra Trees, (b) XGBoost, (c) LightGBM

a lightweight CNN-GRU-based model for intrusion classification. Table II shows the lightGBM FS performance with different numbers of features. We used some selected features such as $10, 15, 20, 25$, and 30 and compared them to find the

TABLE IV
COMPARISON OF INTRUSION IDENTIFICATION WITH DIFFERENT MODELS

Model	Accuracy	Loss	Time-cost	Trainable Parameters
CNN [6]	98.86%	0.0377	0.149 ms	109,437
LSTM [6]	97.64%	0.0532	2.996 ms	55,775
GRU [6]	98.24%	0.0432	3.292 ms	126,623
CNN-LSTM [8]	95.95%	0.1265	0.244 ms	57,798
Proposed Model	**98.95%**	**0.0318**	**0.164 ms**	**5,115**

best result. The proposed model achieved great results with an accuracy of 98.95%, a precision of 99.00%, a recall of 98.91%, a ROC score of 0.9872, a loss of 0.0318, and a computation cost of 0.109 ms when using 30 subset features. Fig. 3 provides the confusion matrices of extra trees, xgboost, and lightGBM techniques. LightGBM FS can classify 13,448 benign, 24,380 DDoS, 19,192 probe, 10,759 DoS, and 204 BFA attack samples from 13,768 benign, 24,387 DDoS, 19,435 probe, 10,833 DoS, and 280 BFA attack testing samples, respectively. Based on these results, the proposed model with lightGBM FS performs superior capabilities to identify cyber-attacks with a high detection rate.

Fig. 4 shows the ROC AUC score for extra trees, xgboost, and lightGBM FS techniques. Combining lightGBM and CNN-GRU-based proposed model outperforms other techniques, with an average ROC AUC score of 0.9672. The ROC AUC scores for each class are 0.9858 for benign, 0.9999 for DDoS, 0.9908 for probe, 0.9957 for DoS, and 0.8639 for BFA attack. Table IV presents the FS performance when using 30 promising selected features. The results show that the lightGBM FS outperforms other ML classifier-based FS techniques (extra-trees and xgboost FS techniques) for intrusion identification tasks. The lightGBM FS technique achieved an accuracy of 97.97% for benign, 100.00% for DDoS, 98.50% for probe, 99.08% for DoS, and 80.95% for BFA attacks, respectively. Table 5 presents a comparison of intrusion identification with different models. The measurement results show that the existing CNN, LSTM, GRU, and CNN-LSTM models achieved an accuracy of 98.86%, 97.64%, 98.24%, and 98.74%, respectively. The proposed model outperforms benchmark models by achieving an accuracy of 98.95%, a loss of 0.0318, and a computation cost of 0.164 ms.

V. CONCLUSION

This study evaluates the lightGBM FS technique to assist with lightweight intrusion identification in SDN-based industrial CPS. The model employed three main modules: pre-block, depth-wiseConv, and stacked GRU. The depth-wiseConv module utilized a residual connection to improve training model performance and resolve the gradient vanishing problem. Furthermore, a factorized convolution architecture was exploited to conduct a lightweight model structure. The proposed model outperforms benchmark models by achieving an accuracy of 98.95%, a loss of 0.0318, and a computation cost of 0.227 ms.

ACKNOWLEDGMENT

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the MSIT (Ministry of Science and ICT) (2018R1A6A1A03024003), Korea and the Grand Information Technology Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation.

REFERENCES

[1] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection," *Wireless communications and mobile computing*, vol. 2021, 2021.

[2] Y.-J. Lin, C.-B. Lan, and C.-Y. Huang, "A Realization of Cyber-Physical Manufacturing Control System Through Industrial Internet of Things," *Procedia manufacturing*, vol. 39, pp. 287–293, 2019.

[3] E. Molina and E. Jacob, "Software-Defined Networking in Cyber-Physical Systems: A Survey," *Computers & electrical engineering*, vol. 66, pp. 407–419, 2018.

[4] A. A. Pranata, T. S. Jun, and D. S. Kim, "Overhead Reduction Scheme for SDN-Based Data Center Networks," *Computer Standards & Interfaces*, vol. 63, pp. 1–15, 2019.

[5] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," *IEEE Access*, vol. 8, pp. 165 263–165 284, 2020.

[6] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," *IEEE Access*, vol. 9, pp. 108 495–108 512, 2021.

[7] M. Meamarian and N. Yazdani, "A Robust, Lightweight Deep Learning Approach for Detection and Mitigation of DDoS Attacks in SDN," in *2022 27th International Computer Conference, Computer Society of Iran (CSICC)*. IEEE, 2022, pp. 1–7.

[8] L. Karanam, K. K. Pattanaik, and R. Aldmour, "Intrusion Detection Mechanism for Large Scale Networks using CNN-LSTM," in *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, 2020, pp. 323–328.

[9] R. Zhao, G. Gui, Z. Xue, J. Yin, T. Ohtsuki, B. Adebisi, and H. Gacanin, "A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things," *IEEE Internet of Things Journal*, 2021.

[10] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An Efficient Deep Learning Model for Intrusion Classification and Prediction in 5G and IoT Networks," in *2019 53rd Annual Conference on information sciences and systems (CISS)*. IEEE, 2019, pp. 1–6.

[11] S. Rani, A. Singh, D. H. Elkamchouchi, I. D. Noya *et al.*, "Lightweight Hybrid Deep Learning Architecture and Model for Security in IIoT," *Applied Sciences*, vol. 12, no. 13, p. 6442, 2022.

[12] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," *IEEE Access*, vol. 7, pp. 42 450–42 471, 2019.

[13] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Efficient Classification of Enciphered SCADA Network Traffic in Smart Factory Using Decision Tree Algorithm," *IEEE Access*, vol. 9, pp. 154 892–154 901, 2021.

[14] P.-C. Nguyen, Q.-T. Nguyen, and K.-H. Le, "An Ensemble Feature Selection Algorithm for Machine Learning based Intrusion Detection System," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*. IEEE, 2021, pp. 50–54.

[15] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. Lee, and D.-S. Kim, "Composite and Efficient DDoS Attack Detection Framework for B5G Networks," *Computer Networks*, vol. 188, p. 107871, 2021.

[16] M. I. Kareem and M. N. Jasim, "DDoS Attack Detection Using Lightweight Partial Decision Tree Algorithm," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*. IEEE, 2022, pp. 362–367.

[17] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks," *IEEE Internet of Things Journal*, 2022.