Deep Learning-Based Anomaly and Intrusion Detection Using the CSE-CIC-IDS2018 Dataset

Al Baraa Bouidaine
STIC Laboratory, Faculty of Technology, Department of Telecommunication, University of Tlemcen, Tlemcen, Algeria
albaraa.bouidaine@univ-tlemcen.dz

Djilali Moussaoui
STIC Laboratory, Faculty of Technology, Department of Telecommunication, University of Tlemcen, Tlemcen, Algeria
djilali.moussaoui@univ-tlemcen.dz

Mourad Hadjila
STIC Laboratory, Faculty of Technology, Department of Telecommunication, University of Tlemcen, Tlemcen, Algeria
mourad.hadjila@univ-tlemcen.dz

Wafaa Ferhi
STIC Laboratory, Faculty of Technology, Department of Telecommunication, University of Tlemcen, Tlemcen, Algeria
wafaa.ferhi@univ-tlemcen.dz

Mohammed Hicham Hachemi
Department of Electronics, Faculty of Electrical Engineering, University of Science and Technology Mohamed Boudiaf, Oran, Algeria
hicham.hachemi@univ-usto.dz (corresponding author)

Received: 27 March 2025 | Revised: 6 May 2025 and 19 May 2025 | Accepted: 21 May 2025

 DOI: https://doi.org/10.48084/etasr.11173

ABSTRACT

Intrusion Detection Systems (IDSs) play a vital role in identifying and mitigating malicious network activities and system misuse. The integration of Artificial Intelligence (AI), particularly Deep Learning (DL), has significantly enhanced the adaptability and efficiency of IDS. This paper proposes an intelligent network-based IDS leveraging a DL model trained on the CSE-CIC-IDS2018 dataset. Key data pre-processing steps included duplicate removal, handling missing values, conversion of categorical data to a numerical form, and feature scaling. Initially, the model aimed to classify all individual attack types alongside benign traffic; however, the frequent misclassification of certain attack types prompted the aggregation of similar attacks into broader categories. This adjustment led to notable improvements in the performance metrics, including accuracy, precision, recall, and F1-score. To mitigate overfitting, weight decay in the context of neural networks, known as L2 weight regularization, was applied. The proposed improved DL model achieved an accuracy of 99.91%, precision of 98.61%, recall of 93.18%, and an F1-score of 94.78%, highlighting both the robustness of DL in intrusion detection and the critical role of comprehensive data preprocessing.

Keywords-network security; IDS; pre-processing; DL; one hot encoding; multi-class classification

I. INTRODUCTION

Traditional security measures, including firewalls, antivirus software, encryption, password protection, and secure network protocols, while useful and necessary, are not always up to date with the constantly evolving nature of cyber threats. Reports from Carnegie Mellon University's Computer Emergency Response Team (CMU's CERT) indicate a sharp rise in cyberattack vulnerabilities [1]. This highlights the need for continuous research and improvement in intrusion detection technologies [2]. Intrusions refer to any unauthorized access that jeopardizes the confidentiality, integrity, availability, or security of network-connected resources [3]. Confidentiality is ensured through cryptographic techniques that limit access to authorized users, while data integrity ensures that information is not altered during transmission, typically verified using digital signatures [4]. A proactive and intelligent approach to combat such vulnerabilities is IDSs. IDSs are designed to promptly and accurately detect threats by identifying abnormal system usage that may exploit vulnerabilities in real-time, a principle shared across all IDS implementations [5-7]. However, developing an effective IDS is challenging, as classifiers must adapt to new attack patterns while avoiding false positives.

Intrusion detection methodologies are typically categorized into Signature-based Detection (SD), Anomaly-based Detection (AD), and Stateful Protocol Analysis (SPA). SD techniques identify known threats by matching data against predefined attack signatures, while AD techniques detect deviations from established behavioral norms using either static or dynamic profiling. SPA techniques monitor protocol compliance by analyzing communication sequences based on formal protocol definitions, such as those specified by the Internet Engineering Task Force (IETF) [8]. The integration of these methodologies alongside Machine Learning (ML) and DL techniques [9] has transformed IDSs, enabling the automatic detection of a wide range of attacks without relying on predefined rules, offering adaptability and effectiveness against evolving threats.

The combination of detection methodologies with ML and DL has been explored. Authors in [10] proposed an anomaly-based intrusion detection method employing Random Forest (RF), Gaussian Naive Bayes (GNB), and Multilayer Perceptron (MLP), enhancing detection accuracy on the CSE-CIC-IDS2018 dataset through rigorous preprocessing and Pearson correlation-based feature selection. Authors in [11] achieved high cyberattack detection accuracy using minimal feature sets, selected via the Artificial Bee Colony (ABC), Flower Pollination Algorithm (FPA), and Ant Colony Optimization (ACO) algorithms, with the best accuracy performance (~99.0%) obtained using ACO. A dense Deep Neural Network (DNN) was proposed in [12] for flow-based intrusion detection, achieving ~90% accuracy on the CSE-CIC-IDS2018 dataset. In [13], a hybrid model combining autoencoders and Long Short-Term Memory (LSTM) networks on the KDDCup99 dataset, improved prediction performance with a 2% increase in accuracy and reduced misclassifications. Authors in [14] presented a taxonomy of DL architectures, benchmarking Feed-forward Neural Networks (FFNN), autoencoders, Deep Belief Networks (DBNs), and LSTMs, identifying supervised FFNN as the most effective. In [15], a comparative study was conducted on botnet attack classification using GNB, K-Nearest Neighbors (KNN), Adaptive Boosting (AB) with Decision Trees (DT), and Support Vector Machines (SVMs), while authors in [16] examined and reviewed prior DBN-based IDS. A detailed taxonomy for integrated IDS frameworks using supervised ML was also proposed in [17], demonstrating a strong classification performance across four benchmark datasets. In [18], dimensionality reduction techniques, including Principal Component Analysis (PCA), autoencoders, and Linear Discriminant Analysis (LDA), were evaluated, showing their impact on classification performance across multiple datasets (UNSW-NB15, ToN-IoT, and CSE-CIC-IDS2018) and DL models. In [19], an LSTM-based IDS attained 99% accuracy on the CSE-CIC-IDS2018 dataset, and in [20], a similar DL-based Network Intrusion Detection System (NIDS) achieved perfect accuracy on CICIDS2018 and 99.64% on Edge Internet of Things (IoT) datasets. The Self-Adaptive Trust-based IDS (SATIDS) presented in [21] utilized enhanced LSTM networks and achieved up to 99.73% accuracy on the ToN-IoT and InSDN datasets. In [22], RF achieved 99.98% accuracy on the MQTT-IoT-IDS2020 dataset, outperforming other ML classifiers, including SVM, k-NN, GNB, DT, and Stochastic Gradient Descent (SGD). Authors in [23] combined MLP with backpropagation and Particle Swarm Optimization (PSO) for cloud-based IDS, reaching 98.97% accuracy on the revised CSE-CIC-IDS2018 dataset. In [24], a hybrid feature selection approach combining Enhanced Feature Selection and Teaching–Learning-Based Optimization (EFS-TLBO) was introduced, using Extreme Learning Machines (ELMs) for improved performance. Finally, authors in [25] proposed a lightweight Convolutional Neural Network (CNN)-LSTM model optimized for IoT environments, like the Raspberry Pi 3, achieving 98.78% accuracy, 98.09% recall, 97.88% precision, and a 97.99% F1-score on the UNSW-NB15 dataset.

This work proposes an FFNN-based IDS, utilizing the CSE-CIC-IDS2018 dataset for training and evaluation. The dataset underwent an extensive preprocessing pipeline to ensure data consistency and quality. A structured methodology was followed, including data preprocessing, model architecture design, training, and performance evaluation. The model and its training parameters were carefully selected to optimize detection accuracy while addressing challenges, such as class imbalance and overlapping attack behaviors.

II. METHODOLOGY

A. Dataset

The CSE-CIC-IDS2018 dataset is a large-scale, real-world network traffic dataset specifically designed for intrusion detection research. It comprises over 16 million instances with 84 features distributed across 14 class labels—one representing normal traffic and 13 corresponding to various attack types. The dataset includes a wide range of cyberattacks, such as Distributed Denial of Service (DDoS), Botnet activity, Brute Force, and Structured Query Language (SQL) Injection attacks, making it a valuable resource for the evaluation of intrusion detection algorithms and cybersecurity solutions [26, 27].

B. Pre-processing

Initially, all 10 individual dataset files were merged into a single unified file to streamline processing. Data type inconsistencies were resolved by standardizing feature formats. Due to file size constraints, a particularly large file was partially excluded—only attack data were retained from it, while a sufficient portion of benign traffic was preserved to maintain class balance. The key preprocessing steps included the removal of missing values, duplicate entries, and irrelevant features (e.g., Timestamp, Flow ID). The categorical variables were transformed into numerical formats using label encoding or one-hot encoding to ensure compatibility with the ML algorithms. Feature normalization was applied using min-max scaling to rescale values within a 0–1 range, thereby improving model convergence and interpretability. Finally, the dataset was partitioned into training, validation, and testing subsets, typically allocating 90% of the data for training, with 10% of them reserved for validation, to ensure effective model learning, minimize overfitting, and enable rigorous evaluation.

C. Model

The model was developed using the Keras Sequential API, which is well-suited for models with a single input-output flow. An FFNN architecture was implemented, comprising six layers: an input layer, four hidden layers with 48, 32, 16, and 16 neurons, respectively, and an output layer with 14 neurons corresponding to the 14 class labels. The Rectified Linear Unit (ReLU) activation function was applied to the hidden layers to introduce non-linearity, while the Softmax function was used in the output layer to support multi-class classification. The model was trained using the Adam optimizer, and categorical cross-entropy was employed as the loss function, appropriate for multi-class classification tasks. To mitigate overfitting, L2 regularization with a lambda value of 0.0001 was incorporated into the model. Training was conducted iteratively to minimize loss and optimize predictive performance on the training data, using a batch size of 2048 for 50 epochs.

III. RESULTS AND ANALYSIS

Figures 1 and 2 illustrate the training accuracy and loss throughout the 50 epochs. The model achieved high accuracy early in the training process, reaching 95% within the first epoch and stabilizing by the fourth, indicating effective learning and convergence without signs of overfitting or underfitting. The corresponding rapid decrease and stabilization in the loss function further confirms the model's ability to learn reliable patterns in the data.

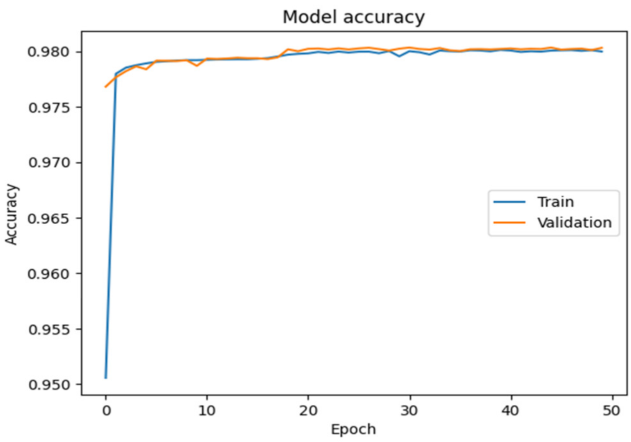

Fig. 1. Training and validation accuracy.

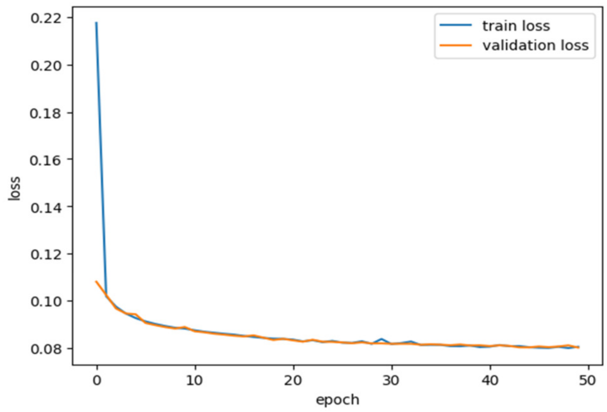

Fig. 2. Training and validation loss.

TABLE I. EVALUATION METRICS FOR EACH CLASS

Attack types	Accuracy	Precision	Recall	F1-score
Benign	0.9993	0.97	1.00	0.99
DDoS attack-HOIC	1.00	1.00	1.00	1.00
DDoS attacks-LOIC-HTTP	0.9982	1.00	1.00	1.00
DoS attacks-Hulk	0.9997	1.00	1.00	1.00
Bot	0.9995	1.00	1.00	1.00
Infilteration	0.0083	0.44	0.01	0.02
SSH-Bruteforce	0.9997	1.00	1.00	1.00
DoS attacks-GoldenEye	0.9939	0.99	0.99	0.99
FTP-BruteForce	1.00	1.00	1.00	1.00
DoS attacks-Slowloris	0.9941	0.95	0.99	0.97
DDoS attack-LOIC-UDP	0.8361	0.80	0.84	0.82
Brute Force-Web	0.2777	0.91	0.28	0.43
Brute Force-XSS	0.5428	1.00	0.54	0.70
SQL Injection	0.00	0.00	0.00	0.00

High Orbit Ion Cannon (HOIC), Low Orbit Ion Cannon (LOIC), Hypertext Transfer Protocol (HTTP), User Datagram Protocol (UDP), Cross-site scripting (XSS)

To evaluate the model's performance, a comprehensive set of metrics was used: accuracy, precision, recall, and F1-score. Table I presents these evaluation metrics for all 14 classes. The model achieves high metrics in several classes (e.g. Bening, DDoS attack-HOIC, SSH-Bruteforce, etc.), but it also underperforms in classes including Infilteration, Brute Force-Web, Brute Force-XSS, and SQL Injection. Table II summarizes the overall model performance. That is, the model achieved 98% accuracy, 86.14% precision, 76.07% recall, and 78.00% F1-score. The discrepancy between high accuracy and lower recall/F1-score indicates a tendency to produce false negatives, potentially missing critical attack classes. This issue was further explored through the confusion matrix (Figure 3), which revealed a frequent misclassification of SQL Injection, Brute Force-XSS, and Brute Force-Web attacks—likely due to their limited representation in the training data. Additionally, although DDoS attack-LOIC-UDP was generally well detected, it exhibited a 30% false positive rate. The Infiltration class, despite having sufficient data, was often misclassified due to its stealthy, human-like behavior designed to evade detection. To address these limitations, it is proposed to eliminate the Infiltration class and consolidate the underrepresented attack types into a single category labeled Other Attacks (OA). This reclassification aims to simplify the classification task, enhance the model's recall, and reduce the confusion between similar low-frequency classes.

TABLE II. GLOBAL EVALUATION METRICS

Accuracy	Precision	Recall	F1-score
98%	86.14%	76.07%	78.00%

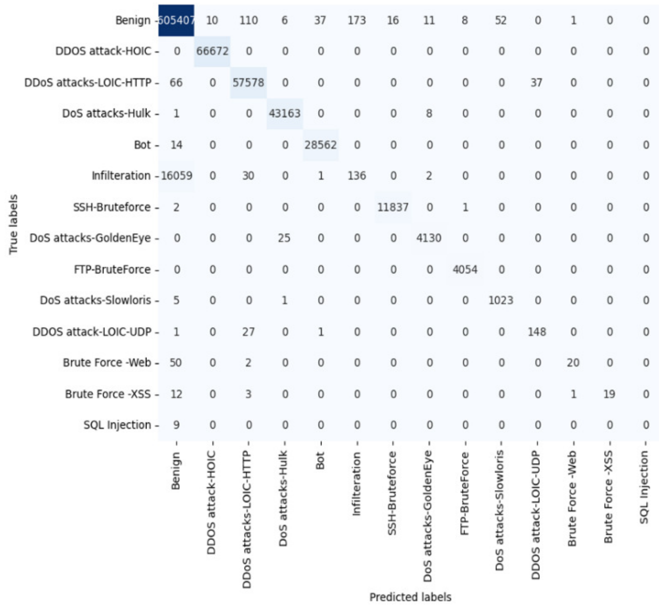

Fig. 3. Confusion matrix multiclass classification.

A. Improved Model

Figures 4 and 5 illustrate the training performance of the improved model in terms of accuracy and loss progression, respectively. Table III presents these evaluation metrics for all classes. The enhanced model achieved 99.91% accuracy, 98.61% precision, 93.18% recall, and an F1-score of 94.78%, mostly improving recall and F1-score compared to the previous version. Nevertheless, the OA class underperforms in terms of accuracy (38.25%), recall (38.26%), and F1-score (54.03%).

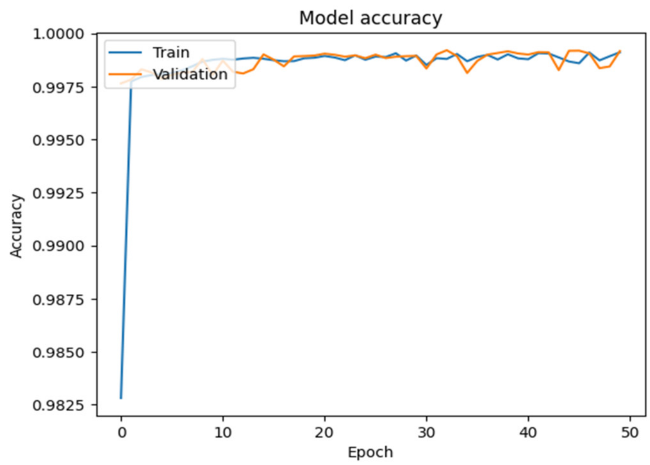

Fig. 4. Training and validation accuracy for the improved model.

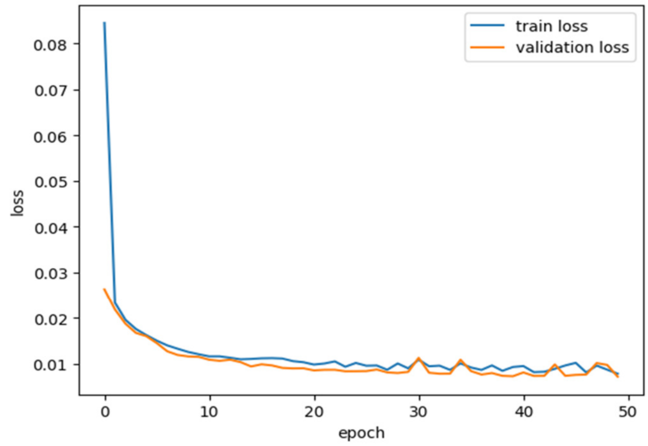

Fig. 5. Training and validation loss for the improved model.

TABLE III. EVALUATION METRICS FOR EACH LABEL (IMPROVED MODEL)

Attack types	Accuracy	Precision	Recall	F1-score
Benign	0.9996	0.9996	0.9996	0.9996
DDoS attack-HOIC	0.9998	1.00	0.9999	0.9999
DDoS attacks-LOIC-HTTP	0.9982	0.9962	0.9982	0.9972
DoS attacks-Hulk	0.9997	0.9960	0.9997	0.9979
Bot	0.9988	0.9991	0.9989	0.9990
SSH-Bruteforce	0.9997	0.9994	0.9997	0.9996
DoS attacks-GoldenEye	0.9595	0.9957	0.9596	0.9773
FTP-BruteForce	1.00	0.9973	1.00	0.9986
DoS attacks-Slowloris	0.9802	0.9586	0.9803	0.9693
OA	0.3825	0.9194	0.3826	0.5403
Overall	**0.9991**	**0.9861**	**0.9318**	**0.9478**

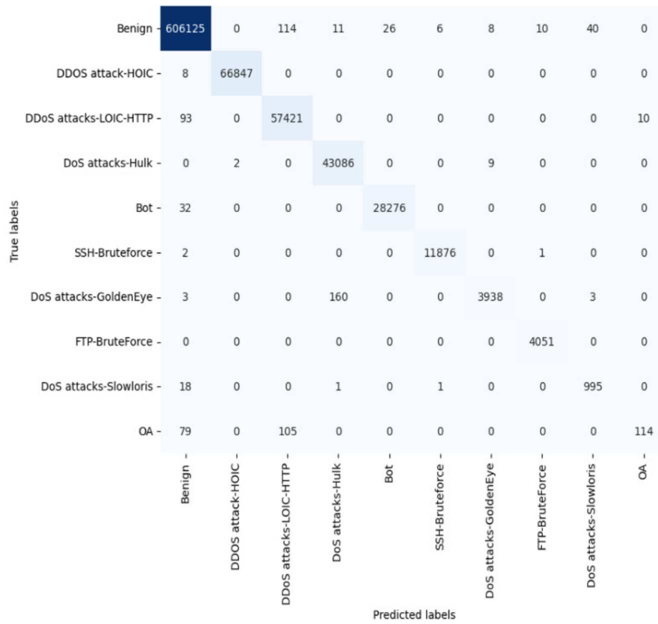

Fig. 6. Confusion matrix multiclass classification for the improved model.

Figure 6 presents the confusion matrix for the improved model. This illustration further validates the success of the model in classifying the majority of the 14 types of cyberattacks, while also misclassifying approximately 2/3 of the OA type attacks as Bening or DDoS attacks-LOIC-HTTP.

Compared to other state-of-the-art methods, the proposed model surpassed the 99% accuracy achieved by the RF-based models reported in [10, 19] and the 98.8% accuracy attained by the ACO-based method described in [11]. This further validates the performance of the proposed model.

IV. CONCLUSION

This study proposed a Deep Learning (DL)-based Intrusion Detection System (IDS) Feed-forward Neural Network (FFNN) model trained on the CSE-CIC-IDS2018 dataset to identify and classify various types of cyberattacks.

The initial evaluations of 14 types of cyberattacks revealed frequent misclassifications among five specific types, including Infiltration, Distributed Denial of Service attack-Low Orbit Ion Cannon-User Datagram Protocol (DDoS attack-LOIC-UDP), Brute Force-Web, Brute Force-Cross-site scripting (XSS), and Structured Query Language (SQL) Injection. To address this, the Infiltration class was excluded, and the other four underrepresented attack categories were merged into a consolidated class labeled Other Attacks (OA). This refinement significantly enhanced classification accuracy and model robustness. The proposed improved model achieved an accuracy of 99.91%, precision of 98.61%, recall of 93.18%, and an F1-score of 94.78%, outperforming several state-of-the-art approaches and demonstrating its effectiveness in detecting a wide range of cyber threats. However, limitations related to class imbalance and insufficient samples for certain attack types persisted, highlighting the need for more diverse and representative datasets.

Future research should explore advanced DL architectures, hybrid models combining traditional and Machine Learning (ML) techniques, and the integration of IDS with complementary cybersecurity tools.

REFERENCES

[1] V. Borhade, A. Nayak, and R. Dakshayani, "Intrusion Detection: A Machine Learning Approach," in *Advanced Computing Technologies and Applications*, Singapore, 2020, pp. 555–561, https://doi.org/10.1007/978-981-15-3242-9_53.

[2] V. Kumar, S. Yadav, V. Kumar, J. Sengupta, R. Tripathi, and S. Tiwari, "Optimal Clustering in Weibull Distributed WSNs Based on Realistic Energy Dissipation Model," in *Progress in Computing, Analytics and Networking*, Singapore, 2018, vol. 710, pp. 61–73, https://doi.org/10.1007/978-981-10-7871-2_7.

[3] M. Abdalla, X. Boyen, C. Chevalier, and D. Pointcheval, "Distributed Public-Key Cryptography from Weak Secrets," in *Public Key Cryptography – PKC 2009*, Berlin, Heidelberg, 2009, vol. 5443, pp. 139–159, https://doi.org/10.1007/978-3-642-00468-1_9.

[4] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, Solan, India, Oct. 2010, pp. 211–216, https://doi.org/10.1109/PDGC.2010.5679895.

[5] D. E. Denning, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987, https://doi.org/10.1109/TSE.1987.232894.

[6] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 517–526, May 2009, https://doi.org/10.1016/j.compeleceng.2008.12.005.

[7] D. Anderson, T. F. Lunt, H. S. Javitz, A. Tamaru, and A. Valdes, "Detecting Unusual Program Behavior Using the Statistical Component of the Next-generation Intrusion Detection Expert System (NIDES) 1," 1997. [Online]. Available: https://api.semanticscholar.org/CorpusID:15146354

[8] H.-J. Liao, C.-H. Richard 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, https://doi.org/10.1016/j.jnca.2012.09.004.

[9] A. H. Sung and S. Mukkamala, "Identifying important features for intrusion detection using support vector machines and neural networks," in *2003 Symposium on Applications and the Internet, 2003. Proceedings*, Orlando, FL, USA, 2003, pp. 209–216, https://doi.org/10.1109/SAINT.2003.1183050.

[10] A. Elhanashi, K. Gasmi, A. Begni, P. Dini, Q. Zheng, and S. Saponara, "Machine Learning Techniques for Anomaly-Based Detection System on CSE-CIC-IDS2018 Dataset," in *Applications in Electronics Pervading Industry, Environment and Society*, vol. 1036, R. Berta and A. De Gloria, Eds. Cham: Springer Nature Switzerland, 2023, pp. 131–140.

[11] H. Najafi Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset," *Applied Sciences*, vol. 14, no. 3, Jan. 2024, Art. no. 1044, https://doi.org/10.3390/app14031044.

[12] R. I. Farhan, A. T. Maolood, and N. F. Hassan, "Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, Dec. 2020, Art. no. 1413, https://doi.org/10.11591/ijeecs.v20.i3.pp1413-1418.

[13] Y. Zhang, Y. Zhang, N. Zhang, and M. Xiao, "A network intrusion detection method based on deep learning with higher accuracy," *Procedia Computer Science*, vol. 174, pp. 50–54, 2020, https://doi.org/10.1016/j.procs.2020.06.055.

[14] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, Nov. 2020, Art no. 102767, https://doi.org/10.1016/j.jnca.2020.102767.

[15] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express*, vol. 7, no. 3, pp. 366–370, Sep. 2021, https://doi.org/10.1016/j.icte.2020.12.004.

[16] I. Sohn, "Deep belief network based intrusion detection techniques: A survey," *Expert Systems with Applications*, vol. 167, Apr. 2021, Art. no. 114170, https://doi.org/10.1016/j.eswa.2020.114170.

[17] E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey," *Procedia Computer Science*, vol. 201, pp. 205–212, 2022, https://doi.org/10.1016/j.procs.2022.03.029.

[18] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digital Communications and Networks*, vol. 10, no. 1, pp. 205–216, Feb. 2024, https://doi.org/10.1016/j.dcan.2022.08.012.

[19] B. I. Farhan and A. D. Jasim, "Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 2, May 2022, Art. no. 1165, https://doi.org/10.11591/ijeecs.v26.i2.pp1165-1172.

[20] V. Hnamte and J. Hussain, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," *Telematics and Informatics Reports*, vol. 10, Jun. 2023, Art. no. 100053, https://doi.org/10.1016/j.teler.2023.100053.

[21] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, Oct. 2023, Art. no. 102211, https://doi.org/10.1016/j.asej.2023.102211.

[22] N. Saran and N. Kesswani, "A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things," *Procedia Computer Science*, vol. 218, pp. 2049–2057, 2023, https://doi.org/10.1016/j.procs.2023.01.181.

[23] S. Alzughaibi 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, Art. no. 2276, https://doi.org/10.3390/app13042276.

[24] D. K. Singh and M. Shrivastava, "Evolutionary Algorithm-based Feature Selection for an Intrusion Detection System," *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7130–7134, Jun. 2021, https://doi.org/10.48084/etasr.4149.

[25] R. H. Altaie and H. K. Hoomod, "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16740–16743, Oct. 2024, https://doi.org/10.48084/etasr.7657.

[26] *A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018).* (2018), Sharafaldin I, A. H. Lashkari Ali A. Ghorbani. [Online]. Available: https://registry.opendata.aws/cse-cic-ids2018.

[27] 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*, Funchal, Madeira, Portugal, 2018, pp. 108–116, https://doi.org/10.5220/0006639801080116.