

Boosting IDS Accuracy with Hybrid LSTM Architectures for IoT Echo Systems

Dr. Anil V Turukmane¹, Mr. M D Ramim Khan² and Mr. Abhishek Chatterjee³

¹⁻³School of Computer Science and Engineering, VIT-AP University, Vijayawada, AP, India

Email: anil.turukmane@vitap.ac.in, Romimkhan5588@gmail.com, Abhishek.chatterjee2005@gmail.com

Abstract—This study delves into an innovative strategy for enhancing the security of the IoT by harnessing the efficacy of LSTM networks, particularly useful for intrusion detection, this kind of (RNN) is skilled at interpreting data over time. The LSTM-based model introduced herein is meticulously crafted to scrutinize patterns in network traffic, aiming to pinpoint malicious activities, which encompass well-established attack signatures as well as emerging, zero-day threats that pose new challenges. By capturing temporal dependencies and long-range correlations present within network data, the LSTM network is adept at differentiating between legitimate and harmful traffic.

In a series of thorough experimental assessments utilizing the CIC-IoT2023 dataset—a rich and diverse benchmark dataset that encapsulates various IoT network traffic scenarios—the model showcased remarkable performance metrics: achieving 98.92% Accuracy, 98.44% Precision, 98.57% Recall, and a 98.47% F1 Score, all derived from an extensive sample size of 90,300 instances. These evaluations reflect the model's capability to accurately categorize network traffic, effectively reduce both false positives and false negatives, and maintain a well-rounded performance across various types of attacks.

This research significantly contributes to the essential domain of IoT security, responding to the pressing demand for adaptable and intelligent methods for detecting attacks that may consistently navigate the constantly evolving landscape of malicious activities targeting interconnected devices. The encouraging results of the LSTM-based methodology set the stage for more resilient and dependable security solutions, ultimately enhancing confidence in IoT technologies and ensuring their continued secure advancement and implementation in an increasingly interconnected environment.

Index Terms— Cyber-security, CIC-IOT 2023, LSTM, Deep learning, IDS, Neural networks.

I. INTRODUCTION

The ever-evolving nature and increasing intricacy of digital assaults demand the development of sophisticated IDS that can effectively recognize malicious activities with precision. Traditional methodologies in IDS often falter when faced with the dynamic characteristics of attack patterns and massive volumes of the data. This situation underscores the urgent necessity for innovative and adaptive solutions to combat such threats. In this research, we explore the potential of deep learning models, particularly focusing on the application of a LSTM neural network to improve the detection capabilities of intrusions while utilizing the CIC 2023 dataset. Due to their special architecture, the LSTM algorithm networks—a variant of (RNNs)—perform exceptionally well while interpreting sequential input.

Their ability to recognize and capitalize on long-term dependencies is exceptional, which positions them as optimal candidates for scrutinizing temporal patterns inherent in network traffic data. By implementing preprocessing techniques and training the LSTM model on the CIC 2023 dataset—an assembly of varied real-world network conditions—our research aspires to achieve outstanding classification efficacy. Through an extensive training regimen and meticulous optimization processes, with an astounding accuracy rate of 98.92%, our LSTM-driven IDS demonstrates its ability to distinguish between safe and dangerous network activity. To strengthen the training procedure for the model, we incorporate critical techniques such as feature normalization, label encoding, and streamlined batch processing. To do an exhaustive assessment of the model's performance, we use evaluation metrics like as precision, recall, F1-score, and confusion matrix construction. This investigation not only highlights the significant promise of LSTM models in the real of cybersecurity but also lays the groundwork for the futuristic integration of deep learning methodologies in developing innovative, adaptable IDS that are able to perform addressing and reducing new risks from the internet.

A. Related to work

[1] This research has devised an innovative IDS for IoT networks, utilizing Denoising Autoencoders (DAEs). The effectiveness of DAEs in real-time identification and prevention of intrusions addresses the constraints present in traditional methodologies within resource-limited IoT settings. Assessment based on standard datasets indicates that the system attained high accuracy levels (up to 99.991%) and demonstrated exceptional performance across critical metrics. This strategy considerably enhances the security of IoT environments by efficiently reducing the risk of unauthorized access and bolstering overall system resilience against advancing cyber threats.

[2] This study unveils a pioneering intrusion detection model tailored to overcome the shortcomings associated with existing techniques, particularly when engaging with small datasets. The model incorporates WGAN-div for data oversampling and InfoGAN for advanced feature extraction, yielding significantly higher rates of accuracy and low false positive occurrences across a variety of datasets. The dual strategy significantly improves the reliability and efficacy of intrusion detection systems, marking a substantial enhancement over conventional methods.

[3] Network-based anomaly detection is vital within the realm of cybersecurity; nevertheless, non-numerical features such as IP addresses and port numbers are frequently underutilized despite their capacity to unveil atypical attack patterns. This study introduces an innovative encoding scheme which ranks non-numerical features based on frequency and maps them onto a normalized scale between 0 and 1, thereby enhancing their interpretable qualities for deep learning models. The implementation of this scheme markedly improves the performance of anomaly detection. For instance, a basic autoencoder achieved an Area Under the Receiver Operating Characteristic (AUROC) score of 0.99 on the CICIDS2017 dataset, surpassing the previous benchmark of 0.91. Experiments conducted with three publicly available datasets validate the effectiveness of the proposed scheme in enhancing detection accuracy.

[4] Network intrusion detection systems (NIDS) powered by artificial intelligence are crucial to the security industry; however, they often encounter challenges in detecting unconventional and polymorphic attacks. This research proposes a novel strategy to augment the detection capabilities of Intrusion Detection Systems (IDS) by generating adversarial polymorphic attacks, assessing their efficacy, and gradually retraining the IDS. This methodology enhances the detection of minority attack samples and ensures that adversarial attacks closely mimic real-world scenarios. Utilizing the CICIDS2017 and CICIoT2023 benchmark datasets, the system exhibited approximately 90% balanced accuracy in identifying dynamic atypical/polymorphic attacks, outperforming pre-existing detection methodologies and class balancing techniques, thereby demonstrating its adaptability and efficacy.

[5] In light of the escalating frequency of cyber-attacks, the protection of sensitive data and the reinforcement of information systems have become paramount. This paper presents an anomaly-based network outlier detection system designed for the efficient classification and mitigation of harmful network traffic. Malicious network outliers are identified and reported for packet blocking, thereby ensuring robust protective measures. The system was optimized through a series of sequential scenarios utilizing the NSL-KDD and CICIDS2017 datasets. Key features were normalized through min-max and z-score methodologies, with selection accomplished via PCA and CFS. Detection models were established using SVM and GNB, with parameter optimization executed via a Genetic Algorithm (GA).

Results indicate that the SVM-based achieved low false alarm rates, shortened detection periods, and high classification accuracy. A comparative evaluation substantiated the proposed system's superiority over existing methodologies, underscoring its efficacy.

II. DATASET OVERVIEW

A. Figures and Tables

The 2023 CIC IoT Dataset has been meticulously crafted to aid in the advancement of security analytics solutions specifically designed for the landscape of the IoT. This comprehensive dataset includes 33 unique types of attacks, conducted across a diverse array of 105 IoT devices, which are organized majorly into seven categories: DDoS, DoS, Recon, web attacks, brute force, spoofing, and mirai-based attacks. Throughout these scenarios, malicious IoT devices target, presenting considerable risks to the systems and networks' availability and integrity. The dataset features an elaborate visualization that emphasizes the occurrence rates of each attack type, conveyed through row counts.

DDoS attacks employ strategies such as flooding and fragmentation, exemplified by UDP and ICMP Floods, while DoS attacks impede access to services by bombarding a singular target. Web-based attacks take advantage of weaknesses in web applications employing methods like SQL -injection and XSS. Brute force attacks seek unauthorized entry through persistent attempts, whereas spoofing attacks manipulate or impersonate entities within the network. Additionally, Mirai-based attacks—like GREIP Flood and UDPPlain—primarily focus on compromising IoT devices. This dataset offers an in-depth view of network traffic features and attack patterns, rendering it an effective source for constructing machine-learning models dedicated to intrusion detection and safeguarding IoT environments. The variety of capabilities offered equips researchers and network security experts with the means to assess network performance and spot irregularities.

For further discussi on or to explore specific applications of this dataset in machine learning models, please contact the authors

III. PROPOSED MODEL FOR DATASET PROCESSING

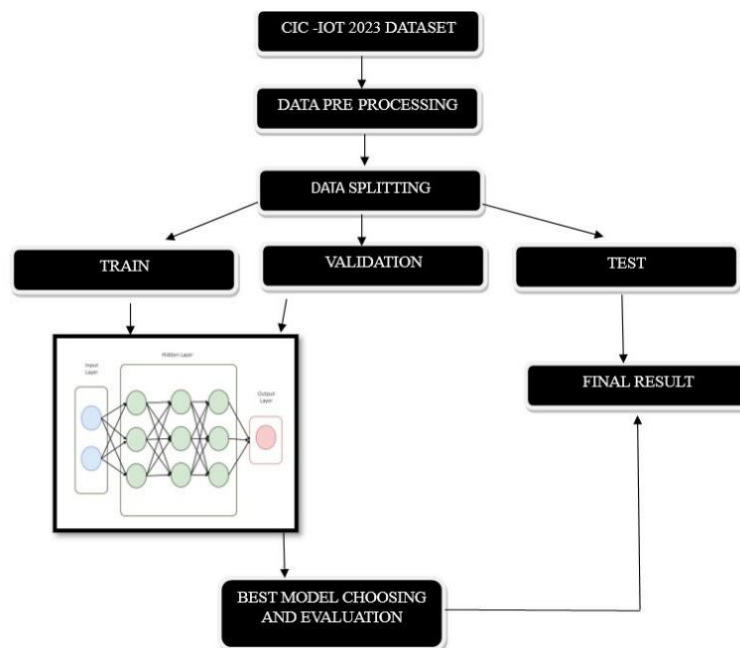


Figure 1

A. Methodology

LSTM

Network with LSTM is exceptionally helpful for processing timeseries data. Both looping feedback and forward-looking connections have been integrated into the LSTM architecture, which enables the model to retain data for extended periods of time. Because of this feature, LSTM may learn from both short-term and long-term dependencies without running the risk of losing important information or become overly crowded. Furthermore, LSTM is intelligent enough to predict future events and remember knowledge from the past. A group of gates, comprising the forget, input, and output gates, are located inside each cell of the LSTM architecture. The mathematical formulations that define the LSTM architecture are presented below.

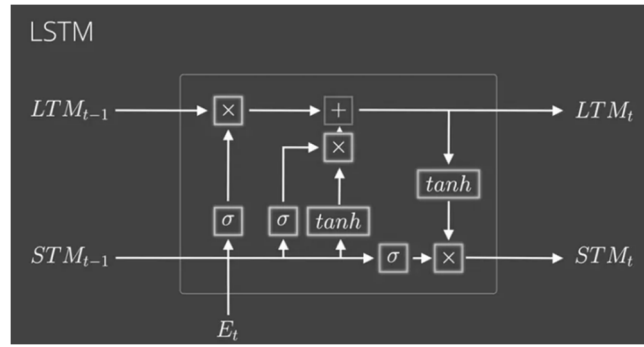


Figure 2

The output produced by the forget gate is represented as F_t , while W_F , U_F , and b_F signify the weights and bias parameters associated with the forget gate. This output corresponds to the forget gate, whereas W_I , U_I , and b_I pertain to the weights and bias of the input gate. Throughout the training process, these weight and bias parameters undergo optimization. The variables x_t and h_t refer to the input vector and hidden vector at time t , respectively.

Here stores the value that is determined by the input and forget gate outputs and stored in the memory cell. The present worth of the value is being discussed. To display the figures neatly, one should position the numbers within parentheses aligned flush to the right side of the column, following the provided format. Initially, utilize the equation editor to formulate the equation. After that, apply the “Equation” markup style to format it appropriately. By pressing the tab key, one can insert the equation number within parentheses. In order to achieve a more condensed representation of your equations, you can incorporate values as needed, where calculations are made for the output and hidden states. The element-wise vector product is shown by the symbol $\odot$.

Each of the four hidden layers in the built LSTM model consists of 64, 64, 128, and 128 neurons.

The activation function for the output layer was SoftMax, while the activation function for the hidden layers was ReLU.

The loss function in fitting model two for categorical data used the binary cross-entropy function for binary data and the categorical cross-entropy function for categorical data.

C. Equations

In the architecture of LSTM cells, weights and biases are associated with each gate, analogous to the framework of neural networks. The ability of the LSTM cell to acquire knowledge is facilitated through the integration of these weight matrices with gradient-based optimization algorithms. The notation used in the preceding equations identifies the weight matrices and biases.

The architecture of the RNN/LSTM network enables it to retain information from previous time intervals and generate predictions for time series, as illustrated in Figure 2. This capability stems from the interconnected nature of the cells within the network, which addresses the vanishing gradient problem effectively through the implementation of the LSTM cell structure. In contrast, earlier RNN models struggled to deliver accurate time-series predictions due to this limitation. To evaluate the model developed in this research for identifying cyber-attacks in IoT environments, we will employ specific valuation metrics using the CIC-IoT2023 Dataset.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1 score} = 2 \times \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Figure 3

IV. RESULT AND DISCUSSION

Accuracy is recorded at an impressive 98.92%. This remarkable figure shows the model's exceptional interpretation in accurately identifying instances across the dataset. The precision, which stands at 98.44%, provides a clear indication of the reliability of positive predictions that the machine learning model has made. High precision signifies that when the model predicts a positive outcome, it is indeed likely to be correct, thereby instilling a sense of confidence in its predictive capabilities. Furthermore, the recall rate of 98.57% highlights the outstanding capability to identify true positives among the total positives available in the dataset. This metric reflects the model's effectiveness in capturing relevant instances, ensuring that very few true positives are overlooked. The F1 Score is an essential metric that balances both precision and recall, achieved a substantial value of 98.47%, reinforcing the model's robust performance across various dimensions. Lastly, the total sample size or support for this evaluation is an impressive 90,300, providing a solid foundation for these results. These comprehensive results collectively demonstrate the efficacy of the model when applied to the CIC-IOT 2023 dataset, which warrants further discussion and in-depth analysis regarding its implications, limitations, and potential applications in real-world scenarios. Such insights are crucial for stakeholders considering the deployment of this model in practical setups.

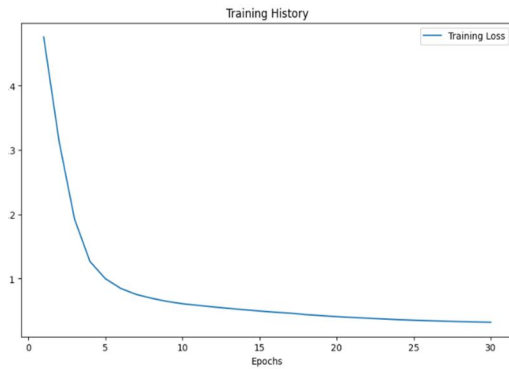


Figure 4

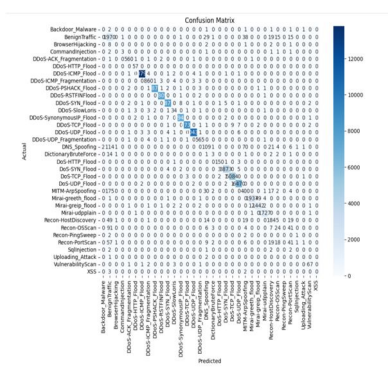


Figure 5

TABLE I

Accuracy	98.92 %
Precision	98.44 %
Recall	98.57 %
F1 Score	98.47 %
Support (Total Sample)	90300

Classification Report:

	precision	recall	f1-score	support
Backdoor_Malware	0.00	0.00	0.00	7
BenignTraffic	0.79	0.94	0.86	2889
BrowserHijacking	0.00	0.00	0.00	14
CommandInjection	0.75	0.33	0.46	9
DDoS-ACK_Fragmentation	0.98	0.99	0.99	567
DDoS-HTTP_Flood	0.89	1.00	0.94	57
DDoS-ICMP_Flood	1.00	1.00	1.00	13886
DDoS-Icmp_Fragmentation	0.98	0.98	0.98	874
DDoS-PSHACK_Flood	1.00	1.00	1.00	7882
DDoS-RSTFINFlood	1.00	1.00	1.00	7813
DDoS-SYN_Flood	1.00	1.00	1.00	7893
DDoS-SlowLoris	0.72	0.72	0.72	47
DDoS-SynonymousIP_Flood	1.00	1.00	1.00	6961
DDoS-TCP_Flood	1.00	1.00	1.00	8755
DDoS-UDP_Flood	1.00	1.00	1.00	18449
DDoS-UDP_Fragmentation	0.97	0.98	0.98	574
DNS_Spoofing	0.53	0.33	0.41	330
DictionaryBruteForce	0.25	0.12	0.16	25
DoS-HTTP_Flood	0.96	0.97	0.96	155
DoS-SYN_Flood	1.00	1.00	1.00	3887
DoS-TCP_Flood	1.00	1.00	1.00	5091
DoS-UDP_Flood	1.00	1.00	1.00	6477
MITH-Arpspoofing	0.74	0.63	0.68	631
MIRAI-greeth_flood	0.99	0.97	0.98	1993
MIRAI-greip_flood	0.97	0.98	0.97	1466
MIRAI-udpplain	0.99	1.00	1.00	1730
Recon-HostDiscovery	0.67	0.63	0.65	292
Recon-OSScan	0.34	0.14	0.19	176
Recon-PingSweep	0.00	0.00	0.00	5
Recon-PortScan	0.31	0.26	0.29	155
SqliInjection	0.00	0.00	0.00	7
Uploading_Attack	0.00	0.00	0.00	3
VulnerabilityScan	0.91	0.89	0.90	75
XSS	0.00	0.00	0.00	5
accuracy			0.99	90300
macro avg	0.70	0.67	0.68	90300
weighted avg	0.98	0.99	0.98	90300

Figure 6

V. CONCLUSION

This research delves deeply into the application of LSTM models a specific kind of RNN that proves particularly effective for analyzing time-series data, to bolster security measures in the IoT. The findings underscore the remarkable capabilities of LSTM models when they are appropriately configured and trained, especially in the domains of anomaly detection and intrusion prevention within IoT settings. With a strong accuracy rate of 98.92%, complemented by a F1 score of 98.47%, a recall of 98.57%, and precision standing at 98.44, the model reveals its dependability and strength. It emerges as an essential tool for tasks requiring precise classification, which are vital for IoT security, such as recognizing harmful traffic patterns and differentiating them from legitimate network activity. Furthermore, the study includes an in-depth examination of the CIC-IoT2023 dataset, a rich and varied collection that encapsulates a wide range of IoT network traffic scenarios, incorporating various attack strategies as well as normal operational behaviors. This dataset is an invaluable asset for future research endeavors in this field, allowing scholars to establish benchmarks and evaluate different techniques for intrusion detection.

The extraordinary performance of the model stands out prominently; however, there remains a pressing need for additional research to bolster its explainability and interpretability. This is especially crucial in scenarios where assessments of the model necessitate a profound understanding and validation of its outputs. To illuminate the model's decision-making journey, methodologies like SHAP values or LIME can be investigated. Moreover, considerations surrounding scalability and efficiency become paramount, particularly in extensive IoT deployments that grapple with resource limitations and substantial data influxes. Future endeavors should aim to broaden the scope and applicability of LSTM models by integrating a variety of data types, inclusive of sensor readings, device logs, and associated metadata. Efforts should also focus on expanding their deployment across different IoT sectors, such as smart homes, industrial control frameworks, and wearable technologies. Delving into optimization methods—including model compression, quantization, and employing hardware acceleration through GPUs or specialized AI processors—is crucial for enhancing model efficiency, minimizing latency, and facilitating real-time intrusion detection capabilities. Collaborating with experts from domains such as healthcare, finance, and NLP could foster the creation of groundbreaking applications and solutions designed to address specific security challenges. The strides made by LSTM-based strategies have notably propelled advancements in IoT security, and this study serves as a significant milestone. It also underscores promising pathways for forthcoming research dedicated to optimizing model efficiency, amplifying interpretability, and streamlining the deployment of resilient and effective intrusion detection systems tailored for the continuously evolving landscape of IoT.

REFERENCES

- [1] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. Iqbal Khan and M. Helal, "Intrusion Detection in IoT Systems Using Denoising Autoencoder," in *IEEE Access*, vol. 12, pp. 122401-122425, 2024, doi: 10.1109/ACCESS.2024.3451726.
- [2] Z. Zhong, C. Xie and X. Tang, "Intrusion Traffic Detection and Classification Based on Unsupervised Learning," in *IEEE Access*, vol. 12, pp. 67860-67879, 2024, doi: 10.1109/ACCESS.2024.3400213.
- [3] M. Kim, W. Jang, J. Hur and M. Yoon, "Relative Frequency-Rank Encoding for Unsupervised Network Anomaly Detection," in *IEEE/ACM Transactions on Networking*, vol. 32, no. 4, pp. 3453-3467, Aug. 2024, doi: 10.1109/TNET.2024.3391396.
- [4] U. Sabeel, S. S. Heydari, K. El-Khatib and K. Elgazzar, "Incremental Adversarial Learning for Polymorphic Attack Detection," in *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 869-887, 2024, doi: 10.1109/TMLCN.2024.3418756.
- [5] O. Alghushairy et al., "An Efficient Support Vector Machine Algorithm Based Network Outlier Detection System," in *IEEE Access*, vol. 12, pp. 24428-24441, 2024, doi: 10.1109/ACCESS.2024.3364400.
- [6] M. S. Powell and B. M. Drozdenco, "SSOLV: Real-Time AI/ML-Based Cybersecurity via Statistical Analysis," in *IEEE Access*, vol. 12, pp. 114786-114794, 2024, doi: 10.1109/ACCESS.2024.3444703.
- [7] A. A. E. -B. Donkol, A. G. Hafez, A. I. Hussein and M. M. Mabrook, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks," in *IEEE Access*, vol. 11, pp. 9469-9482, 2023, doi: 10.1109/ACCESS.2023.3240109.
- [8] H. Elubeyd, D. Yiltas-Kaplan and Ş. Bahtiyar, "A Multi-Modal Deep Transfer Learning Framework for Attack Detection in Software-Defined Networks," in *IEEE Access*, vol. 11, pp. 114128-114145, 2023, doi: 10.1109/ACCESS.2023.3324878.
- [9] A. Balla, M. H. Habaebi, E. A. A. Elsheikh, M. R. Islam, F. E. M. Suliman and S. Mubarak, "Enhanced CNN-LSTM Deep Learning for SCADA IDS Featuring Hurst Parameter Self-Similarity," in *IEEE Access*, vol. 12, pp. 6100-6116, 2024, doi: 10.1109/ACCESS.2024.3350978.

- [10] O. Barut, Y. Luo, P. Li and T. Zhang, "R1DIT: Privacy-Preserving Malware Traffic Classification With Attention-Based Neural Networks," in *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 2071-2085, June 2023, doi: 10.1109/TNSM.2022.3211254.
- [11] X. Wang, Y. Zhang, M. He, S. Guo and L. Yang, "Supervised Representation Learning for Network Traffic With Cluster Compression," in *IEEE Transactions on Sustainable Computing*, vol. 9, no. 1, pp. 1-13, Jan.-Feb. 2024, doi: 10.1109/TSUSC.2023.3292404.
- [12] Z. Wu, H. Zhang, P. Wang and Z. Sun, "RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System," in *IEEE Access*, vol. 10, pp. 64375-64387, 2022, doi: 10.1109/ACCESS.2022.3182333.
- [13] A. Raza, K. Munir, M. S. Almutairi and R. Sehar, "Novel Class Probability Features for Optimizing Network Attack Detection With Machine Learning," in *IEEE Access*, vol. 11, pp. 98685-98694, 2023, doi: 10.1109/ACCESS.2023.3313596.
- [14] A. A. Alhabshy, B. I. Hameed and K. A. Eldahshan, "An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers," in *IEEE Access*, vol. 10, pp. 52724-52743, 2022, doi: 10.1109/ACCESS.2022.3174482.
- [15] C. -S. Shieh, F. -A. Ho, M. -F. Horng, T. -T. Nguyen and P. Chakrabarti, "Open-Set Recognition in Unknown DDoS Attacks Detection With Reciprocal Points Learning," in *IEEE Access*, vol. 12, pp. 56461-56476, 2024, doi: 10.1109/ACCESS.2024.3388149.
- [16] M. S. E. Sayed, N. -A. Le-Khac, M. A. Azer and A. D. Jurcut, "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1862-1880, Dec. 2022, doi: 10.1109/TCCN.2022.3186331.
- [17] H. Ding, Y. Sun, N. Huang, Z. Shen and X. Cui, "TMG-GAN: Generative Adversarial Networks-Based Imbalanced Learning for Network Intrusion Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1156-1167, 2024, doi: 10.1109/TIFS.2023.3331240.
- [18] A. -A. Maiga, E. Ataro and S. Githinji, "Intrusion Detection With Deep Learning Classifiers: A Synergistic Approach of Probabilistic Clustering and Human Expertise to Reduce False Alarms," in *IEEE Access*, vol. 12, pp. 17836-17858, 2024, doi: 10.1109/ACCESS.2024.3359595.