Journal of Applied Informatics and Computing (JAIC)
Vol.8, No.2, December 2024, pp. 235~240
e-ISSN: 2548-6861

DDoS Attacks Detection With Deep Learning Approach Using Convolutional Neural Network

Rafiq Amalul Widodo [1]*, Mera Kartika Delimayanti [2], Asri Wulandari [3]*****
* Program Pascasarjana, Magister Terapan Teknik Elektro, Politeknik Negeri Jakarta
** Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta
*** Jurusan Teknik Elektro, Broadband Multimedia, Politeknik Negeri Jakarta
rafiqamalulwidodo.te23@stu.pnj.ac.id [1], mera.kartika@tik.pnj.ac.id [2], asri.wulandari@elektro.pnj.ac.id [3]

Article Info

Article history:

Received 2024-07-16
Revised 2024-08-08
Accepted 2024-08-09

Keyword:

Convolutional Neural Network,
DDoS attacks,
Deep Learning,
Electric Vehicle.

ABSTRACT

The detection system of DDoS (Distributed Denial-of-Service*)* attacks aims to enhance network security across all facets of internet technology utilization. One is at SPKLU, which stands for Public Electric Vehicle Charging Station. The research employed a deep learning approach utilizing a Convolutional Neural Network (CNN) on a publicly available dataset. Based on our study and analysis, CNN has a precision rate of 95%. Its high accuracy and balanced performance across diverse attack types indicate the model's practical application in real-life situations. The model demonstrates promising performance in detecting different network traffic anomalies, offering significant insight into its potential for practical use. Further investigation is necessary to strengthen the resilience of DDoS assault tactics against emerging dangers and to tackle any potential constraints.

I. INTRODUCTION

DDoS (Distributed Denial-of-Service*)* attacks, which overwhelm systems with malicious traffic and disrupt services for authorized users, present a substantial risk to the security of a network. The service availability can be significantly compromised, resulting in financial losses and a loss of customer trust due to the severity of these attacks[1], [2]. According to recent statistics, DDoS attacks continue to be prevalent, posing a threat despite ongoing mitigation efforts. DDoS attacks can potentially disrupt service operations at public electric vehicle charging stations, resulting in protracted delays and substantial financial repercussions[3]. Due to the critical nature of the authentication systems in these stations, they are ideal targets for such attacks; therefore, robust DDoS detection systems are essential to guarantee the continuous and dependable availability of services.

DDoS attacks can cause severe network security concerns by disrupting internet-based services. The susceptibility of public electric vehicle charging systems to DDoS attacks is effectively underscored by the incorporation of mobile applications for booking, payment, and authentication through these systems. Service failures can occur when the authentication system is compromised, leading to the server being offline and impeding operations at the charging station[3]. In addition to resulting in monetary losses, this undermines user trust in the system. As a result, it is critical to implement a robust DDoS detection system to preserve the integrity of services and avert potential disruptions.

Increasingly, machine learning is being implemented to improve the precision and effectiveness of DDoS attack detection. This research paper employs datasets that simulate DDoS attacks to train machine learning models, thereby enabling the detection of distinct attack patterns. The utilization of machine learning methodologies, including Support Vector Machine (SVM), Naïve Bayes, and Random Forest, has demonstrated potential in delivering attack mitigation insights through prediction[4], [5], [6]. By employing signal processing algorithms such as Fast Fourier Transform (FFT) and Short-Time Fourier Transform (STFT), these methods analyse time and frequency domain characteristics of the assaults with the ability to maintain high levels of accuracy despite the use of limited datasets.

Advancements in machine learning and deep learning have recently been dedicated to developing enhanced techniques for detecting Distributed Denial of Service (DDoS) attacks. A study analysed the efficacy of datasets in detecting DDoS attacks using machine learning algorithms, including Support Vector Machine (SVM), Artificial Neural Networks (ANN), Naive Bayes (NB), Decision Tree (DT), and Reinforcement Classification. The results demonstrated that the KDD99 dataset outperformed the UNBS-NB 15 dataset in accuracy, false positives, and additional metrics[7]. An additional investigation identified DDoS attacks utilizing a deep learning methodology. For DDoS detection, the researchers proposed an innovative method that combined a Stacked Auto Encoder (SAE) and a Convolutional Neural Network (CNN)[8].

Deep learning has significantly advanced in detecting and predicting in many businesses, improving accuracy and resilience compared to conventional approaches. Convolutional Neural Networks (CNN) are highly proficient in recognizing intricate patterns in traffic data[9], [10]. However, Recurrent Neural Networks (RNN)[11] and Long Short-Term Memory (LSTM) networks are effective in analysing sequential data to discover temporal irregularities that indicate assaults. Autoencoders are utilized for anomaly detection by training to compress and rebuild data, emphasising departure from regular flow[12]. Generative Adversarial Networks (GAN) provide artificial data to enhance the training and assessment of detection models[13]. However, there are still obstacles to overcome to achieve immediate identification, the ability to adjust to changing methods of assault and reduce the occurrence of both false positives and false negatives. The current study is centred on improving these models' ability to adapt in real-time, ultimately resulting in more efficient and dependable DDoS detection.

This study constructs a DDoS detection model by utilizing Convolutional Neural Networks (CNN), an extension of prior research. CNNs are highly suitable for processing substantial quantities of numerical data, which are typical of DDoS attack patterns. By utilizing the publicly available CICEV2023 DDoS attack dataset from the Canadian Institute for Cybersecurity, the training data is guaranteed to be adequately annotated and encompass a wide range of attack scenarios[14]. During the data preprocessing phase, feature extraction is performed, and recorded DDoS attack data is converted to numerical formats in preparation for subsequent processing.

II. MATERIAL AND METHOD

This article presents a method for detecting DDoS attacks using a Convolutional Neural Network with deep learning. The suggested model aims to optimize the detection process. The complete process is depicted in Figure 1.

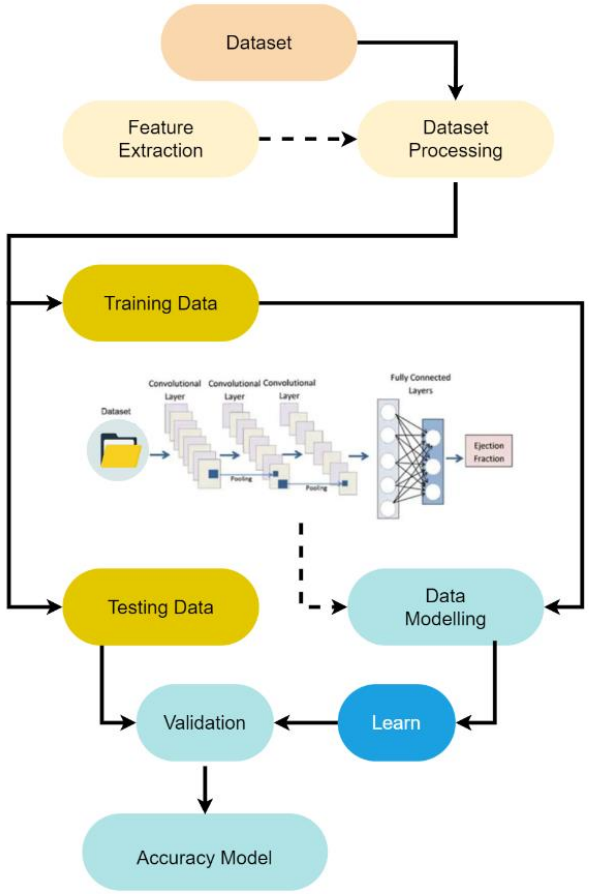

Figure 1. The block diagram of DDoS attacks detection with deep learning approach

A. Dataset

The CICEV2023 dataset, known as the DDoS Attack Dataset, is a comprehensive and reliable resource specifically created to support studies in cybersecurity for electric vehicle (EV) charging infrastructures. The dataset consists of many data points, indicating a large amount of network activity logs. The abstract does not provide an exact count of the data points. However, datasets of this nature generally consist of millions of entries to ensure a thorough depiction of network traffic in both normal and attack scenarios.

The dataset has 384,934 data points, encompassing 33 distinct categories of DDoS attacks on the SPKLU grid system. The dataset has three classes: regular attack, gaussian assault, and standard (genuine users)[14]. A normal class refers to a queue of requests on the server that authorized users execute. The Normal Attack class refers to an unplanned DDoS attack intentionally designed to be easily noticed in the server log or monitoring system. The Gaussian Attack is a well-prepared offensive manoeuvre that poses significant challenges in terms of detection. This attack demonstrates DDoS assailants' utilization of more advanced and intricate tactics. An imbalance was detected in the Gaussian Attack

class within the dataset. The Synthetic Minority Over-Sampling Technique (SMOTE) performs oversampling by introducing fresh samples to the minority class to achieve a more equitable class distribution. This technique facilitates the realistic filling of gaps in unbalanced classes without altering the original class[15].

The dataset consists of many classifications, primarily divided into three classes: normal attack, gaussian assault, and normal. The dataset contains a diverse range of features that are necessary for thorough analysis and training of models. The following characteristics are included:

- Timestamp: Captures the precise timestamp of every network event, which is essential for monitoring traffic patterns and determining the timing of attacks.
- Source IP address is used to identify the origin of network traffic and is helpful in identifying potential sources of malicious activity.
- Destination IP Address refers to the specific location to which the network traffic is being sent. It is used to identify the specific elements of the infrastructure that are being targeted during an attack.
- Port Numbers, for identifying the communication endpoints and services that are the target of attacks, port numbers are crucial, both source and destination.
- Protocol: Specifies the communication protocol employed (e.g., TCP, UDP), offering information about the characteristics of the traffic.
- Payload Information: This consists of the amount of data and the type of content, which is crucial for differentiating between regular and abnormal network traffic.
- Traffic Volume Metrics: Packet rate and byte count are crucial for identifying volumetric attacks.

The CICEV2023 dataset is a highly significant resource for conducting cybersecurity research. It provides a thorough and well-balanced combination of regular and attack traffic and extensive sets of features. This dataset is essential for advancing sophisticated DDoS detection and mitigation methods, which are critical for protecting the integrity and availability of EV charging infrastructures.

B. Dataset Preprocessing

The dataset extracts a unique timestamp parameter. The timestamp is converted to epoch time. Time difference as a feature addition by observing the time difference between rows of data. To determine the time difference between a DDoS attack and regular activity, it is necessary to be aware of the time difference for each line. The feature in question is the duration difference between the first and subsequent lines. The time value in the i th entry of a column with the datetime data type is denoted as T_i. The POSIX time for T_i is represented as $P[8]_i$. The equation that converts datetime to POSIX time is as follows:

$$P_i = POSIX\_Time\ (T_i) \quad (1)$$

$$\Delta T_i = P_i + 1 - P_i \quad (2)$$

$$\Delta T_i = \begin{cases} P_{i+1} - P_i & if\ i < n \\ 0 & if\ i = n \end{cases} \quad (3)$$

Calculating the time difference between lines is obtained by subtracting the time between lines, as shown in equation 3. n represents the total number of rows in the column with a datetime data type. Next, data normalization is performed to obtain consistent data and ensure that features have equal weights in the model.

C. Deep Learning and Convolutional Neural networks

Deep learning is a method that employs artificial neural network layers. This technique applies to scenarios with abundant and intricate data, such as datasets generated in prior research, as deep learning can automatically identify data representations or features. Previous studies have implemented deep learning techniques to detect DDoS attacks. Deep learning is a branch of machine learning that uses artificial neural networks to acquire knowledge from data. It draws inspiration from the organization and operation of the human brain and excels at handling intricate information, such as images, signals, text, and speech[15].

Convolutional Neural Networks (CNNs) are highly suitable for jobs involving image and signal processing, making them highly useful for evaluating patterns in network traffic. The architecture comprises convolutional and pooling layers, which extract features from the data and fully linked layers for classification. Convolutional neural networks (CNNs) can acquire the knowledge necessary to identify specific patterns in network traffic indicative of Distributed Denial of Service (DDoS) attacks[16].

The architecture of CNN consists of several components, namely:

- The network's input layer receives unprocessed network traffic data, which is then subjected to preprocessing to extract pertinent information.
- Convolutional layers utilize convolution procedures to extract distinctive features from the input data. It is possible to stack many convolutional layers to capture more intricate patterns.
- Pooling layers are utilized to decrease the spatial dimensions of feature maps and regulate overfitting.
- Fully connected layers are responsible for classification and providing the probability of a packet being associated with a DDoS assault.

The CNN diagram utilized in this research is illustrated in Figure 2. The CNN architecture consists of 3 CONV1D layers with ReLu activation and MaxPooling1D, followed by 1 Flatten layer, 2 Dropout layers, 1 Dense layer, and 1 Output layer with SoftMax activation. The number of Epochs is set to 25, and batch_size is defined to 32.

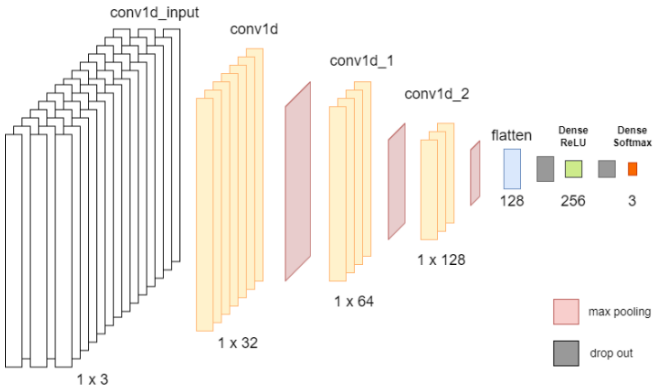

Figure 2. The Illustrated of CNN in this Research

III. RESULT AND DISCUSSION

This study examines many attacks, including advanced DDoS attacks like the "Gaussian Attack" and standard DDoS attacks. Identifying sophisticated attacks is difficult since they are complicated and resemble normal network activity. The model's capacity to attain high precision and recall for these intricate attacks underscores its resilience and efficacy. The Rectified Linear Unit (ReLU) function is employed as the activation function for both the convolutional and fully connected layers, while SoftMax is utilized for the outer layer. After conducting 25 epochs of training using the dataset, the model achieved an accuracy rate of 95%. The outcomes of the CNN model may be observed in below which provide a comprehensive breakdown of the output for each epoch. Figure 3 shown the model train and test accuracy performance and Figure 4 show train and test loss performance.

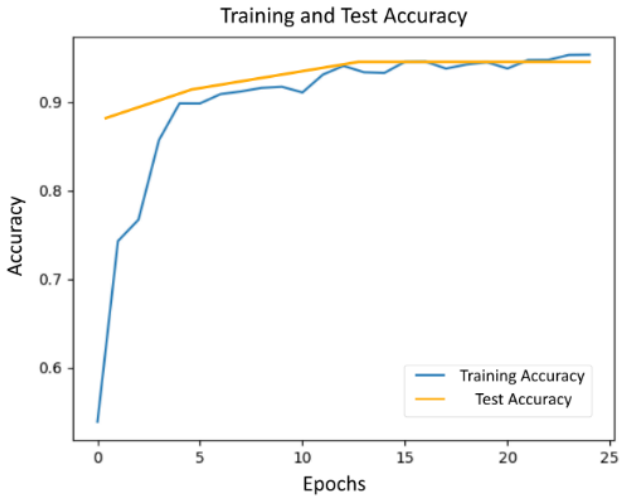

Figure 3. CNN train and test accuracy

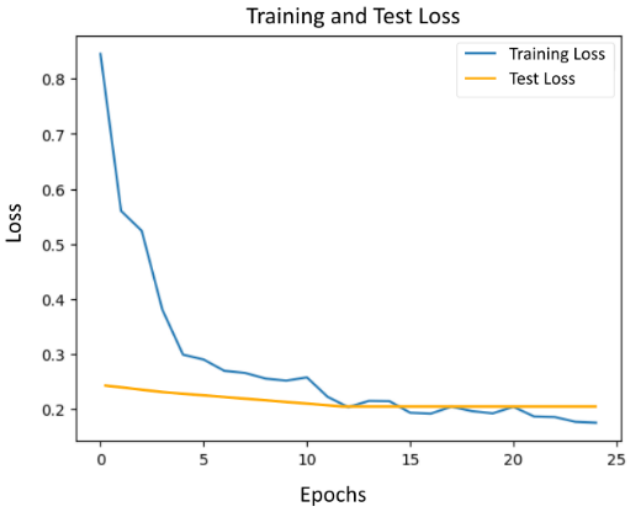

Figure 4. CNN training and test loss

Figure 5 indicates that the model effectively distinguishes between normal and sophisticated DDoS. It is also good at classifying normal traffic. The confusion matrix provides a detailed, comprehensive performance analysis of the CNN model. It demonstrates that 63,549 sophisticated DDoS attacks were correctly identified. However, there were 2,034 instances where normal DDoS attacks were incorrectly labelled as sophisticated DDoS attacks.

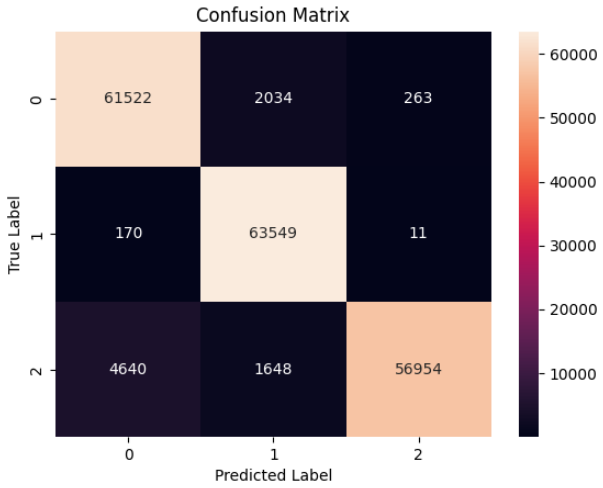

Figure 5. Confusion matrix of CNN model

Furthermore, the model misclassified 170 instances of sophisticated DDoS attacks as normal ones. On a positive note, the model accurately identified 56,954 cases of normal traffic and classified them as legitimate users. An F1-score of 0.95 in the current table indicates a good balance of precision and recall for this class. Given its high precision value of 0.95 and perfect recall value of 1.00, the "Gaussian Attack" class accurately identifies sophisticated DDoS attacks. The model can identify and classify sophisticated and intricate DDoS

attacks accurately included in the dataset. The F1-score is 0.97. Meanwhile, in the "Normal" class, the precision is perfect with a value of 1.00, meaning that all traffic estimates given by authorized users are right according to the model. However, the recall is somewhat lower at 0.90, resulting in an F1-score of 0.95.

TABLE 1
MATRIX EVALUATION

Class	Precision	Recall	F1-score
Normal Attack	0.93	0.96	0.95
Gaussian Attack	0.95	1.00	0.97
Normal	1.00	0.90	0.95

An F1-score of 0.95 in Table 1 indicates a favourable balance of precision and recall for this class. Given its high precision value of 0.95 and perfect recall value of 1.00, the "Gaussian Attack" class accurately identifies sophisticated DDoS attacks. The model can identify and classify sophisticated and intricate DDoS attacks accurately included in the dataset. The F1-score is 0.97. Meanwhile, in the "Normal" class, the precision is perfect with a value of 1.00, meaning that all traffic estimates given by authorized users are right according to the model. However, the recall is somewhat lower at 0.90, resulting in an F1-score of 0.95. The results of our study were the most excellent among the previous ones, as evidenced by Table 2. Research findings indicate that the CNN deep learning technique is capable of accurately identifying DDoS attacks based on their category classification. The SMOTE approach has been utilized to address unbalanced data. The accuracy results have demonstrated a substantial improvement compared to earlier research findings using the similar dataset[8], [9], [14], [16].

The outcomes of this Convolutional Neural Network (CNN) model demonstrate substantial enhancements compared to prior studies that utilized the identical dataset, principally attributable to the implementation of the Synthetic Minority Over-sampling Technique (SMOTE) to address the issue of imbalanced data. This approach guarantees that the model is trained on a dataset with an equal distribution of different classes, resulting in more dependable and precise predictions[15]. Compared to conventional approaches like SVM or decision trees, CNNs utilize the advanced capabilities of deep learning to extract features from the data automatically[8], [16]. This results in higher performance in complicated classification problems, such as DDoS attack detection.

Integrating this Convolutional Neural Network (CNN) model into practical infrastructure, like Electric Vehicle (EV) charging systems, can significantly improve cybersecurity protocols. Electric vehicle charging systems are susceptible to Distributed Denial of Service (DDoS) attacks, which can disrupt services and jeopardize the security of user data. By integrating this model, the system can consistently monitor network traffic, detect potential Distributed Denial of Service (DDoS) assaults in real time, and implement proactive actions to minimize their impact[3].

TABLE 2
THE COMPARISON OF RESEARCH FINDINGS

Method	Precision (Normal)	Recall (Normal)	F1-score (Normal)	Precission (Gaussian Attack)	Recall (Gaussian Attack)	F1-score (Gaussian Attack)
Current CNN Model	**1.00**	**0.90**	**0.95**	**0.95**	**1.00**	**0.97**
Shurman et al. [1]	0.92	0.87	0.89	0.93	0.88	0.90
Al-Shareeda et al. [2]	0.91	0.85	0.88	0.90	0.86	0.88
Khupiran et al. [4]	0.94	0.89	0.91	0.92	0.87	0.89
Kumari and Mrunalini [5]	0.90	0.86	0.88	0.91	0.85	0.88
Alzahrini and Alzahrini [6]	0.93	0.88	0.90	0.94	0.89	0.91
Wani et al. [7]	0.92	0.86	0.89	0.93	0.88	0.90
Tekleselassie [8]	0.94	0.88	0.91	0.95	0.90	0.92
Cil et al. [9]	0.93	0.87	0.90	0.94	0.89	0.91
Shaaban et al. [16]	0.95	0.89	0.92	0.96	0.91	0.93

IV. CONCLUSION

This study illustrates the successful use of CNNs in identifying DDoS assaults against the grid system in EV charging stations, underscoring their potential to improve cybersecurity in this critical infrastructure. Our research and analysis indicated that CNN achieved an accuracy rate of 95%. Its high accuracy and balanced performance across various attack types indicate the model's practical applicability in real-world scenarios. The model also exhibits optimistic performance in identifying various network traffic anomalies, providing valuable insight into its potential for real-world applications. The CNN model's exceptional success in identifying DDoS attacks, as demonstrated by its high accuracy, precision, recall, and F1 score, underscores its

potential for practical implementation in enhancing cybersecurity. The following studies should prioritize the enhancement of the model, the investigation of supplementary deep learning methods, and the execution of comprehensive real-world trials to guarantee its resilience and dependability in diverse network settings. Future research is required to enhance the robustness of DDoS attack strategies against evolving threats and to address potential limitations.

ACKNOWLEDGMENT

We would like to express our highest gratitude to Ministry of Education, Culture, Research, and Technology for supporting this research through Penelitian Tesis Magister 2024 Schema.

REFERENCES

[1] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," *Int. Arab J. Inf. Technol.*, vol. 17, no. 4A, pp. 655–661, Jul. 2020, doi: 10.34028/iajit/17/4A/10.

[2] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bull. Electr. Eng. Inform.*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[3] G. Lee, T. Lee, Z. Low, S. H. Low, and C. Ortega, "Adaptive Charging Network For Electric Vehicles," 2016.

[4] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa, and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, Chiang Mai, Thailand: IEEE, Nov. 2018, pp. 1–4. doi: 10.1109/ICSEC.2018.8712757.

[5] K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," *J. Big Data*, vol. 9, no. 1, p. 56, Dec. 2022, doi: 10.1186/s40537-022-00616-0.

[6] R. J. Alzahrani and A. Alzahrani, "Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic," *Electronics*, vol. 10, no. 23, p. 2919, Nov. 2021, doi: 10.3390/electronics10232919.

[7] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Dubai, United Arab Emirates: IEEE, Feb. 2019, pp. 870–875. doi: 10.1109/AICAI.2019.8701238.

[8] H. Tekleselassie, "A Deep Learning Approach for DDoS Attack Detection Using Supervised Learning," *MATEC Web Conf.*, vol. 348, p. 01012, 2021, doi: 10.1051/matecconf/202134801012.

[9] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Syst. Appl.*, vol. 169, p. 114520, May 2021, doi: 10.1016/j.eswa.2020.114520.

[10] M. K. Delimayanti, A. Mardiyono, B. Warsuta, and E. S. Puspitaningrum, "Implementation of Convolutional Neural Network for COVID19 Screening using X-Rays Images." Accessed: Sep. 14, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10127845

[11] Koneru Lakshmaiah Education Foundation *et al.*, "The Prediction of Diseases using Rough Set Theory with Recurrent Neural Network in Big Data Analytics," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 5, pp. 10–18, Oct. 2020, doi: 10.22266/ijies2020.1031.02.

[12] R. F. Naryanto, M. K. Delimayanti, A. Naryaningsih, B. Warsuta, R. Adi, and B. A. Setiawan, "Diesel Engine Fault Detection using Deep Learning Based on LSTM," in *2023 7th International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM)*, Medan, Indonesia: IEEE, Dec. 2023, pp. 37–42. doi: 10.1109/ELTICOM61905.2023.10443110.

[13] Z. Zhai, "Auto-encoder generative adversarial networks," *J. Intell. Fuzzy Syst.*, vol. 35, no. 3, pp. 3043–3049, Oct. 2018, doi: 10.3233/JIFS-169659.

[14] Y. Kim, S. Hakak, and A. Ghorbani, "DDoS Attack Dataset (CICEV2023) against EV Authentication in Charging Infrastructure," in *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, Aug. 2023, pp. 1–9. doi: 10.1109/PST58708.2023.10320202.

[15] F. Setiawan and C.-W. Lin, "A Deep Learning Framework for Automatic Sleep Apnea Classification Based on Empirical Mode Decomposition Derived from Single-Lead Electrocardiogram," *Life*, vol. 12, no. 10, p. 1509, Sep. 2022, doi: 10.3390/life12101509.

[16] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo, Egypt: IEEE, Dec. 2019, pp. 233–238. doi: 10.1109/ICICIS46948.2019.9014826.