Enhancing DNP3 Security Using CNN Deep Learning Techniques

Amenah A. Jasim [1], Khattab M. Ali Alheeti [1,*]

[1]College of Computer and Information Technology, Computer Science Department, University of Anbar, Ramadi, Iraq

Email: ami21c1009@uoanbar.edu.iq; co.khattab.alheeti@uoanbar.edu.iq

Abstract

Industrial Automation and Control Systems (IACS) are necessary for enabling secure information exchange between smart devices; ensuring security in Industrial Control Systems (ICS) is of importance due to the presence of these devices at distant locations and their control over vital plant activities. Intelligent devices and hosts use protocols such as Modbus, DNP3, IEC 60870, IEC 61850, and others. This paper focuses on the analysis and development of techniques for detecting of network traffic within the industrial environment, more specifically anomalies in the application ZZZAlayer in the to the protocol called Distribution Network Protocol (DNP3) is an open-source protocol used in Supervisory Control and Data Acquisition (SCADA) systems and widely recognized as the standard for the water, sewage, and oil and gas industries. it is used in the realm of industrial automation; they are critical facilities for the population and must be secured against any security breaches. One of the main objectives of cyber attackers is related with these systems. In This paper presents an architecture that, classification system by Deep Learning algorithm with (CNN). The proposed model was evaluated using standard Intrusion Detection Dataset for DNP3, with 7326) and 86field. The CNN algorithm obtained the best results accuracy

Keywords: Cyberattack, DNP3; ICS; Intrusion Detection; SCADA; Convolutional Neural Network (CNN); Deep Learning (DL)

1. Introduction

Securing industrial control systems (ICS) and Internet of Things (IoT) devices is essential to prevent cyber threats and ensure the reliability and safety of critical infrastructure. With recent developments in power grid systems connected to the Internet and data sharing, it opens the door for attackers to commit malicious attacks based on vulnerabilities in industrial control systems. Nowadays, most substations are controlled by a Supervisory Control and Data Acquisition (SCADA) system that is responsible for controlling the status of the substation and collecting information about sensors or actuators [1],[2]. Communication between these entities is through a network protocol called Distributed Network Protocol (DNP3), which has some security vulnerabilities. One of the most important solutions. Using an intrusion detection system, which is considered the second line of defense in addition to the firewall. It collects and examines data from a wide range of sources within the computer or network in order to detect intrusions that include both (attacks from the outside) and misuse (attacks from within). The term "Intrusion Detection System" (IDS) refers to a system that monitors network traffic and classifies it into "normal" and "abnormal" categories to detect any potential threats to data integrity [3],[4]. A vulnerability assessment, which is created to evaluate the integrity of a computer system or network, is used in the IDS.[5] [6]. It is widely agreed that data is the most important part. However, there has always been a constant external threat to data. Every day, hackers invent new methods to compromise and steal vital information on which all industrial systems depend [3],[4]. As a result, several initiatives have been proposed and studied in the academic, industrial and international communities that set standards to enhance the cybersecurity of SCADA and ICS in general. Security monitoring in the form of intrusion detection systems (IDS) is one viable strategy for cybersecurity [7]. However, IDS solutions still face issues with false alarms and low detection rates. In recent years, artificial intelligence has seen widespread application in classification and pattern recognition. The main objective of this paper is to develop a

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

CNN-based deep learning model over the DNP3 protocol to classify network traffic and identify potential attacks. Hence, the model conclusion and possible changes to improve the proposed model to ensure security. [8],[9] .This paper's remaining sections are structured as follows: Section II presents related work addressing the problem statement, while Section III details the intrusion detection system. Section IV provides an overview of the proposed intrusion detection system's framework as well as the dataset that will be used for testing. The experiment and preliminary data processing. In Section V we saw classification models, confusion matrix. Next, the model analysis and outcomes are presented in Section VI. Future directions are discussed at the end of the paper.

2. Related Work

This section presents research on intrusion detection from earlier studies, which is relevant to and close to the topic of this paper:

According K. Huang et. al. [10] an intrusion detection system was presented based on the deep learning method (CNN) model using the NSL-KDD data transformation method, and the performance of the CNN. The results showed that the CNN model is sensitive to the transformation of attack data images. It can be used to detect intrusion better than most standard classifiers, although CNN has not quite improved the state of the art.

J. Chine et al. [11] In this study, it is proposed, for the first time, to classify SCADA attacks into temporally linked and unrelated attacks using FNN and LSTM deep learning algorithms. Through, we apply to 10% of the KDD99 dataset in this experiment. Firstly, the KDD99 dataset is organized into three useful groups. In detecting unrelated and linked attacks, the superiority of LSTM in detecting linked attacks was demonstrated, detecting all types of SCADA attacks with high degrees, regardless of the temporal correlations between data packets.

P. Sun et al. [12] Proposing the development of a DL-IDS system, which utilises a hybrid network consisting of a convolutional neural network (CNN) and a long short-term memory (LSTM) network. This system aims to extract both spatial and temporal information from network traffic data. The model underwent testing on the CICIDS2017 dataset, achieving an accuracy of 98.67%. At last. In order to enhance the resilience of the model, the class weight optimization approach may be used to mitigate the influence of an uneven distribution of attack types in the training samples, which may adversely affect the model's performance.

S. Diaba et al. [13] proposed a hybrid deep learning algorithm Convolutional Neural Network algorithm; simulations were done using the Canadian Institute of Cybersecurity Standard CICIDS-2017 dataset specifically. According to the simulation results, the proposed algorithm outperforms the current intrusion detection algorithm, with an overall accuracy rate of 97.7%. However, the proposal focuses on distributed denial of service attacks on the communication infrastructure of the smart grid.

3. Literature Survey

Defines intrusion detection systems as the process of monitoring host system or network activity and analyzing it for indicators of intrusion. Whenever AN ID detects a potential threat to the network's or host system's security, it alerts the administrator immediately. Aderson has been conducting IDS research since the 1980s. In order to perform system behavior analysis, IDSs typically require anomaly and attack data sets for training and validation [14],[15]. IDS is divided into anomaly and misuse detection. Anomaly detection finds unusual data patterns, while misuse detection tracks traffic with precise descriptions. Both methods have drawbacks, such as the need for performance updates and the difficulty of creating signatures for unexpected attacks. Clustering and classification are common IDS methods. Clustering group’s unlabelled data patterns to identify anomalous invasions unsupervised. Classification, on the other hand, uses clustering results to distinguish malicious from benign traffic. Deep learning methods convert lower-level features into higher-level ones to learn feature hierarchies. These techniques can learn features independently at multiple abstraction levels without expert customization. From raw data, they can find complex functions that map input to output. Since data volume increased, understanding complex properties became crucial. Feature engineering or feature extraction transforms unprocessed data into features that better represent the problem and improve model accuracy on undiscovered data. Recent studies have shown that deep learning can detect and prevent malicious traffic by extracting features from unprocessed data.[16],[17]

4. Intrusion Detection Model Framework

Figure 1 shows the schematic representation of the proposed system is a network intrusion detection framework based on convolutional neural network algorithm used in this paper. It can be seen that the framework mainly consists of four steps:

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

Step1: Download, compile, and read the collection: The dataset used here, the standard DNP3 ID datasets, contains normal and abnormal DNP3 traffic patterns. Each CNN algorithm will be trained to identify patterns in network traffic using this data set as its basis

Step2: Data pre-processing: It mainly converts symbolic data into numerical data, and then, clean, and prepare the data for training. Convert the DNP3 traffic into a format suitable for input into the CNN. Details are given section IV

Step3: Training, feature extraction and classification: Use the selected training dataset to train the proposed model, which includes a CNN algorithm, and Python programming will be used for pre-processing. In addition, splitting the data into a training and test set to classify the DNP3 dataset, normal and anomalous traffic flows will be combined to train the network to distinguish between the two.

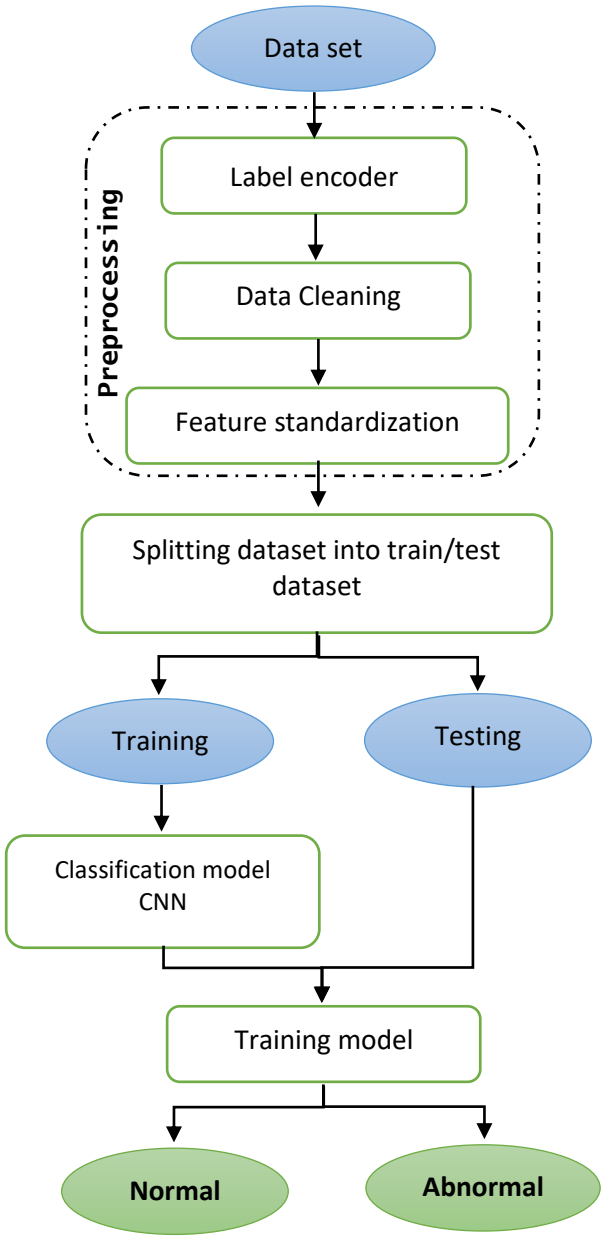

Figure 1. Main Architecture of the Proposed System

Step4: classification: Use the SoftMax classifier to classify and get the classification result.

Step5: Evaluation: Performance is measured using the 'accuracy' metric.

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

We built a powerful convolutional neural network to differentiate between abnormal and harmful activities. There are three discrete levels beneath. There are convolutional layers and pooling layers in each hidden layer. The number of convolution kernels is different for each hidden layer. The greater the variety of kernels used after convolution, the by mapping the original features into high-dimensional space with a larger number of convolution kernels, feature learning is improved.

5. Methodology

A. Dataset Used

A sufficient quantity of high-quality datasets is needed for IDS implementation in order to train and test the algorithm in a real-time setting. The current paper uses the standard DNP3 ID data set source from IEEE for training and testing. Nine DNP3 cyberattacks are included in the dataset's labelled DNP3 flow statistics (Excel format). The targets of these cyberattacks are Denial of Service (DoS) and DNP3 unauthorized commands. About 70% of the total dataset is set aside expressly for training, with the remaining 30% going toward testing and validation. Each record in the DNP3 ID dataset contains 86 attributes representing various features along with a label designating whether the traffic is malicious or not.

Table1: Displays a portion of the features used in the dataset

Feature	Description
Flow ID	ID of the flow
Src IP	Source IP address
Src Port	Source TCP/UDP port
Dst IP	Destination IP address
Dst Port	Destination TCP/UDP port
Protocol	The protocol related to the corresponding flow
Timestamp	Flow timestamp
Flow Duration	Duration of the flow in Microsecond
Tot Fwd Pkts	Total packets in the forward direction
Tot Bwd Pkts	Total packets in the backward direction
TotLen Fwd	Total size of packets in forward direction
TotLen Bwd Pkts	Total size of packets in backward direction
Fwd Pkt Len Max	Maximum size of packet in forward direction
Fwd Pkt Len Min	Minimum size of packet in forward direction
Fwd Pkt Len Mean	Mean size of packet in forward direction

B. Data Pre-processing

The dataset is pre-processed using four phases: Label encoder, Data Cleaning, Features Selection and Features standardization, Figure 1 depicts the proposed system simplified. Start by downloading the DNP3 ID dataset from this IEEE data resource. We then pre-process the data to avoid errors like missing or empty values. Using median, addition, transforming equally to the model. Common methods include Min-Max scaling and Z-score normalization. Finally, normalization and standardization data to ensure that features have similar metrics.

C. Feature Selection Phase

Data preparation phase to train the model numerical data is selected, and the variables (features) and target (label) that the model will learn are selected. The two steps help prepare the data for the training process and confirm that the model is learning correctly from the available data. In this step, `select_dtypes` is used to select columns in the data frame that contain numeric data types.

6. Model Design

A. Architecture of Convolutional Neural Network

This subsection explains in detail the current Convolutional Neural Network (CNN) model, which is used to classify records as normal classes and attack classes such as MITM, STOP_APP, and DNP3_INFO. The rules created and used as knowledge in the CNN to train the model are what determine the classification accuracy [18],[19].

Figure 2 depicts the basic design of a CNN. Here, we use the widely used DNP3 intrusion dataset as input for the training process of a convolutional neural network (CNN). The main goal of the proposed system is to detect malware for DNP3 streams, so that industrial devices can communicate securely and reliably with each other.

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

There are three stages of system startup: data collection and processing, training, and testing. The architecture of the proposed system is part of a neural network classification model using one-dimensional (1D) artificial neural layers [20]. The model is based on iterative computation and previous flows to process string data. All necessary modules (TensorFlow's Keras API) are used. The proposed CNN model includes the following layers:

Step1: we created a sequential model that is a linear combination of layers where we added a 1D convolutional layer with 32 filters, kernel size 3, and ReLU activation. Convolutional layers are typically used to process network-like data, such as time series data.

Step2: ◌Added MaxPooling1D (a one-dimensional pooling layer with a maximum pooling size of 2), which reduces the spatial dimensionality of the input volume.

Step3: flatten the outputs of convolutional layers. The "Flatten" layer is used to flatten the output of the previous layer. It transforms the data into a one-dimensional array, which is required before passing it to a fully connected (dense) layer.

Step4: A dense layer with 11 units (assuming it is a classification problem with 11 classes) and an activation function (SoftMax). It is commonly used in classification problems where it outputs the probabilities for each class and clusters the model.

Finally, compiling model, refine, and train the model using the “fitting” method.

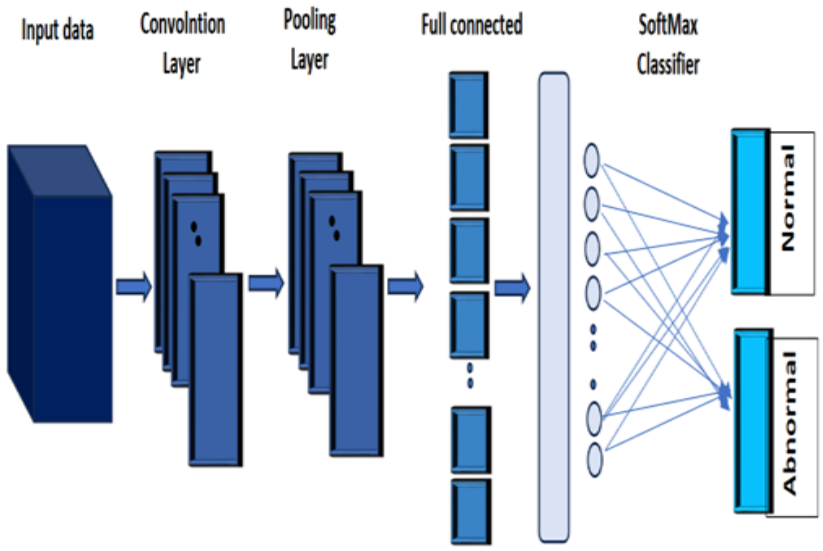

Figure 2. CNN Architecture

B. Performance Metrics

Since detecting malicious DNP3 flows is the main goal of the proposed system, we decided to put it to use in the gateways of industrial control gadgets. The security system can distinguish between two types of behaviour thanks to the intrusion detection system (IDS): normal and abnormal/malicious. We must compute four metrics in order to assess and gauge the effectiveness of IDSs: True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). The following formula should be used to determine the system result's accuracy [21],[22],[23]. Table II shows the structure of confusion matrix.[24],[25],[26].

Table 2: Shows the structure of confusion matrix

Predicted class	Actual class	
	Normal	Attack
Normal	True Negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

i. True Positive (TP): The classifier correctly identified the data instances as attacks.

ii. False Negative (FN): Incorrectly identified as Normal instances in the data.

iii. False Positive (FP): The classifier correctly identified the data instances as attacks.

iv. True Negative (TN): Incorrectly identified as Normal instances in the data.

Evaluation metrics like the one accuracy, recall, and precision are calculated based on these terms. Four primary evaluation metrics, ranging from the number of correct predictions to the total number of predictions, were used to assess the performance of the deep learning model during the testing phase [27].

Accuracy: is used to find ratio of correct predictions to total number of predictions [28],[29].

Accuracy = (TP+TN)/(TP+FP+FN+TN)*100%_____(4)

Recall: offers a summary of the model's sensitivity or the ratio of the positive data that was correctly classified as positive to the total amount of positive data [30].

Recall = Detection Rate = TP/TP + FN*100%_____(5)

Precision: resembles the ratio of the correctly predicted data to the overall positively predicted data, hence, a model with high precision is able to identify majority of the predicted data correctly [31].

Precision=TP/(TP+FP)*100% _____(6)

Furthermore, using it in this application is crucial because it will help us comprehend the system better [25].These metrics were chosen because CNN is a deep learning algorithm with a variety of features, and we anticipate that each algorithm will perform well on one or more of the evaluation matrices.

7. Results and Analysis

The main goal of the proposed system is to detect malware for DNP3 flows, so that industrial devices can communicate securely and reliably with each other. What is stated in this research defines a convolutional neural network (CNN). By tracking the structure of the system and using different criteria to evaluate the (CNN) algorithm to determine its suitability to the challenge of classifying the data set. In addition to using the Python programming language in this data analysis to create multiple ways to classify the data. Table (III) shows the results that are obtained when using the classification models on all variables of the dataset. Based on the evaluation metrics, algorithm (CNN) performance is displayed in Fig.3.

Table 3: The description for Results of The Classification Models CNN

model	Accuracy	RecalI	Precision	F1_score
CNN	98.9%	99%	99%	99%

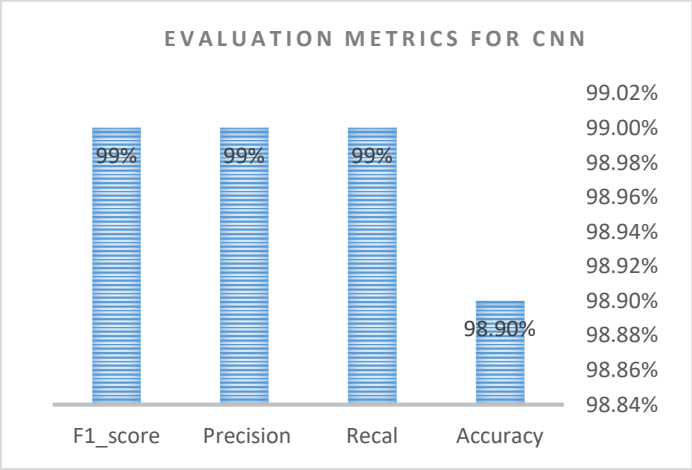

Figure 3. Show Evaluation Metrics for CNN.

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

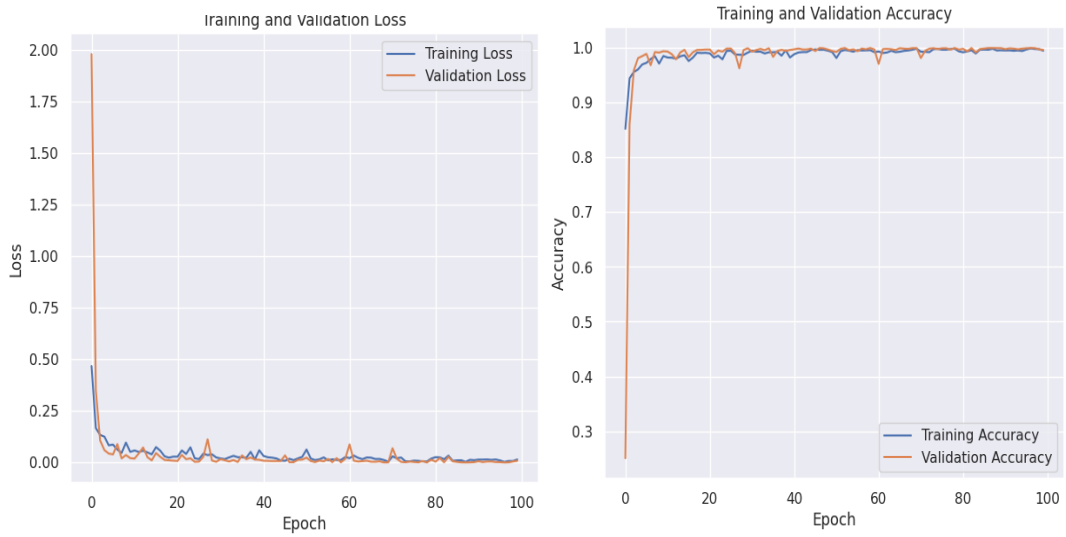

Figure 4. Shows the classification performance Accuracy and loss from CNN

8. Conclusion

The main objective of the proposed system is to implement secure communication for DNP3 by identifying malware in industrial hardware environment. This is done using the deep learning algorithm Convolutional Neural Network (CNN), an algorithm often used for identification on images, but is applied here for its ability to analyse patterns in data by classifying network traffic and detecting anomalies or potential intrusions on a comprehensive data set within traffic. Normal and abnormal DNP3 passage. Which contains 9 different attack scenarios, and this data set serves as a basis for training and testing the model. By using multiple classification on the dataset, it proved to be able to classify with 98% accuracy.

For future work, suggested that the same techniques used here could be used in other datasets, and continuous improvement and updating of the IDS with the latest threat and models is essential given the evolving nature of cybersecurity threats.

References

[1] V. Kelli et al., "Attacking and defending DNP3 ICS/SCADA systems," in 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2022, pp. 183–190.

[2] S. Alem, D. Espes, L. Nana, E. Martin, and F. De Lamotte, "A novel bi-anomaly-based intrusion detection system approach for industry 4.0," Futur. Gener. Comput. Syst., vol. 145, pp. 267–283, 2023.

[3] F. S. Mubarek, S. A. Aliesawi, K. M. A. Alheeti, and N. M. Alfahad, "Urban-AODV: an improved AODV protocol for vehicular ad-hoc networks in urban environment," Int. J. Eng. Technol., vol. 7, no. 4, pp. 3030–3036, 2018.

[4] A. K. Kareem, A. M. Shaban, A. A. Nafea, M. Aljanabi, S. A. S. Aliesawi, and M. Mal-Ani, "Detecting Routing Protocol Low Power and Lossy Network Attacks Using Machine Learning Techniques," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 57–62.

[5] I. Chakraborty, B. M. Kelley, and B. Gallagher, "Industrial control system device classification using network traffic features and neural network embeddings," Array, vol. 12, no. July, p. 100081, 2021.

[6] P. M. B, R. Amin, and G. P. Biswas, "A Deep Learning Based Artificial Neural Network Approach for Intrusion Detection," vol. 1, no. July 2019, pp. 34–43, 2017.

[7] N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, "Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon," Baghdad Sci. J., vol. 21, no. 1, p. 234, 2024.

[8] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," Appl. Sci., vol. 12, no. 16, 2022.

[9] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," Veh. Commun., vol. 21, p. 100198, 2020.

[10] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, "Intrusion detection using convolutional neural networks for representation learning," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10638 LNCS, pp. 858–866, 2017.

[11] M.-W. Mak and J.-T. Chien, "Omni SCADA Intrusion Detection Using Deep Learning Algorithms," Mach. Learn. Speak. Recognit., pp. 13–35, 2020.

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024

[12] P. Sun et al., "DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system," Secur. Commun. Networks, vol. 2020, 2020.
[13] S. Y. Diaba and M. Elmusrati, "Proposed algorithm for smart grid DDoS detection based on deep learning," Neural Networks, vol. 159, pp. 175–184, 2023.
[14] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," Int. J. Crit. Infrastruct. Prot., vol. 34, p. 100433, 2021.
[15] M. A. Ferrag and L. Maglaras, "Deliverycoin: An IDS and blockchain-based delivery framework for drone-delivered services," Computers, vol. 8, no. 3, pp. 1–15, 2019.
[16] M. Erza and K. Kim, "Deep Learning in Intrusion Detection System : An Overview," pp. 1–12.
[17] L. Rosa et al., "Intrusion and anomaly detection for the next-generation of industrial automation and control systems," Futur. Gener. Comput. Syst., vol. 119, pp. 50–67, 2021.
[18] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," Soft Comput., vol. 24, no. 22, pp. 17265–17278, 2020.
[19] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," Futur. Gener. Comput. Syst., vol. 113, pp. 418–427, 2020.
[20] N. N. Jamil and A. K. Kareem, "Comparative Analysis on Machine Learning and One-Dimensional Convolutional Neural Network to Predict Surface Enhanced Raman Spectroscopy," in 2023 3rd International Conference on Computing and Information Technology (ICCIT), 2023, pp. 216–221.
[21] B. Al-Rami, K. M. A. Alheeti, W. M. Aldosari, S. M. Alshahrani, and S. M. Al-Abrez, "A New Classification Method for Drone-Based Crops in Smart Farming", Int. J. Interact. Mob. Technol., vol. 16, no. 09, pp. pp. 164–174, May 2022.
[22] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. M. Chaabani, and A. Taleb-Ahmed, "Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features," IoTaIS 2020 - Proc. 2020 IEEE Int. Conf. Internet Things Intell. Syst., pp. 23–29, 2021.
[23] D. Prusti and S. K. Rath, "Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques," 2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019, pp. 1–6, 2019.
[24] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, pp. 1–29, 2021.
[25] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," Comput. Networks, vol. 184, no. November 2020, 2021.
[26] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, "Using Deep Learning Techniques for Network Intrusion Detection," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 171–176, 2020.
[27] N. Thapa, Z. Liu, D. B. Kc, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," Futur. Internet, vol. 12, no. 10, pp. 1–16, 2020.
[28] S. A. Rafa, Z. M. Al-qfail, A. A. Nafea, S. F. Abd-hood, M. M. Al-Ani, and S. A. Alameri, "A Birds Species Detection Utilizing an Effective Hybrid Model," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 705–710.
[29] K. M. A. Alheeti, A. Alzahrani, M. Alamri, A. K. Kareem, and D. Al_Dosary, "A Comparative Study for SDN Security Based on Machine Learning." Int. J. Interact. Mob. Technol., vol. 17, no. 11, 2023.
[30] Z. H. Abdaljabar, O. N. Ucan, and K. M. A. Alheeti, "An intrusion detection system for IoT using KNN and decision-tree based classification," in 2021 International conference of modern trends in information and communication technology industry (MTICTI), 2021, pp. 1–5.
[31] H. J. Mohammed, A. A. Nafea, H. K. Almulla, S. A. S. Aliesawi, and M. M. Al-Ani, "An Effective Hybrid Model for Skin Cancer Detection Using Transfer Learning," in 2023 16th International Conference on Developments in eSystems Engineering (DeSE), 2023, pp. 840–845.

DOI: https://doi.org/10.54216/JCIM.150217
Received: May 16, 2024 Revised: July 15, 2024 Accepted: November 04, 2024