DEEP LEARNING FOR SMART GRID INTRUSION DETECTION: A HYBRID CNN-LSTM-BASED MODEL

Abdulhakim Alsaiari and Mohammad Ilyas

Department of Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL, USA

ABSTRACT

As digital technology becomes more deeply embedded in power systems, protecting the communication networks of Smart Grids (SG) has emerged as a critical concern. Distributed Network Protocol 3 (DNP3) represents a multi-tiered application layer protocol extensively utilized in Supervisory Control and Data Acquisition (SCADA)-based smart grids to facilitate real-time data gathering and control functionalities. Robust Intrusion Detection Systems (IDS) are necessary for early threat detection and mitigation because of the interconnection of these networks, which makes them vulnerable to a variety of cyberattacks. To solve this issue, this paper develops a hybrid Deep Learning (DL) model specifically designed for intrusion detection in smart grids. The proposed approach is a combination of the Convolutional Neural Network (CNN) and the Long-Short-Term Memory algorithms (LSTM). We employed a recent intrusion detection dataset (DNP3), which focuses on unauthorized commands and Denial of Service (DoS) cyberattacks, to train and test our model. The results of our experiments show that our CNN-LSTM method is much better at finding smart grid intrusions than other deep learning algorithms used for classification. In addition, our proposed approach improves accuracy, precision, recall, and F1 score, achieving a high detection accuracy rate of 99.50%.

KEYWORDS

Security, Smart Grid, SCADA, DNP3, Intrusion Detection & Deep Learning.

1. INTRODUCTION

Traditionally, the term "grid" indicates the infrastructure that supports four essential electricity functions within the realm of electricity: power generation, long-distance transmission, distribution, and consumption [1]. The traditional power grid system (TG) is outdated, and it’s no longer capable of meeting the growing demand for electricity. It’s limited when using distributed and renewable energy sources, and it’s also inefficient when dealing with faults and issues. Hence, there is a shared motivation across academia and industry to upgrade to a smart power grid that aligns with contemporary living standards [2]. The smart grid is considered one of the most prominent applications of the Internet of Things (IoT). It consists of two infrastructures, known as the power infrastructure for electricity flow and the communication infrastructure for information flow [3]. These grids are capable of transmitting power from generating stations to consumers and information from consumers to generating stations. Moreover, the term "Smart Grid" (SG) refers to the next generation of power grids that integrate Information and Communication Technologies (ICT) [4]. The implementation of these technologies enhances the efficiency and reliability of monitoring and regulating the generation, distribution, and consumption of electrical energy [5]. However, with the integration of information and communication infrastructure, modern power grids have become more susceptible to various cyberattacks. Therefore, ensuring the timely and precise identification of potential threats is important, particularly in the context of industrial operations and smart grids,

DOI:10.5121/ijaia.2024.15301

to effectively address and minimize risks. Thus, deep learning techniques are commonly used in such smart grid systems to protect SCADA systems.

The use of Supervisory Control and Data Acquisition systems (SCADA) in critical infrastructure sectors is extensive. They contribute efficiently to monitoring and controlling industrial processes, enhancing operational efficiency, maintaining safety and regulatory compliance, and optimizing resource utilization. SCADA systems are widely employed across various industries, including energy, water and wastewater management, transportation, manufacturing, and more. In the context of the smart grid, SCADA is essential for enabling the smart grid to operate efficiently, reliably, and securely [6]. It provides real-time monitoring, control, and management capabilities across the electrical grid. Thus, securing the SCADA system from cyber threats is considered a serious concern. Another issue to consider is the lack of security features in many ICS/SCADA-oriented protocols like DNP3, widely used in manufacturing processes and particularly in the utility and energy sectors, including smart grids. Therefore, integrating technologies into ICS/SCADA systems for protection commonly involves utilizing machine learning and deep learning to develop an Intrusion Detection System (IDS) [7]. These technologies aim to enhance the security of ICS/SCADA systems and protect them against cyberattacks. Currently, there is a growing trend in the utilization of deep learning algorithms for the purpose of intrusion detection in a SCADA-based smart grid. Moreover, securing the smart grid from cyber threats is considered a serious concern [8]. Therefore, the implementation of IDSs has significantly enhanced the efficiency of these intelligent infrastructures by detecting potential security threats and mitigating their risks [9].

An Intrusion Detection System (IDS) is designed to monitor network traffic and enhance the security level by promptly identifying and potentially mitigating security threats. The implementation of IDS is crucial in securing essential networks from the rising challenges caused by malicious activities. The three components that comprise an IDS architecture are agents, an analysis engine, and a response module. An IDS can include several agents to monitor and capture the network activities of one or more systems. Furthermore, the analysis engine component initiates an investigation into potential cyberattacks. Eventually, when the response module detects a possible security breach, it notifies the system administrator or security team [10]. Additionally, one feature of the analysis engine is its ability to incorporate several methods for detecting cyberattacks. Signature-based and anomaly-based are the two main types of these mechanisms [11]. Signature-based intrusion detection mostly employs a blacklist approach, which is limited to identifying unknown attacks, and it’s necessary to update the attack detection library continuously [12]. On the other hand, the objective of the anomaly-based IDS is to detect atypical behavioral patterns via the comparison of characteristics between normal and abnormal activities. An anomaly-based approach is distinguished by its capacity to identify novel forms of attacks and exhibit reduced long-term costs while maintaining a high level of resilience to changes in the environment [11]. Typically, this mechanism incorporates techniques derived from machine learning and deep learning, including decision trees, Artificial Neural Networks (ANN), and clustering algorithms [10]. Researchers have conducted extensive research in the field of intrusion detection systems to develop advanced IDSs [13]. Furthermore, the utilization of intrusion detection technology is a highly efficient method for ensuring the security of a network. Additionally, an intrusion detection system can be created by utilizing a hybrid methodology that merges a feature selection model with a proficient classification technique [6].
Smart grids emerged as a result of the integration of digital technology into power systems. This revolution has raised security concerns, especially regarding the communication networks that support these systems. The main purpose of this research paper is to develop an efficient hybrid DL model to enhance the performance of smart grid IDS. This paper's contribution can be briefly stated as follows:

- To exploit the power of DL, we proposed a hybrid DL model that combines CNN and LSTM for smart grid IDS.
- For training and testing our model for binary-class classification, we employed an intrusion detection dataset, namely DNP3, focusing on unauthorized commands and DoS cyberattacks against the IEC 60870-5-104 protocol, which is commonly used in smart grid SCADA systems.
- Furthermore, numerous comprehensive experiments were executed, including hyperparameter tuning, to verify the effectiveness of the proposed technique for IDS in smart grids.
- The findings of our proposed approach show significant improvements across key performance metrics such as accuracy, precision, recall, and F1 score, with an accuracy rate of 99.50% and a detection rate of nearly 100%.

This paper is organized as follows: Section 2 provides a literature review of related studies. Section 3 describes the background of deep learning architecture. Section 4 introduces the proposed CNN-LSTM deep learning model and describes the applied dataset. In Section 5, the performance evaluation of the model and the result analysis of the experiment are illustrated. Finally, the conclusion and future work are described in Section 6.

2. RELATED STUDIES

The use of technology is rapidly advancing in today’s organizations. However, the IoT networks have a certain number of weaknesses in the field; one of them is the scope of security itself. New technologies must improve the ability to find breaches on the Internet of Things network. Based on the nature of the input data, the authors of [14] implemented the current solution using convolutional neural networks (CNNs), which generally offer an appropriate and effective deep learning method for processing inputs, especially with large numbers of dimensions that a standard neural network would be ill-equipped to handle. [15] implemented a multi-scale convolutional neural network (CNN) to automatically classify anatomical MR brain images into several groups. The approach achieves accurate segmentation details while preserving spatial consistency thanks to the use of a multi-scale methodology. The research paper [16] proposes a CNN model that uses binary and multiclass classification for detecting anomalies. The CSE-CICIDS 2018 dataset includes Advanced Denial of Service (DoS) attacks, including those targeting the application layer.

Researchers in [17] combined convolutional neural networks (CNNs) and recurrent gated units (RGUs) to evaluate network traffic patterns and identify anomalous behaviors indicative of DDoS assaults. Their studies' findings demonstrate how well the suggested hybrid deep-learning system performs, as evidenced by its 99.86% accuracy rate in identifying DDoS assaults. Abu Bakar et al. have expanded on earlier work by proposing and designing an IDS system. They have also tested the suggested architecture under a range of malicious instances, including DDoS assaults and floods. The suggested technique, fully dispersed, sounds like an early warning siren when pre-attack actions use network traffic.

The paper [18] provides a new decentralized method that uses Federated Learning (FL) to identify anomalies in smart grids with a precision that is equivalent to conventional techniques. To detect unusual usage of power in smart grids, they created FL models. To increase the breadth of smart grid recognition, the authors of [19] developed a local detection approach based on CNNs and GRUs, installed it in many isolated branch nodes, and extracted the important stream data using the technique of attention. For DDoS assaults in the cyber-physical combination of the smart grid, [20] suggests an approach fused with a convolutional neural network (CNN) and a gated recurrent unit (GRU).

[1] offers an anomaly detection approach that can identify abnormalities and categorize anomalies into specific incident types. The suggested MENSA model integrates two deep neural networks (DNNs) at the same time: an autoencoder and a generative adversarial network (GAN). The model provided by [21] applies initial condensed hidden layers to extract the necessary details from the input data and rebuild the supplied network sample. Using the chosen ideal threshold, it can accurately identify both known and unknown harm. A CNN-LSTM model was developed by [23] for smart grid data categorization to calculate the omitted cases in the dataset using the local quantities about the missing data point, a unique data preliminary processing technique.

The authors of [27] developed an efficient approach for reproducing the input data at the output layer with minimal reconstruction error. When anomalies arise, the trained model has a high error rate and is unable to recreate aberrant occurrences. The system uses mistakes as an indication to distinguish between typical and anomalous situations. To minimize harm to vital infrastructure, the research paper [45] suggests a computerized, multifaceted alerting method for identifying abnormalities in SCADA networks. An approach for the complex identification of anomalies and reliable gathering of features. The Gated Recurrent Units (GRU) deep learning technique has been used in [2] to identify DDoS and intrusion attempts in their proposed SDN defensive system, which depends on the examination of individual IP traffic records. Accelerating mitigating actions using direct flow inspection reduces the effect of the attack on the SDN.

The writers of [28] suggest using particle swarm optimization (PSO) to find FDIA in the SG framework using convolutional neural networks with long short-term memory (CNN-LSTM). It detects an anomalous monitoring value and identifies the kind of anomaly using phasor measurement unit (PMU) readings. To detect islanding, the 1D CNN and CNN-LSTM models are suggested by [41]. This study presents proactive islanding methods for recognizing coordinated and inverter-based microgrids. To estimate the condition of the power system during denial-of-service attacks, the researchers in [43] suggest a hybrid adjustment model based on deep neural networks that also uses a self-regressive model to address the issue of neural system models' scaling apathy.

The research paper [8] provides a framework that uses a convolutional neural network to create an equilibrium between two inputs by combining scales of time-series data and network traffic parameters. The suggested machine learning topology aids in the very precise detection ability of their anomaly detector. Snort outperformed Suricata in terms of detection precision, as reported by [333]. According to [39], cutting-edge machine learning (ML) algorithms can anticipate harmful attack anomalies, which are then used to train security models and forecast any unusual activity.

3. Background

3.1. Deep Learning

Deep learning is a broader field of artificial intelligence that has recently exhibited substantial achievements in several fields due to its capability to autonomously learn and make decisions. Deep learning techniques are inspired by the neural networks of the human brain. It utilizes complicated architectures consisting of multiple layers of interconnected nodes to independently learn complex patterns and characteristics in photos, text, audio, and other various data [17]. Moreover, deep learning algorithms autonomously identify complex relationships within extensive input data, enabling the model to generate predictions or execute tasks without explicit programming. As a result, deep learning has exhibited notable successes across various fields such as cybersecurity, natural language processing, and many other autonomous systems [41].

Several deep learning architectures have recently emerged to tackle different tasks. Those architectures employ multiple hidden layers between the input and output layers to extract more advanced patterns and characteristics from vast amounts of data. Furthermore, deep learning employs various architectures and algorithms to efficiently address various types of tasks by identifying complex patterns in a large amount of data [39]. Notably, CNN and LSTM are the most widely implemented deep learning architectures in a variety of applications in which the objective to be predicted is explicitly annotated within the training data.

3.2. Convolutional Neural Network (CNN) for Intrusion Detection

Convolutional Neural Networks (CNNs) are specific types of artificial neural networks that are inspired by the human visual cortex to recognize objects in real time. The main objective of using CNNs is to automatically handle and analyze visual data, making the data useful in tasks such as pattern and image recognition. In general, CNN is defined as a classic neural network architecture where data flows hierarchically from input to output across a series of interconnected nodes organized in layers. Convolutional, pooling, and fully-connected layers are the three key components of building CNN architecture [23]. Due to the capability of CNNs to automatically learn hierarchical representations from data, they have become a fundamental aspect in many fields, such as intrusion detection systems (IDSs).

CNNs in intrusion detection can analyze patterns in network traffic and identify unusual behaviors or potential security risks. The application of CNNs in vital infrastructures such as smart grids exploits the power of deep learning to improve security aspects. While incorporating information and communication technologies into traditional power grids has its benefits, there is an increased risk of various cyber threats and attacks targeting smart grids [7]. The following are several advantages of utilizing CNNs for smart grid intrusion detection:

- CNNs capability to handle heterogeneous and high-dimensional data makes them highly suitable for the complex and varied data sources present in smart grids.
- Their capacity to handle substantial volumes of data allows for effective and immediate analysis of network traffic, ensuring prompt identification and response to any security breaches.
- CNNs have the capability to acquire knowledge and adjust to evolving attack strategies, thereby enhancing their resilience against emerging threats.
- CNN-based IDS can decrease the occurrence of false positives by accurately differentiating between normal network behaviors and malicious actions. This helps to alleviate the workload of security staff.
- By autonomously acquiring features from the data, CNN-based intrusion detection systems can decrease reliance on manual feature engineering, which is both time-consuming and prone to errors [24].

3.3. Long Short-term Memory (LSTM) for Intrusion Detection

Long Short-Term Memory (LSTM) is a specific type of Recurrent Neural Network (RNN) that was developed to capture long-term temporal dependencies and address the issue of vanishing gradient difficulties. RNNs' concealed layers are substituted with LSTM units, which encompass memory cells and gates. The memory cells retain and store information under the control of the gates. The input gate, output gate, and forget gate are utilized to regulate the influx or outflow of information within the memory cell. Before adding new data to each memory cell, the LSTM network's architecture allows for the historical data to be forgotten from each memory cell [41]. For instance, the forget gate determines, given the previous concealed state and the current input data, which parts of the cell state are useful at time step t. The forget gate's cell state can have irrelevant values removed by the LSTM network, while important values can be identified and updated [25]. LSTMs are highly suitable for processing and analyzing sequential data, making them especially useful in applications such as time series prediction, natural language processing, speech recognition, and intrusion detection.

The Intrusion Detection System (IDS) is an essential tool that aims to ensure the availability, confidentiality, and integrity of data [21]. In fact, deep learning models are effective in dynamic and vast network environments due to their capacity to extract unique features without relying on manually designed feature extractions. Consequently, many researchers in smart grids concentrate on the advancement of IDS that are based on deep learning [22]. In addition, the LSTM deep learning technique is exceptionally effective and resilient when applied to smart grid intrusion detection systems [23]. LSTM demonstrates efficacy in capturing and evaluating temporal relationships in the data, rendering it highly suitable for detecting abnormalities and potential security breaches in the realm of smart grids. By exploiting the capabilities of LSTM, the intrusion detection system can improve its capacity to identify and react to cyber threats in the everchanging and dynamic environment of smart grids [24]. The following are some advantages of adopting LSTM in smart grid intrusion detection:

- Long Short-Term Memory (LSTM) networks demonstrate proficiency in representing temporal dependencies in data, enabling them to accurately capture the sequential patterns and temporal relationships inherent in smart grid activities. The identification of potential anomalies or intrusions that may occur over time is of utmost importance [14].
- Time series data, such as energy usage patterns and variations in the condition of the grid, are frequently included in smart grid data. Thus, LSTM's ability to handle time-dependent data makes it useful for identifying anomalous patterns or behaviors that could be signs of an intrusion [25].
- The LSTM architecture incorporates memory cells capable of retaining and transmitting substantial information from the early stages of the network to the final stage. This functionality facilitates the network's capacity to preserve long-term dependencies within Smart Grid data, hence improving its capability to identify tiny deviations or anomalies [23].
- LSTM models are highly efficient in processing sequential data, enabling real-time intrusion detection within smart grids. Quick identification and response to security threats is crucial for avoiding any potential disruptions [26].
- In RNN models, improperly assigned weights can cause vanishing and expanding gradient issues. LSTMs effectively address the common issue of vanishing gradients in RNNs, facilitating more efficient training on complex smart grid data [27].

4. PROPOSED HYBRID MODEL

4.1. System Description

Figure 1 illustrates the proposed hybrid deep-learning model for the Intrusion Detection System (IDS). The proposed hybrid model combines the Convolutional Neural Network model (CNN) and the Long Short-Term Memory model (LSTM) to develop an advanced Deep Learning (DL) technique to detect various types of cyberattacks. CNN is chosen to be applied due to its ability to capture position-invariant features. This position-invariant property is particularly valuable for tasks where the precise location of a feature or object in an image may vary, such as object recognition in computer vision, where objects can appear at different positions and orientations in images [17]. On the other hand, LSTM is a special type of RNN that adds some specific gate structures, including forgetting gates, input gates, and output gates. Furthermore, when compared to RNN with a single gate, LSTM offers a more robust technique for retaining short-term memories while also not losing long-term dependencies. In addition, designing an intrusion detection system model that combines CNN and LSTM is a powerful approach that allows for the extraction of both spatial features using CNNs and temporal dependencies using LSTMs [28].

For the purpose of strengthening the network, the algorithm architecture is equipped with two LSTM blocks and three CNN blocks. The convolution layer is responsible for extracting features from the input data and generating a feature map. To capture the feature mapping, the convolutional network multiplies the convolutional kernel by the input data, and then a non-linear activation function is applied to the feature map. The weights and biases in the convolutional kernel are initialized randomly [12]. Each CNN layer is followed by a max-pooling layer. The max-pooling operation creates a down-sampled version of the input feature map by selecting the maximum value from each feature within a certain area. In the concatenation layer, the final flattened output of CNN and the output of LSTM are combined. The concatenation layer is followed by a fully connected layer. The purpose of adding a dropout layer after the fully connected layer is to avoid overfitting. To convert the output to a probability distribution, the classification layer is linked to the SoftMax layer. This enables the classification layer to generate precise predictions regarding the different types of labels [20]. Eventually, the model is trained and tested using the DNP3 intrusion detection dataset.

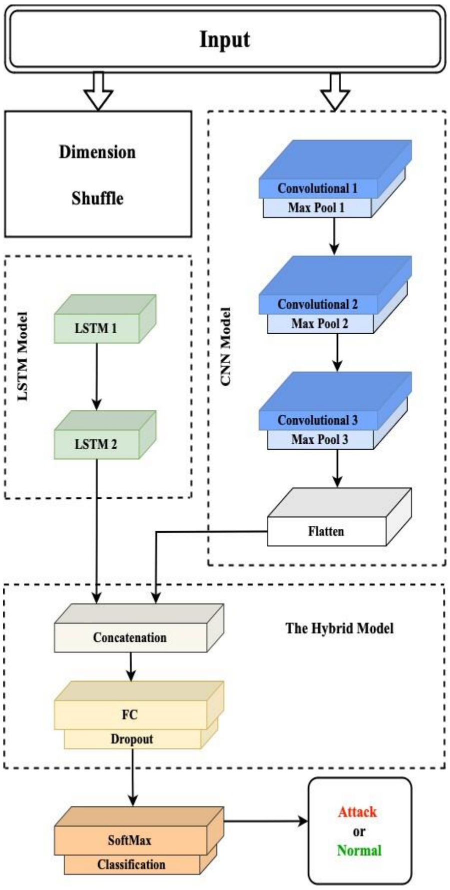


Figure 1. Proposed CNN–LSTM hybrid model

4.2. Dataset Description

Table 1. Samples for training and testing the model.

Type	Total Samples	Training Samples	Test Samples	Label
Normal	666	466	200	0
Attack	5,328	3,728	1600	1

DNP3 is widely utilized as a SCADA communication protocol, and its popularity has grown, particularly in the context of smart grids. Thus, an intrusion detection dataset from ITHACAUniversity of Western Macedonia (DNP3) [29] is applied to train and test our hybrid DL model for smart grid IDS. This dataset is publicly available and contains a wide range of normal and DNP3 attack scenarios that meet real-world criteria. Denial of Service (DoS) and unauthorized DNP3 commands are the focus of these malicious attacks. Based on flow features such as time stamps, source and destination IPs, source and destination ports, protocols, and attacks, the network traffic analysis is generated and included in this dataset by utilizing CICFlowMeter with labeled flows. Additionally, a custom DNP3 Python parser is also used for parsing and analyzing DNP3 communication packets within Supervisory Control and Data Acquisition (SCADA) and industrial control systems to ensure the security and reliability of critical infrastructure. The dataset generated consisted of 40,420 network flows, each containing 99 features. There were a total of nine labels utilized, consisting of eight attack labels and one normal flow label. Consequently, this dataset may be utilized to develop AI-powered Intrusion Detection and Prevention (IDPS) systems based on ML and DL techniques.

Data cleaning is the first step in preparing the dataset to be suitable for binary and multi-class classification using machine learning and deep learning methods. The features are then converted into numerical features and incorporated into the dataset along with any other numerical features. Furthermore, the labels in the dataset are numerically encoded, with the label "Normal" represented by 0 and the other DNP3 cyberattack labels such as “DNP3_ENUMERATE” and STOP_APP represented by 1. To reduce the feature variations, the dataset was uniformly normalized and mapped within the range of [0, 1]. The decision to consider all features and not perform feature selection has been made due to the absence of irrelevant features in the dataset, as shown in Figure 2, and based on the belief that each feature contributes valuable information to the model. Furthermore, the model's decision-making process is influenced by all available features in the dataset because omitting any might lead to a loss of relevant information or compromise the model's performance.

A normalization procedure has been applied to the dataset to bring the numerical values of different features onto a similar scale. In addition, the applicable dataset has a total of 99 columns with 5994 records. Each record is identified and labeled as an attack or not, where 1 represents the attack labels and 0 represents the normal labels. As illustrated in Table 1, the dataset is split into a training set and a testing set with a ratio of 70:30. The model is trained using 70% of the data, while the remaining 30% of the data is allocated for validation and testing after the training is completed.

- The following are the components of the confusion matrix that are used to calculate various performance metrics for the hybrid model classifier:
- True Positive (TP): This denotes a correct prediction by the algorithm when the instance is classified as positive, and it’s truly positive.
- True Negative (TN): This denotes a correct prediction by the algorithm when the instance is classified as negative, and it’s truly negative.
- False Positive (FP): This denotes a wrong prediction by the algorithm when the instance is classified as positive, but it is negative.
- False Negative (FN): This denotes a wrong prediction by the algorithm when the instance is classified as negative, but it’s positive.

The four metrics that are utilized to evaluate the hybrid model's performance are represented mathematically as in [18, 20, 28, 17] and written in subsequent equations as follows:

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

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

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

$$F1\ score = \frac{2(precision \times recall)}{(precision \times recall)}$$

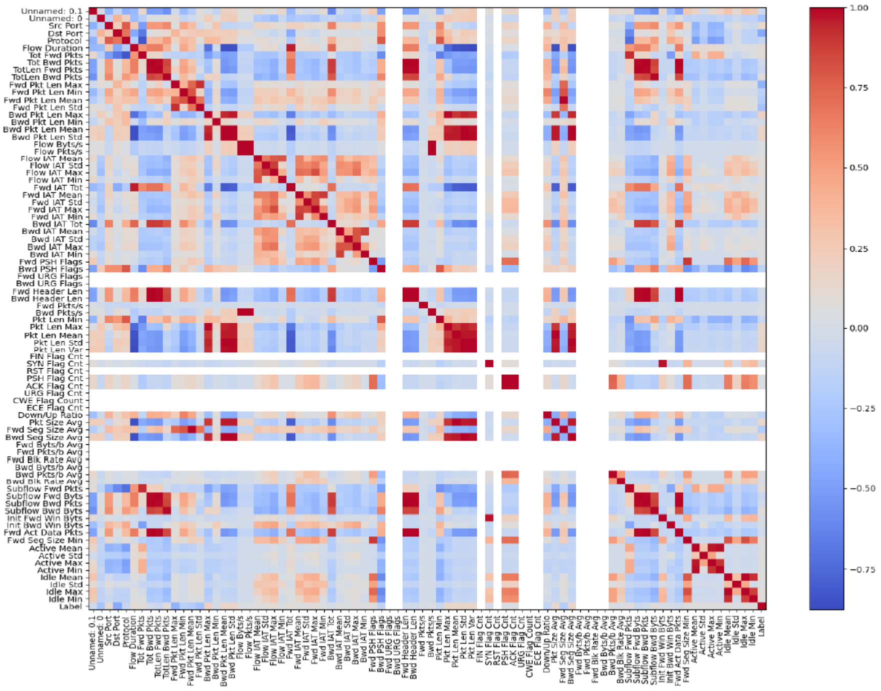


Figure 2. The dataset correlation map

5. Experiments and Results

To develop a reliable intrusion detection model, it is necessary to preprocess the large dataset first. After preparing the dataset, it has been applied to the proposed model and to different standalone deep learning models, such as CNN and LSTM. The experiments were conducted in the Python programming language on Jupyter Notebook, and Keras was employed as a deep learning framework. I have executed many experiments with various hyperparameters to get better results. The primary goal of hyperparameter tuning was to enhance the performance of the deep neural network on the chosen dataset.

The optimal selection of hyperparameters is crucial for building a successful neural network architecture, as the performance of the trained model depends on these values. Therefore, we must consider various hyperparameters when initiating effective deep learning classifiers for intrusion detection systems. Thus, I have assessed the model's performance by carefully varying hyperparameter values such as batch size, epochs, and learning rate. By applying the hyperparameter values illustrated in Table 2, I have successfully enhanced the performance of our intrusion detection model. After conducting various experiments, I realized that the learning rate clearly affects the performance of deep learning models. Even though a high learning rate can lead to faster convergence during training, it's more likely to be susceptible to the risk of overshooting the optimal solution. Thus, Adam (Adaptive Moment Estimation) was utilized as an adaptive learning rate optimizer. Moreover, a learning rate of 0.0001 consistently delivers strong performance, prevents overshooting, and improves model performance across different datasets. It is also critical to select the optimal number of epochs to effectively train a deep learning model. Overfitting can occur when the model learns noises and exhibits poor performance when applied to unseen data. We prevented underfitting and overfitting by applying epochs between 50 and 100 during our training process. An increased batch size provides the potential to capture a greater number of global patterns, which can speed up the training process.

However, a large patch size increases computational complexity and memory demands. As a result, a patch size in the range of 16 and 32 was appropriate for our model and resulted in a high rate of accuracy. In addition, with experimentation with different dropout rates, I figured out that a dropout rate of 0.5 is the optimal value for our model and dataset, and it can help correct overfitting. When dealing with datasets that contain complex patterns, it’s recommended to increase the number of convolutional layers, which results in improved performance. However, larger convolutional layers often include more parameters and computations, resulting in higher computational costs and memory consumption during training and inference. Hence, to achieve the best results, we propose employing three convolutional layers. We employed 64 and 128 LSTM units in our model, considering factors like model performance, computational efficiency, and potential overfitting.

Table 2. Hyperparameters for our model.

Parameter	**Value**
Learning rate	0.0001
Epoch	50 to 100
Batch size	16 to 32
Optimizer	Adam
Dropout rate	0.5
Convolutional layers	3
LSTM units	64, 128

Figure 3. illustrates the performance of the proposed approach compared to existing algorithms in terms of accuracy, precision, recall, and f1-score. I have assessed the model's performance by carefully varying hyperparameter values such as batch size, epochs, and learning rate. By applying the hyperparameter values illustrated in Table 2, I have successfully enhanced the performance of our intrusion detection model. The results demonstrate that the algorithm we suggest achieves high levels of accuracy, precision, recall, and f1-score, specifically 99.50%, 99.51%, 99.93%, and 99.72%, respectively. The CNN exhibits an accuracy of 99.33%, a precision of 99.50%, a recall of 99.75%, and a f1-score of 99.62%. On the other hand, the LSTM model achieved 94.39% accuracy, a precision of 93.82%, a recall of 99.94%, and a f1-score of 96.72%. Noticeably, the proposed CNN-LSTM hybrid model demonstrated superior performance compared to the comparison algorithms in all categories, except for the recall category. The CNNLSTM algorithm's recall dropped because of the increased FN value compared to the LSTM algorithm, which plays a crucial role. For clarification, the CNN-LSTM algorithm achieved an FN percentage of 0.18, while the LSTM achieved an FN percentage of 0.06. In terms of intrusion detection, the proposed algorithm provides distinctive performance compared to the existing algorithms (see Table 3).

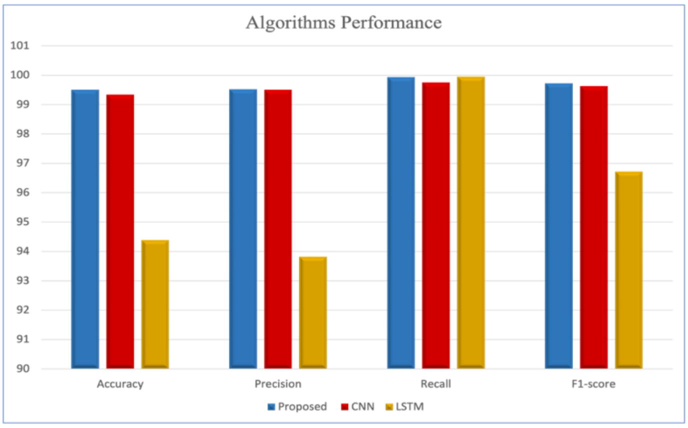
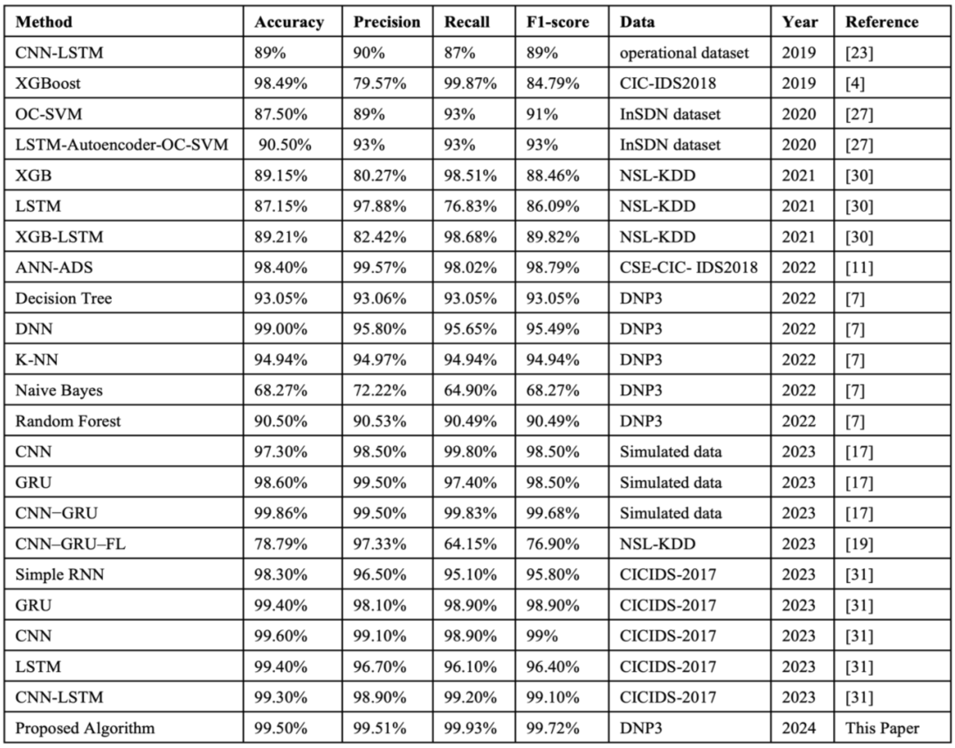


Figure 3. Performance Comparison of the considered algorithms

Table 3. Comparison with relevant works.



Method	Accuracy	Precision	Recall	F1-score	Data	Year	Reference
CNN-LSTM	89%	90%	87%	89%	operational dataset	2019	[23]
XGBoost	98.49%	79.57%	99.87%	84.79%	CIC-IDS2018	2019	[4]
OC-SVM	87.50%	89%	93%	91%	InSDN dataset	2020	[27]
LSTM-Autoencoder-OC-SVM	90.50%	93%	93%	93%	InSDN dataset	2020	[27]
XGB	89.15%	80.27%	98.51%	88.46%	NSL-KDD	2021	[30]
LSTM	87.15%	97.88%	76.83%	86.09%	NSL-KDD	2021	[30]
XGB-LSTM	89.21%	82.42%	98.68%	89.82%	NSL-KDD	2021	[30]
ANN-ADS	98.40%	99.57%	98.02%	98.79%	CSE-CIC- IDS2018	2022	[11]
Decision Tree	93.05%	93.06%	93.05%	93.05%	DNP3	2022	[7]
DNN	99.00%	95.80%	95.65%	95.49%	DNP3	2022	[7]
K-NN	94.94%	94.97%	94.94%	94.94%	DNP3	2022	[7]
Naive Bayes	68.27%	72.22%	64.90%	68.27%	DNP3	2022	[7]
Random Forest	90.50%	90.53%	90.49%	90.49%	DNP3	2022	[7]
CNN	97.30%	98.50%	99.80%	98.50%	Simulated data	2023	[17]
GRU	98.60%	99.50%	97.40%	98.50%	Simulated data	2023	[17]
CNN–GRU	99.86%	99.50%	99.83%	99.68%	Simulated data	2023	[17]
CNN–GRU–FL	78.79%	97.33%	64.15%	76.90%	NSL-KDD	2023	[19]
Simple RNN	98.30%	96.50%	95.10%	95.80%	CICIDS-2017	2023	[31]
GRU	99.40%	98.10%	98.90%	98.90%	CICIDS-2017	2023	[31]
CNN	99.60%	99.10%	98.90%	99%	CICIDS-2017	2023	[31]
LSTM	99.40%	96.70%	96.10%	96.40%	CICIDS-2017	2023	[31]
CNN-LSTM	99.30%	98.90%	99.20%	99.10%	CICIDS-2017	2023	[31]
Proposed Algorithm	99.50%	99.51%	99.93%	99.72%	DNP3	2024	This Paper

The validation loss metric is used to assess how well the model performs on unseen data during training. In this context, a lower validation loss indicates better performance, as it means the model is making more accurate predictions on new data. The proposed CNN-LSTM algorithm achieved its best validation performance, with a validation loss of 0.0155, at the 39th epoch. The CNN algorithm performed better than the LSTM algorithm, achieving a validation loss of 0.0172 at the 39th epoch, while the LSTM algorithm achieved its best validation performance, with a loss of 0.1660 at the 49th epoch (see Figures. 4, 5, and 6). Overall, lower validation loss values indicate better model performance when generating predictions on new data, and the epoch at which these low validation loss values are obtained indicates when the model is at its most accurate. Additionally, the comparison with CNN and LSTM algorithms demonstrates the superiority of the CNN-LSTM hybrid architecture in generalizing unseen data, as it outperformed both standalone CNN and LSTM models in terms of validation loss.

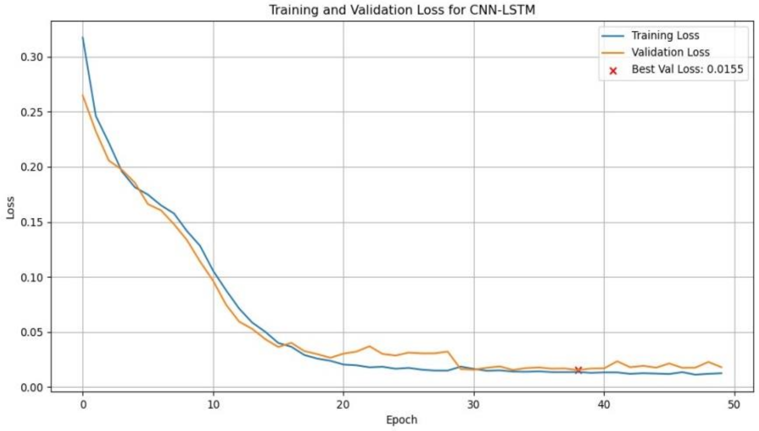


Figure 4. Validation Performance for the proposed CNN-LSTM

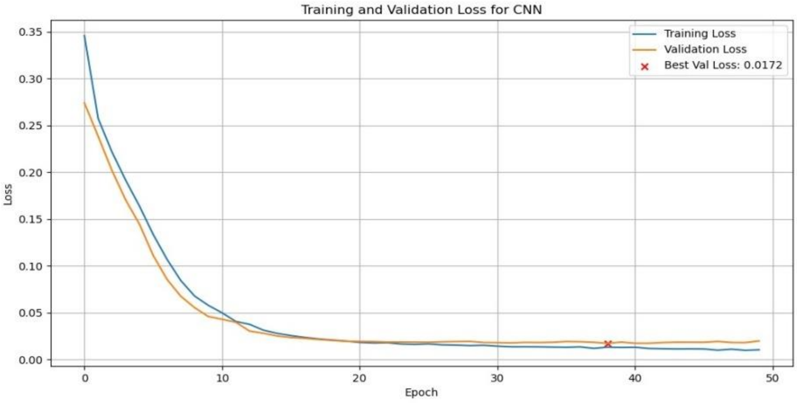


Figure 5. Validation Performance for the CNN

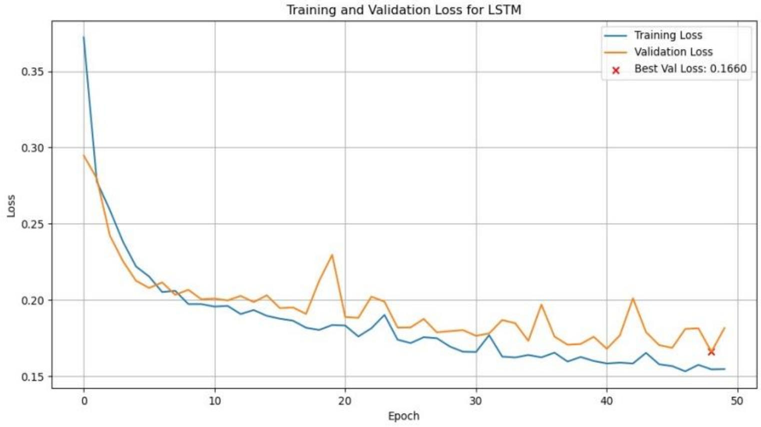


Figure 6. Validation Performance for the LSTM

6. CONCLUSION AND FUTURE WORK

Securing smart grid communication networks is crucial since electricity systems are becoming more digital. Smart grids that rely on SCADA are capable of gathering and controlling data in real-time because of Distributed Network Protocol 3 (DNP3) and other protocols. Robust intrusion detection systems are essential for early threat identification and mitigation since these connected networks are vulnerable to different cyberattacks. In this paper, a hybrid DL model specifically designed for intrusion detection in smart grids is proposed to address the problem of protecting smart grid communication networks. By combining the CNN and LSTM algorithms, we have developed a deep learning model for detecting intrusions in smart grid systems. The model was trained and tested using a recent intrusion detection dataset that focused on DNP3. Therefore, our proposed approach performed effectively in detecting DNP3 unauthorized commands and DoS cyberattacks on the DNP3 Intrusion Detection dataset. In addition, our hybrid CNN-LSTM model performed well in detecting and classifying intrusions, achieving high performance rates across various metrics. Exploiting the power of deep learning, the model obtained a high accuracy rate of 99.50%, precision of 99.51%, recall of 99.93%, and F1score of 99.72%. Furthermore, superior generalization was exhibited by our model on unseen data, reflected by low validation loss values. Overall, the result of our study demonstrates the effectiveness of using deep learning approaches, particularly hybrid architectures, for IDS in complex smart grid environments.

Our future work will focus on enhancing and examining the proposed model's performance by combining various DL techniques and expanding the performance analysis. Moreover, different intrusion detection datasets will be applied to our DL model, such as IEC 60870-5-104, which contains cyberattack activities against the IEC 60870-5-104 communication protocol, which is widely used in smart grid SCADA. In addition, we aim to improve the model's performance and reduce the manual effort required for hyperparameter tuning. This is achieved by applying hyperparameter optimization techniques such as Bayesian optimization, genetic algorithms, or reinforcement learning-based approaches. Eventually, several strategies and techniques will be investigated to enhance computational and memory consumption without compromising the accuracy and effectiveness of our intrusion detection model.

REFERENCES

[1] M. A. Judge, A. Khan, A. Manzoor, and H. A. Khattak, “Overview of smart grid implementation: Frameworks, impact, performance and challenges,” *Journal of Energy Storage*, vol. 49, p. 104056, May 2022, doi: 10.1016/j.est.2022.104056.

[2] Haji Mirzaee, M. Shojafar, H. Cruickshank and R. Tafazolli, "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," in IEEE Access, vol. 10, pp. 52922-52954, 2022, doi: 10.1109/ACCESS.2022.3174259.

[3] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.

[4] D. D. Roy and D. Shin, "Network Intrusion Detection in Smart Grids for Imbalanced Attack Types Using Machine Learning Models," 2019 International Conference on Information and Communication

[5] Technology Convergence (ICTC), Jeju, Korea (South), 2019, pp. 576-581, doi: 10.1109/ICTC46691.2019.8939744.

[6] P. Gope and B. Sikdar, "A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 53355348, Nov. 2021, doi: 10.1109/TSG.2021.3106105.

[7] D. Upadhyay, J. Manero, M. Zaman and S. Sampalli, "Intrusion Detection in SCADA Based Power Grids: Recursive Feature Elimination Model with Majority Vote Ensemble Algorithm," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2559-2574, 1 July-Sept. 2021, doi: 10.1109/TNSE.2021.3099371.

[8] V. Kelli et al., "Attacking and Defending DNP3 ICS/SCADA Systems," 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, Los Angeles, CA, USA, 2022, pp. 183-190, doi: 10.1109/DCOSS54816.2022.00041.

[9] X. Niu, J. Li, J. Sun and K. Tomsovic, "Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning," 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2019, pp. 1-6, doi: 10.1109/ISGT.2019.8791598.

[10] Ameli, A. Hooshyar, E. F. El-Saadany and A. M. Youssef, "Attack Detection and Identification for Automatic Generation Control Systems," in IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 47604774, Sept. 2018, doi: 10.1109/TPWRS.2018.2810161.

[11] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree," 2018 Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 2018, pp. 1-5, doi: 10.1109/GIIS.2018.8635743.

[12] M. Abdelkhalek, G. Ravikumar and M. Govindarasu, "ML-based Anomaly Detection System for DER Communication in Smart Grid," 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, USA, 2022, pp. 1-5, doi: 10.1109/ISGT50606.2022.9817481.

[13] H. Liang, C. Ye, Y. Zhou and H. Yang, "Anomaly Detection Based on Edge Computing Framework for AMI," 2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT), Qingdao, China, 2021, pp. 385-390, doi: 10.1109/ICEEMT52412.2021.9601888.

[14] Sharafaldin, A. Habibi, and A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” ICISSP, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[15] M. Alabadi and Y. Celik, "Anomaly Detection for Cyber-Security Based on Convolution Neural Network: A survey," 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2020, pp. 1-14, doi: 10.1109/HORA49412.2020.9152899.

[16] P. Moeskops, M. A. Viergever, A. M. Mendrik, L. S. de Vries, M. J. N. L. Benders and I. Išgum, "Automatic Segmentation of MR Brain Images With a Convolutional Neural Network," in IEEE Transactions on Medical Imaging, vol. 35, no. 5, pp. 1252-1261, May 2016, doi: 10.1109/TMI.2016.2548501.

[17] Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-Based Network Intrusion Detection against Denial-of-Service Attacks,” Electronics, vol. 9, no. 6, p. 916, Jun. 2020, doi: 10.3390/electronics9060916. [17] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, “Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks,” Sensors, vol. 23, no. 17, p. 7464, Aug. 2023, doi: 10.3390/s23177464.

[18] Jithish, B. Alangot, N. Mahalingam and K. S. Yeo, "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," in IEEE Access, vol. 11, pp. 7157-7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[19] F. Zhai, T. Yang, H. Chen, B. He, and S. Li, “Intrusion Detection Method Based on CNN–GRU–FL in a Smart Grid Environment,” Electronics, vol. 12, no. 5, p. 1164, Feb. 2023, doi: 10.3390/electronics12051164.

[20] S. Y. Diaba and M. Elmusrati, “Proposed algorithm for smart grid DDoS detection based on deep learning,” Neural Networks, vol. 159, pp. 175–184, Feb. 2023, doi: 10.1016/j.neunet.2022.12.011.

[21] S. Aktar and A. Yasin Nur, “Towards DDoS attack detection using deep learning approach,” Computers & Security, vol. 129, p. 103251, Jun. 2023, doi: 10.1016/j.cose.2023.103251.

[22] Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.

[23] Md. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. M. Islam, and J.-M. Kim, “Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach,” Energies, vol. 12, no. 17, p. 3310, Aug. 2019, doi: 10.3390/en12173310.

[24] V. Ramanathan, K. Mahadevan, and S. Dua, "A Novel Supervised Deep Learning Solution to Detect Distributed Denial of Service (DDoS) attacks on Edge Systems using Convolutional Neural Networks (CNN)," arXiv, vol. 1, no. 2309.05646, Sep. 2023.

[25] Y. Wei, J. Jang-Jaccard, F. Sabrina, W. Xu, S. Camtepe, and A. Dunmore, "Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data," arXiv, vol. 1, no. 2305.09475, Aug. 2023.

[26] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 3, pp. 825–831, Mar. 2022, doi: 10.1016/j.jksuci.2019.04.010.

[27] Elsayed, N.-A. Le-Khac, S. Dev, and A. Jurcut, "Network Anomaly Detection Using LSTM Based Autoencoder," the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp. 37– 45, Nov. 2020.

[28] Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," International Journal of Critical Infrastructure Protection, vol. 40, p. 100582, Mar. 2023, doi: 10.1016/j.ijcip.2022.100582.

[29] Panagiotis Radoglou-Grammatikis, Vasiliki Kelli, Thomas Lagkas, Vasileios Argyriou, Panagiotis Sarigiannidis, November 22, 2022, "DNP3 Intrusion Detection Dataset", IEEE Dataport, doi: https://dx.doi.org/10.21227/s7h0-b081.

[30] C. Song, Y. Sun, G. Han, and J. J. P. C. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," Computers & Electrical Engineering, vol. 93, p. 107212, Jul. 2021, doi: 10.1016/j.compeleceng.2021.107212.

[31] N. Elmrabit, F. Zhou, F. Li and H. Zhou, "Evaluation of Machine Learning Algorithms for Anomaly Detection," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 2020, pp. 1-8, doi: 10.1109/CyberSecurity49315.2020.9138871.