Neural Networks 159 (2023) 175–184

Contents lists available at ScienceDirect

Neural Networks

journal homepage: www.elsevier.com/locate/neunet

Proposed algorithm for smart grid DDoS detection based on deep learning

Sayawu Yakubu Diaba *, Mohammed Elmusrati

Department of Telecommunication Engineering, School of Technology and Innovations, University of Vaasa, Vaasa, Finland

ARTICLE INFO

Article history:
Received 16 August 2022
Received in revised form 27 October 2022
Accepted 14 December 2022
Available online 21 December 2022

Keywords:
State estimation
Smart grid
Distributed denial of service
Intrusion detection
Gated recurrent unit
Convolutional neural network

ABSTRACT

The Smart Grid's objective is to increase the electric grid's dependability, security, and efficiency through extensive digital information and control technology deployment. As a result, it is necessary to apply real-time analysis and state estimation-based techniques to ensure efficient controls are implemented correctly. These systems are vulnerable to cyber-attacks, posing significant risks to the Smart Grid's overall availability due to their reliance on communication technology. Therefore, effective intrusion detection algorithms are required to mitigate such attacks. In dealing with these uncertainties, we propose a hybrid deep learning algorithm that focuses on Distributed Denial of Service attacks on the communication infrastructure of the Smart Grid. The proposed algorithm is hybridized by the Convolutional Neural Network and the Gated Recurrent Unit algorithms. Simulations are done using a benchmark cyber security dataset of the Canadian Institute of Cybersecurity Intrusion Detection System. According to the simulation results, the proposed algorithm outperforms the current intrusion detection algorithms, with an overall accuracy rate of 99.7%.

1. Introduction

The modernized grid enables a two-way flow of electricity and information while providing efficient, dependable, computerized, and decentralized energy distribution. The Supervisory Control and Data Acquisition (SCADA) Master Terminal Unit (MTU) and the Intelligent Electronic Devices (IED) on the electric network establish communication. The Remote Terminal Units (RTUs), Phasor Measurement Unit (PMU), Micro Phasor Measurement Unit (μPMU), and Programmable Logic Controls (PLC) mounted at various locations on the electric network provide telemetry data to the SCADA's server (Oyewole & Jayaweera, 2020). Electric utilities all around the world use various SCADA protocols to communicate between IEDs on the network and control center applications using different SCADA protocols, such as International Electrotechnical Commission (IEC) 61850, Modbus, and Distributed Network Protocol 3 (DNP3) (Mohan, Ravikumar, & Govindarasu, 2020). With these SCADA protocols, parameters are measured, processes are monitored, and operations are controlled using measurement and control systems (Yohanandhan, Elavarasan, Manoharan, & Mihet-Popa, 2020), which are frequently utilized in operational technology (OT) such as Smart Grid.

The SCADA system in the context of the electric network is a crucial infrastructure made up of computer-based networked systems that exchange important data across networks. Such systems are vulnerable to intrusion attacks owing to the extensive use of information technology (Liu, Li, Shuai, & Wen, 2017). Therefore, one crucial task is to evaluate the system security by considering the probable attack that could be launched by network intruders from the communication network lateral. Knowing the system security valuation would help maintain the modern electric infrastructure's security and operational stability (Fu et al., 2019).

Intrusion detection is an approach to identifying attacks before or after gaining access to a secure network. Incorporating this approach into the gateway is the quickest way to integrate it with an IEC61850-based network. Even though attack detection and self-healing are not specified in IEC 61850, a specific technique like Intrusion Detection System (IDS) may be employed within the grid to support IEC 61850's security (Elgargouri, Virrankoski, & Elmusrati, 2015). As machine-to-machine (m2 m), and human-machine-interface (HMI) connectivity increases, the potential hostile threats in the electric infrastructure become prevalent. The IDS is essential for monitoring Smart Grid security and situational awareness (Hu, Yan, & Liu, 2020; Ullah & Mahmoud, 2017). Likewise, the transmission of data via the radio medium which represents the fundamental pillar by which all devices in the Smart Grid network communicate has become prone to cyber-attack. Due to the interconnectivity (Chen, Zhang, Liu, & Tang, 2018) of the various technologies (Attia, Sedjelmaci, Senouci, & Aglzim, 2015) which was not historically known in the

* Corresponding author.
E-mail address: sdiaba@uwasa.fi (S.Y. Diaba).

https://doi.org/10.1016/j.neunet.2022.12.011

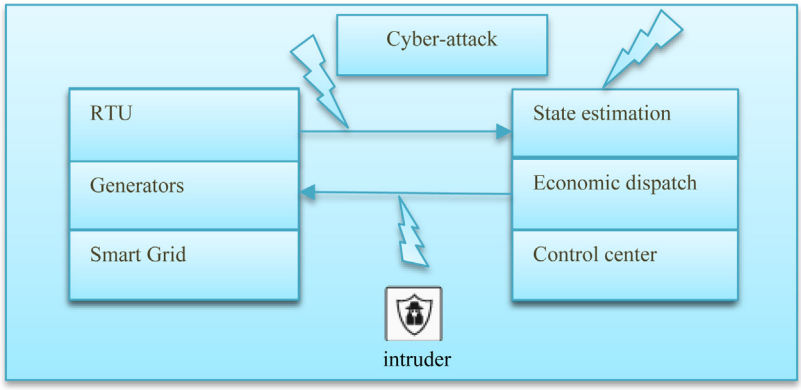


Fig. 1. Depicts a cyberattack on the smart grid.

electric networks. This makes the system vulnerable to intrusion attacks (Mahmud, Vallakati, Mukherjee, Ranganathan, & Nejadpak, 2015), which can result in significant financial losses (Gao, Li, Jiang, Li, & Quan, 2020; Jiang, Xu, Zhang, Hong, & Cai, 2020) but, more crucially, put public safety at risk. The risk is increased when new connections are added to such critical infrastructures. Therefore, a high-priority area of study in the realm of cyber security is intrusion detection in the SCADA network of a Smart Grid (Hosseinzadehtaher, Khan, Shadm, & Abu-Rub, 2020; Xu, 2020) (see Fig. 1).

On the other hand, distributed generation (DG) has been the means to shift toward renewable energy sources (RES). Establishing DG at various points of an existing network affects the primary contour of the electric network. This causes alterations in voltage and current at different nodal points and also increases the points of entry into the electric network (de Figueiredo, Ferst, & Denardin, 2019). The total Smart Grid's communication technologies and supporting infrastructure are directly impacted by the scale of the electrical network (Talha & Ray, 2016).

Looking at the shortcomings of the current Smart Grids communication mechanisms has inspired several researchers to explore cyber risks to Smart Grids. We propose an algorithm for detecting Distributed Denial of Service (DDoS) in Smart Grid in response to the aforementioned facts. The DDoS includes bombarding a target with a large volume of data and internet traffic, typically with the aid of a network of compromised machines. The following summarizes this paper:

- To identify DDoS attacks we propose an algorithm hybridized by a Convolutional Neural Network (CNN) and a Gated Recurrent Unit (GRU) for DDoS attacks in the cyber–physical system of the Smart Grid.
- Utilizing benchmark datasets from the Canadian Institute of Cybersecurity Intrusion Detection System (CICIDS2017), in-depth simulation studies are presented. Comparative analyses are drawn and the proposed algorithm performed better in comparison to other state-of-the-art algorithms with a 99.7% accuracy and 99.9% detection rate.

The remainder of the paper is organized as follows. A review of the literature is in Section 2. Presenting the proposed hybrid algorithm is given in Section 3. The proposed algorithm's performance is compared to current algorithms in simulations described in Section 4. Finally, concluding observations are made in Section 5.

2. Related studies

Communication networks' reliability, confidentiality, and integrity are just a few of the difficulties involved in protecting sensitive infrastructure, such as Smart Grid. To protect this crucial infrastructure, the Smart Grid requires a security strategy. It is necessary to meet requirements for data authentication, confidentiality and integrity assurance, and other security-related issues (Subasi et al., 2018). Owing to the above-stated reasons, researchers have evaluated intrusion detection in the cyber–physical of the Smart Grid from different perspectives. For example, Li et al. suggested various monitoring measures to track suspicious branch flow changes and abnormal load deviations. Two-stage approaches are suggested to identify false data injection (FDI) attacks. The article introduces the FDI cyber-attack to investigate the impact of FDI attacks on system reliability (Li & Hedman, 2020). The alert system with the developed unique metrics serves as the foundation for the suggested FDI detection approach.

A customized firewall model SCADAWall was proposed to address the limitations of the traditional firewall system in protecting the SCADA networks (Li, Guo, Zhou, Zhou, & Wong, 2019). The traditional SCADA systems were working in the principle of deep packet inspection that was designed to inspect the payload contents in the communication. A proprietary industrial protocols extension algorithm and an out-of-sequence detection algorithm were added to the SCADAWall to improve its ability to identify abnormal changes in industrial operations. The experimental analysis indicates that the SCADAWall framework is effective in the detection process by maintaining the latency parameters of the SCADA system (Li et al., 2019). A testbed model was developed for SCADA systems (Almgren, 2018) to confirm the effectiveness of the suggested algorithms in a real-time scenario. The virtual model is equipped with an energy management model monitored by a SCADA system. The testbed was created to give various real-world scenarios like attack generation and defense algorithms. An anomaly-based method was created to detect malicious packet movement in the SCADA network (Singh, Ebrahem, & Govindarasu, 2018). The experimental work indicates a better latency and detection rate. The rule-based intrusion detection system presented in Yang et al. (2013) employs a deep packet inspection technique and was designed specifically for SCADA systems. It also contains signature-based and model-based techniques. The suggested signature-based rules are capable of correctly identifying several known suspicious or malicious assaults.

An algorithm was made to address the SCADA system's Dynamic Link Library (DLL) injection attack (Lee & Hong, 2020). The model utilizes the Windows Application Programming Interface (API) function that verifies the changes in the DLL load and enables the diversion algorithm when an attack is detected. A security layer was structured between the physical and link layer of the SCADA system to overcome the issues observed from the existing firewall and authentication mechanisms (Cherifi &

Hamami, 2018). An IEC 60870 — 5 — 101 communication protocol was employed in the work and that is un-routable by the intrusion algorithms. The simulation implementation of the security layer protection in an electrical substation testbed indicates a satisfactory performance over the previous models.

An analysis was performed to identify the effectiveness of artificial intelligence (AI)-based techniques in detecting Denial of Service (DoS) attacks in SCADA systems (Aldossary, Ali, & Alasaadi, 2021). The experimental result indicates that a model developed as Bidirectional Long Short-Term Memory (Bi-LSTM) was capable of detecting intrusions against the other methods. To identify intrusion detection and DoS in the smart meter, a cyber–physical monitoring system was proposed (Sun, Guan, Liu, & Liu, 2013). The idea is predicated on the informational fusion of online occurrences and objective data. The test shows that by linking the cyber and physical signals, the model successfully detects threats.

A temporal pattern recognition technique was proposed to observe the cyber-attack intrusions in the SCADA systems (Kalech, 2019). The technique was also designed to monitor the abnormal changes in the operation of the connected system. This was achieved by implementing the model with a hidden Markov model and the artificial neural network (ANN) algorithm. The effectiveness of the proposed model was verified with simulations and real-time scenarios with five different feature extraction strategies and the approach that was implemented with the time feature extraction model was found satisfactory.

A C4.5 decision tree algorithm was proposed to give a security model over the SCADA system implemented in gas and oil plants. The performance analysis of the proposed model explores a betterment in handling large-scale distributed attacks in the SCADA setup (Yang, Liu, & Zhang, 2019). A SCADA network attack detection technique was developed with a random forest algorithm and its attainments were compared over the support vector machine (SVM). It indicates a 96.47% of f1 score on detecting the DoS attacks (Lopez Perez, Adamsky, Soua, & Engel, 2018). The performances of the decision tree and K-nearest neighbor algorithms (KNN) were analyzed on cyber security identification. The experimental work was performed with three different cybersecurity datasets. The work findings found satisfactory results with a fine tree and weighted KNN (Ahakonye, Nwakanma, Lee, & Kim, 2021). A DDoS attack detection approach on the SCADA system was performed with J48, Naïve Bayes, and random forest algorithms. The experimental work utilizes the KDDCUP99 dataset for the analysis and was found satisfied with the accuracy rate of 99.99% in the random forest algorithm (Alhaidari & AL-Dahasi, 2019).

For Software Defined Networking (SDN), the authors of Fouladi, Ermiş, and Anarim (2022) provided a DDoS attack detection and countermeasure technique based on discrete wavelet transform and auto-encoder neural network. In the suggested method, wavelet transform was used to extract statistical features that are then processed by an auto-encoder neural network to identify samples of DDoS attacks. In order to effectively resist DDoS attacks, a novel feature selection-whale optimization algorithm deep neural network approach is presented in Agarwal, Khari, and Singh (2021). The usual data are homomorphically encrypted and safely stored in the cloud to increase the security of the proposed paradigm. A 95.35% accuracy in detecting DDoS attacks was shown by simulation results. A swarm intelligence technique was developed to identify the optimum features for making a good accuracy rate in the intrusion detection system process. An Aquila optimizer model was also employed in the work after the feature selection process for assigning desirable weights to the extracted features. The work offered a reasonable result when implemented with a CNN classifier with a particle swarm optimization model (Fatani, Dahou, Al-qaness, Lu, & Abd Elaziz, 2022).

Concerning internet-based computer network attacks, a neural network-based intrusion detection method is presented in Shum and Malki (2008). IDS were developed to foresee and stop potential attacks. To find and forecast anomalous system behavior, neural networks were used. The study specifically used feedforward neural networks with the back-propagation training algorithm. The experimental outcomes utilizing real data demonstrated positive outcomes for neural-network-based IDS. In Peng, Kong, Peng, Li, and Wang (2019), a deep learning-based technique for network intrusion detection is presented. In the model, network monitoring data features are extracted using deep neural networks, and intrusion types are classified at the top-level using back propagation neural networks. The KDDCUP99 dataset from the Massachusetts Institute of Technology's Lincoln Laboratory was used to validate the approach. The findings indicate that the proposed method meaningfully outperforms the accuracy of conventional machine learning. In Hai-He (2018) the authors proposed an IDS based on the improved neural network where feature extracting was carried out using the adaptive weighted control method. The model showed higher accuracy using a back propagation neural network for classification and detection. However, the back propagation neural network algorithm proposed in Jaiganesh, Sumathi, and Mangayarkarasi (2013) with the primary duty of detecting threats to the resources demonstrated a poor attack detection rate.

To categorize network threats, the study in Lin, Lin, Wang, Wu, and Tsai (2018) concentrated on network intrusion detection utilizing CNNs based on LeNet-5. The experiment's findings indicate that with samples larger than 10,000, intrusion detection prediction accuracy increases and gains overall accuracy of 97.53%. The authors of Khan, Zhang, Alazab, and Kumar (2019) offer a network intrusion detection approach using CNN. The approach is intended to efficiently categorize intrusion data by automatically extracting useful features from intrusion samples. An automated vision-based android malware detection algorithm was proposed with a fine-tuned CNN algorithm. The byte codes extracted from the various malware devices are collected in the work for training the classifiers. The experimental work attains an accuracy of 99.4% and 98.05% on both balance and imbalanced datasets (Almomani, Alkhayer, & El-Shafai, 2022). In the blockchain-based energy network, Ferrag and Maglaras (2019) presented a learning-based method to identify network threats and fraudulent transactions. The suggested system generates blocks using short signatures and hash functions to thwart Smart Grid attacks.

Peng (2020) propose a hybrid CNN-based intrusion detection approach. The hybrid deep learning network structure extracts and encapsulates the features of unfamiliar malicious behavior as well as more complex structure aspects of the full network traffic matrix, in contrast to the typical machine learning approach. In the network traffic matrix, a CNN first extracts the correlation between several features. Then, by using a Recurrent Neural Network (RNN) to fully mine the temporal and spatial features of the entire network traffic matrix, the accuracy of the intrusion detection model is boosted. Al-Emadi, Al-Mohannadi, and Al-Senaid (2020) developed an intelligent detection system that can recognize various network intrusions using deep learning approaches, specifically CNN and RNN. The authors compared the results of the offered solution and evaluated the performance of the proposed solution using several evaluation matrices to select the best model for the network IDS. Koutsandria et al. suggested a hybrid control paradigm that constantly tracks and examines the network traffic that is transferred inside the physical system. It detects communication patterns that diverge from expectations or physical constraints that can put the system in a dangerous mode of operation. The simulations show that, by utilizing data

on the physical component of the power system, the paradigm is capable of identifying a wide variety of attack scenarios intended to compromise the physical process (Koutsandria et al., 2014).

In Vijayanand, Devaraj, and Kannapiran (2019) a unique attack detection system that uses deep learning algorithms to detect attacks by carefully examining smart meter communications is presented. To detect cyber-attacks accurately, the attack detection system uses several multi-layer deep algorithms that are set up in a hierarchical order. In Farrukh, Ahmad, Khan, and Elavarasan (2021) the authors proposed a two-layer hierarchical machine learning model with 95.44% accuracy in detecting cyber-attacks. Using the model's first layer, the two modes of operation, normal state and cyberattack are identified. The authors of Zhao, Chen, and Luo (2011) suggested a methodology incorporating real-time neural network training and expert system detection to improve detection accuracy. The model employs neural networks to detect and converts pattern recognition into numerical calculation to speed up the detection rate. The state is divided into many categories of cyberattacks using the second layer.

In our humble opinion, as so many articles have consisted of IDS in power systems annals with little reference to the hybridization milieu, a revisit of that background could yield a novelty. This paper seeks to present one.

3. System model

Fig. 2 shows the proposed hybrid deep learning algorithm. In our earlier study (Diaba, Shafie-khah, & Elmusrati, 2022), this algorithm was tested using the Network Security Laboratory-Knowledge Discovery and Data Mining (NSL-KDD99) dataset, and the results were compared with CNN, GRU, and LSTM algorithms. The algorithm performed better in terms of accuracy, detection rate, precision, and force positive rate (FPR). However, Elmrabit, Zhou, Li, and Zhou (2020) argued that the NSL-KDD99 dataset had expired. Since the network traffic in that dataset was established in 1998, the authors claimed that it is impossible for it to accurately reflect the most recent network topologies and attack dynamics. We, therefore, seek to apply the CICIDS2017 cyber security dataset to the algorithm because of the presence of a large variety of up-to-date attack scenarios in the dataset, which satisfy real-world requirements.

The proposed IDS integrates a CNN model and a GRU model. It is believed that CNN is effective at capturing position-invariant characteristics, thus the choice. The GRU module collects the long-dependence features and uses memory cells to extract key information from the previous data. The reset gate is employed to erase or eliminate pointless data. These influenced the decision to use the GRU model (Aldossary et al., 2021). Three GRU blocks and four CNN blocks are mounted in the algorithmic architecture to deepen the network (Huang, Li, Deng, Yu, & Ma, 2022). The purpose of the convolution layer is to produce a feature map by separating features from the input data. To capture the feature mapping, the input data are multiplied by the convolutional kernel in the convolutional network, which is then activated by a nonlinear function. The convolution kernel randomly initializes weights and biases (Liang, Ye, Zhou, & Yang, 2021). After each CNN layer, a normalization layer and a max-pooling layer are added. The procedure of obtaining the maximum or average value for all features within the immediate area is referred to as a "pooling operation".

The concatenation layer, where the GRUs output and the CNN outputs are combined, receives the flattened final output of the CNN layers. Two completely connected layers are connected after the concatenation layer. A dropout layer is used after the last fully connected layer to prevent overfitting. The SoftMax layer connects to the classification layer to map the output to a probability distribution, which allows the classification layer to predict the types of labels.

3.1. Deep neural network structure

Artificial neural networks were inspired by research on biological neural network processing, a type of computer structure. An artificial neural network is a self-motivated system made up of highly connected, parallel nonlinear processing components, units, or nodes that exhibit extremely high levels of computation efficiency. It can alternatively be viewed as versatile mathematical structures that can recognize intricate nonlinear correlations between input and output datasets (Suppitaksakul & Saelee, 2009). A typical neural network comprises numerous small, interconnected processes called neurons, each generating a string of activations with real values. Environmental sensors activate input neurons, and weighted connections from previously active neurons excite more neurons (Komyakov, Erbes, & Ivanchenko, 2015; Liang et al., 2021; Schmidhuber, 2015) (see Fig. 3).

3.2. System description

The mathematical formulation of the proposed algorithm considers a features vector ξ, given as

$$\xi = [\xi_1, \xi_2, \ldots, \xi_n]^T \tag{1}$$

as inputs to the proposed model. The GRU's first layer processes the data and generates the outputs. The first layer's outputs are fed into the second layer. Again, the outputs of the second layer are inputted into the third layer. The final outputs of the GRU model are achieved by using an activation function. We apply the most used activation functions, the sigmoid, and the tanh, respectively, given as in Ismail et al. (2022) and Valdes, Macwan, and Backes (2016).

$$s(x) = \frac{1}{1+e^{1-x}} \tag{2}$$

$$\tanh(x) = \frac{2}{1+e^{-2x}} - 1 \tag{3}$$

Mathematically, the GRU gate $\in\{0,1\}$ and thus, the model can be written mathematically as

$$\varsigma_0 = \sigma\left(\omega_0\left[\widetilde{\xi}^{(t-1)}, x^{(t)}\right] + b_0\right) \tag{4}$$

$$\varsigma_1 = \sigma\left(\omega_1\left[\widetilde{\xi}^{(t-1)}, x^{(t)}\right] + b_1\right) \tag{5}$$

where, ς_0, ς_1 represent the update gate and the reset gate, respectively. The ω_0 and ω_1 are weights functions representing the update and reset gates in the order given. Correspondingly, the b_0 and b_1 represents the bias vectors for reset and update gates. Where $\widetilde{\xi}^{(t-1)}$ is the input of the current layer and the output of the prior layer. The recurrent unit's candidate activation function is written as

$$\widetilde{\xi}^{(t)} = tanh\left(\omega_0\left[\varsigma_0 \times \widetilde{\xi}^{(t-1)}, x^{(t)}\right] + b_0\right) \tag{6}$$

where, $\widetilde{\xi}^{(t)}$ represents the candidate activation function, ω_0 is the activation functions weight, the bias vector is b_0 and $x^{(t)}$ is the inputs of the training data. One GRU unit's output is provided as

$$\xi^{(t)} = \left((1-\zeta_1) \times \widetilde{\xi}^{(t-1)}\right) + \left(\zeta_1 \times \xi^{(t)}\right) \tag{7}$$

where, $\xi^{(t)}$ is the output of a single GRU unit. The proposed algorithm uses a single-dimensional layer with the convolution operation represented as

$$h_1 = convblock1(\xi) \tag{8}$$

$$h_2 = convblock2(h_1) \tag{9}$$

$$h_3 = convblock3(h_2) \tag{10}$$

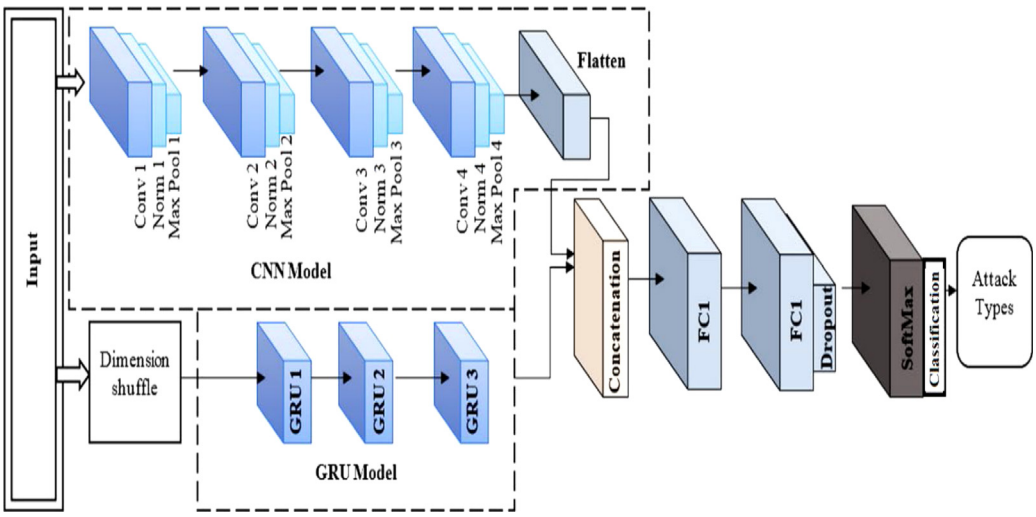


Fig. 2. Process flow of proposed intrusion-detection system model.

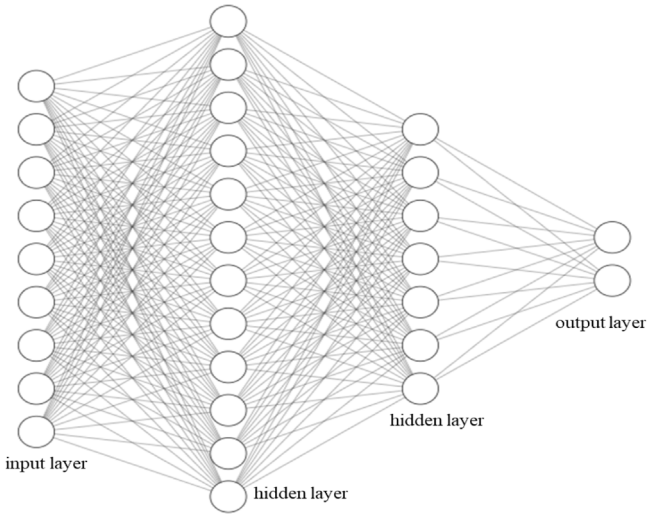


Fig. 3. Illustrations of a feed-forward multilayer perceptron.

$$h_4 = convblock4\,(h_3) \tag{11}$$

The hidden vectors are h_1, h_2, h_3, and h_4 respectively. A normalization layer is fixed next to the convolutional layer to speed up training. By using the pooling layer, the features map is downsampled by summarizing the presence of features in patches of the feature map, hence reducing the dimension of the features. The main pooling techniques are average and max pooling. The average pooling determines the average value of the patches of the features map. The average pooling at the pooling layer is given as

$$\Psi^n = P_{avg}\ \left(\psi^{n-1}\right) \tag{12}$$

where ψ^{n} represents the pooling layers, and output and $\psi^{\mathrm{n-1}}$ represent previously acquired values from the convolution layer. The pooling layers are denoted by n and the flattening layer is mounted to convert the data into a one-dimensional vector.

$$L = flatten\,(h_4) \tag{13}$$

$$c_t = concate\,(K, L) \tag{14}$$

Table 1
Dataset considered for the simulation.

Type	Total	Training set	Test set	Label
BENIGN	67,343	53 874	13 469	0
DDoS	45,927	36 742	9185	1

The outputs from the GRU's K, and the outputs from the CNN's L, are concatenated as written in Eq. (14). The normalized exponential function (SoftMax) $\hat{y}: \mathbb{R}^{c_t} \rightarrow \{0, 1\}$ is written when c_t is greater than 1 as

$$\hat{y}(z)_i = \frac{e^{z_i}}{\sum_{n=1}^{c_t} e^{z_n}} \tag{15}$$

For $i = 1, 2,\ldots, c_{\mathrm{t}}$ and $\mathbf{z} = (z_1, z_2,\ldots,\mathrm{zc}_{\mathrm{t}}) \in \mathbb{R}^{c_t}$. Where $\mathbf{z}$ is the input vector taken from the c_t. The loss function for the proposed model assessment is the cross-entropy function (Graves & Schmidhuber, 2005), which is given as

$$E_p\,(l) = -\frac{1}{b}\sum_{i=1}^{n} y_i\, log_2\, y_i' \tag{16}$$

b is for the batch size given, whilst n represents the training sample size, the actual value is represented by y_i and it is y_i' for the predicted value.

3.3. Description of dataset

The simulation evaluation phase of our proposed model is carried out using the CICIDS-2017 (Radoglou-Grammatikis & Sarigiannidis, 2018) dataset, specifically, the *Friday WorkingHours Afternoon DDos* dataset (Sharafaldin, Habibi, & Ghorbani, 2018) which is publicly accessible and utilized by related studies in the cyber security community. The *benign* and most recent common attacks such as *DDoS* are included in the CICIDS-2017 dataset, which closely reflects data from the actual world. Additionally, it contains the outcomes of the CICFlowMeter network traffic analysis with flows categorized according to the source, timestamp, destination IP addresses, destination ports, protocols, and attacks. The features present there in the dataset are shown in Table 1.

Cleaning up the data and replacing not a number (NaN) and infinite fields with the column's mean value are the first steps in the preprocessing stage. The features are converted to numerical features and integrated with already-existing numerical features

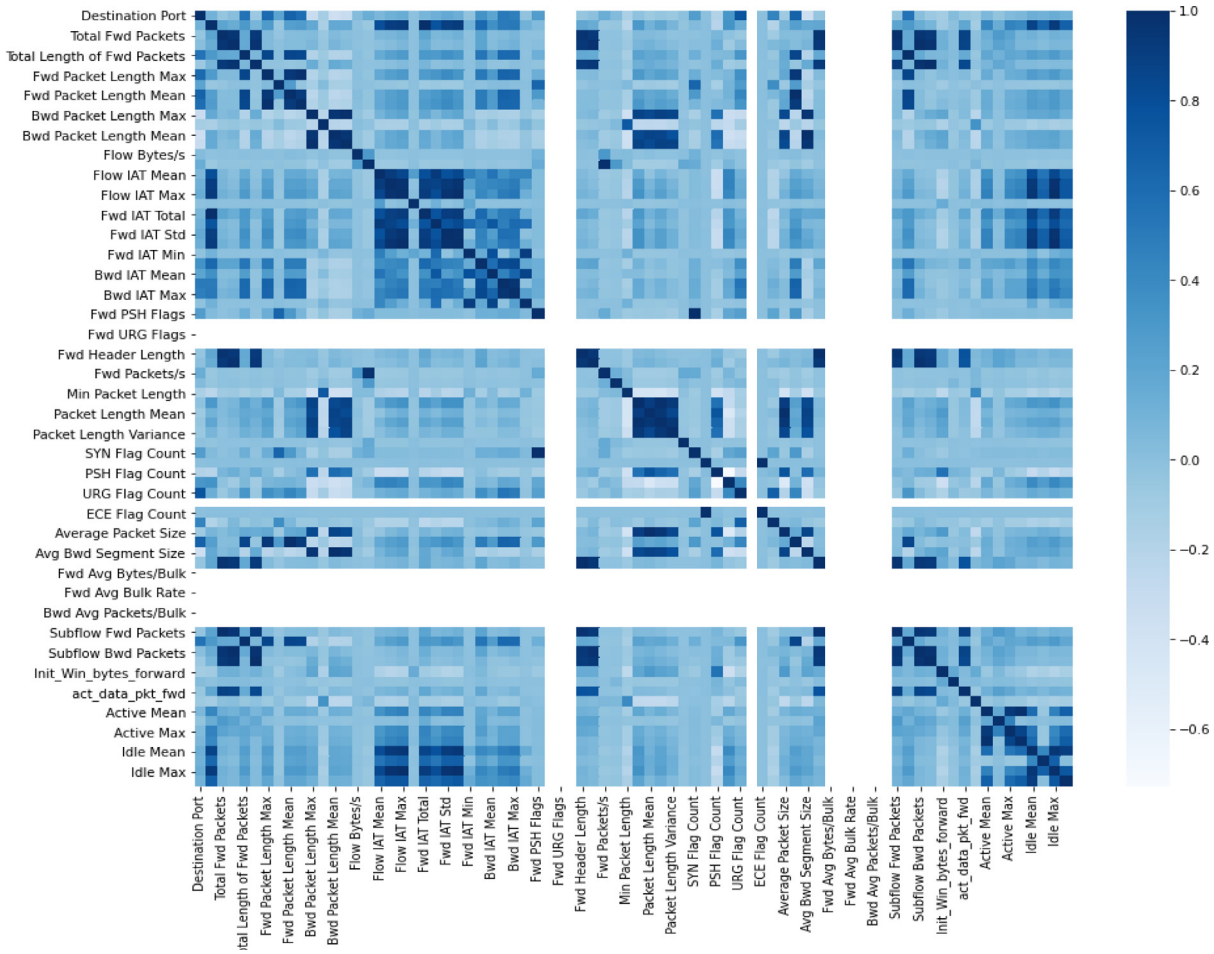


Fig. 4. The correlation heatmap for the employed dataset.

in the dataset. Additionally, the labels in the dataset are numerically processed so that the two labels in the dataset, *benign* is represented by 0, and *DDoS* is represented by 1. The dataset is equally mapped and normalized in order to lessen the feature discrepancies. The uniform mapping interval range is [0, 1]. Since there are no irrelevant characteristics in the dataset and the dataset contains correlated features as shown in the correlation matrix in Fig. 4, feature selection was not used in the study. Therefore, the model's decision-making was influenced by all of the available features.

The list in Table 1 is the results after the normalization had been performed on the data set and therefore all the character features had been converted to their numerical values. Then, the data set is split into a training set and a testing set in a 70:30 ratio. The training is done using 70 percent of the data, and the validation and testing are done using the remaining 30 percent of the data.

The four fundamental characters that make up the confusion matrix are utilized to specify the classifier's measurement parameters. They are as follows: True Positive (TP) describes an algorithm's accurate prediction that is accurate. Also, the True Negative (TN) designates a truly negative prediction made by the algorithm that is negative. False Positive (FP) describes situations where the algorithm predicted a positive class but the actual class is negative. False Negative (FN) is a label that was predicted by the algorithm to be negative but is actually positive. An algorithm's performance measurements are its accuracy, precision, recall, and f1-score. These scenarios are mathematically represented as in Albulayhi and Sheldon (2021), Khoei, Aissou, Hu, and Kaabouch (2021), Peng et al. (2019), Radoglou-Grammatikis and Sarigiannidis (2018), Sharafaldin et al. (2018) and Siniosoglou, Radoglou-Grammatikis, Efstathopoulos, Fouliras, and Sarigiannidis (2021) and written in subsequent equations as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

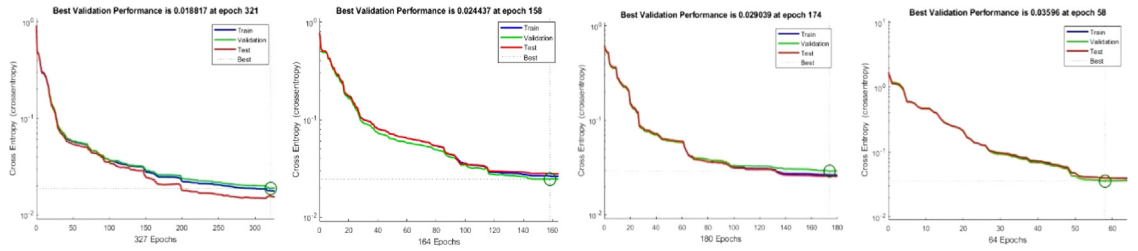
$$Precision = \frac{TP}{TP + FP} \tag{18}$$

$$Recall = \frac{TP}{TP + FN} \tag{19}$$

$$F1score = \frac{2(precision \times recall)}{(precision \times recall)} \tag{20}$$

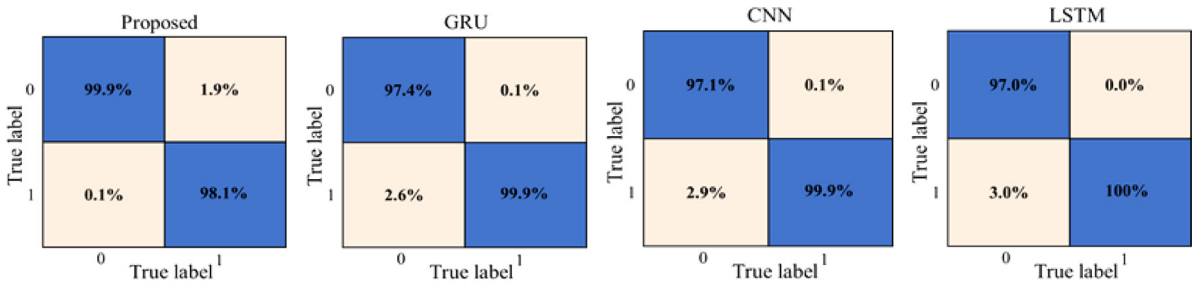
4. Results and analysis

The simulation results of our proposed algorithm are all contained in this section. Figures representing each outcome are presented step-by-step along with explanations of the findings. We give a succinct explanation of our proposed algorithm's performance and comparisons to that of some of its main contestants such as CNN, GRU, and LSTM. The heatmap depicts the correlation matrix between the target variable and the input features, including the destination port, flow bytes, forward header length, subflow forward packet, active mean, minimum packet length, packet length mean, packet length variance, average packet size, active max, ideal mean, ideal max, etc.



a. Proposed algorithm. **b.** GRU. **c.** CNN. **d.** LSTM

Fig. 5. Convergence ability of the considered algorithms.



a. Proposed algorithm. **b.** GRU. **c.** CNN. **d.** LSTM

Fig. 6. The confusion matrices..

Table 2
The configuration of the hyperparameters.

Number	Parametric	Quantity
1.	Input layer	78
2.	Hidden layer	55
3.	Activation function	ReLU
4.	Iteration limit	1000
5.	Cost function	Cross entropy
6.	Batch size	128

A heat map is a graphic representation of a two-dimensional tabular representation of multivariate data that is set up as a matrix. The heat map shows the relationships between several numerical variables, which can be used to identify patterns and anomalies. It helps to find characteristics that are best for developing machine learning models and transforms the correlation matrix into a color designation. It generates color coding from the correlation matrix and the correlation matrix shows the relationships between the variables on a scale from a perfect positive correlation to a perfect negative correlation with the perfect positive correlation showing the association between the variables. Each cell represents a square region of space in a certain measuring distance, and the colors signify the intensity of the investigated event that occurred on each mapping cell. A heat map provides a visual representation of data and facilitates the understanding of large data sets. A range of values is represented by various colors in a two-dimensional tabular depiction of the data.

Further simulations are run with the hyperparameters settings in Table 2. The proposed algorithm's convergence ability outperforms that of the other comparative algorithms. The algorithm's best validation performance is achieved at 0.018817 at epoch 321. The GRU is the next best-performing algorithm, with the best validation performance at 0.024437 on the 158th epoch. The CNN algorithm also outperformed the LSTM algorithm, achieving the best validation performance of 0.029039 at the 174th epoch, while the LSTM achieved its best validation performance of 0.03596 at an epoch of 58 (see Fig. 5).

The confusion matrices of the performance of the algorithms are depicted in Fig. 6a, b, c, and d. A confusion matrix is used to evaluate the algorithms based on parameters such as accuracy, precision, recall, and the false positive rate (Aldossary et al., 2021).

The error histograms are depicted in Fig. 7 to determine the error between the predicted and target values. Bins are the vertical bars seen on the graph. The total error range is divided into 20 smaller bins on the x-axis. The Y-axis represents the number of samples from the input dataset that fall into a given bin. On the plot, the midpoint bin corresponds to an error of 0.01599, the height of the bin for the training dataset is below 2×10^4 and the height of the bin for validation is between a little below 2×10^4 and halfway above 2×10^4. The test dataset is halfway between 2.5×10^4 and 2×10^5.

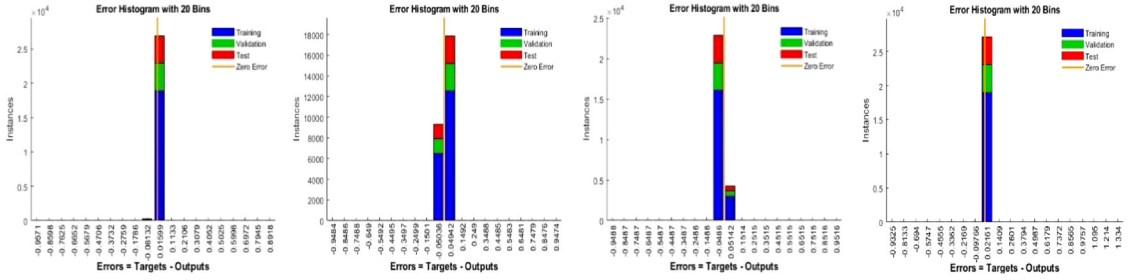
In terms of overall accuracy, precision, recall, and f1-score, Fig. 8 shows how well the proposed algorithm performed against the other algorithms Simulation results show that the proposed algorithm achieves accuracy, precision, recall, and f1-score, of 99.7%, 98.1%, 99.9%, and 98.9%, respectively. The GRU achieves an accuracy of 98.6%, precision of 99.5%, recall of 97.4%, and an f1-score of 98.5. The accuracy of the CNN is 98.5%, the precision is 99.8, the recall is 97.3% and the f1-score is 98.5%. The LSTM obtains 98.5% accuracy, 99.9% precision, 97% recall, and an f1-score of 98% FPR. The proposed model outperformed the comparative algorithms in all categories except the recall category. This is a result of the algorithm's high value of the false positive (FP). Since the FP is a denominative factor in determining the recall, its higher value caused the recall of the proposed algorithm to drop (see Table 3).

5. Conclusion

Finding vulnerabilities in SCADA networks used by Smart Grids is a top research objective in the field of cyber security. However, it is very challenging to choose an efficient deep

Table 3
Comparison of algorithms.

The proposed algorithm is compared to the existing algorithms altogether							
Algorithms	Detection rate %	Precision %	F1-score	Accuracy %	Data	Year	Reference
ANN	96.18		96.9	96.94	Simulated data	2018	Subasi et al. (2018)
SVM	97.25		97.8	97.8	Simulated data	2018	Subasi et al. (2018)
K-NN	98.05		98.4	98.44	Simulated data	2018	Subasi et al. (2018)
Randon forest	98.67		0.98	98.94	Simulated data	2018	Subasi et al. (2018)
Feed-forward neural network	90.13	88	87.4	88.2	Power system attack	2021	Aldossary et al. (2021)
Hybrid Deep belief network GRU	93.5	93.57	93.68	94.14	Power system attack	2021	Aldossary et al. (2021)
Recommended Bi-LSTMIDS	99.89	95.89	95.94	95.93	Power system attack	2021	Aldossary et al. (2021)
Random forest				99.9	KDDCup'99	2019	Alhaidari and AL-Dahasi (2019)
Naïve Bayes				97.74	KDDCup'99	2019	Alhaidari and AL-Dahasi (2019)
Proposed scheme	100	99.9	99.9	99.9	MAWI and world cup traffic dataset	2022	Fouladi et al. (2022)
Random forest	94			94	CICDDoS 2019	2021	Khoei et al. (2021)
Naïve Bayes	87			77.1	CICDDoS 2019	2021	Khoei et al. (2021)
KNN	94.4			94.6	CICDDoS 2019	2021	Khoei et al. (2021)
Stacking	96			97.3	CICDDoS 2019	2021	Khoei et al. (2021)
Logistic regression	72.2		72.2	90.7	Distribution substation operational dataset	2021	Siniosoglou et al. (2021)
Decision tree	99.1		99.1	97.7	Distribution substation operational dataset	2021	Siniosoglou et al. (2021)
Multi-layer perceptron	73.3		73.3	91.1	Distribution substation operational dataset	2021	Siniosoglou et al. (2021)
Proposed algorithm	99.9	98.1	98.9	99.7	CICIDSS2017	2022	



a. Proposed algorithms. **b.** GRU. **c.** CNN **d.** LSTM

Fig. 7. Error histograms.

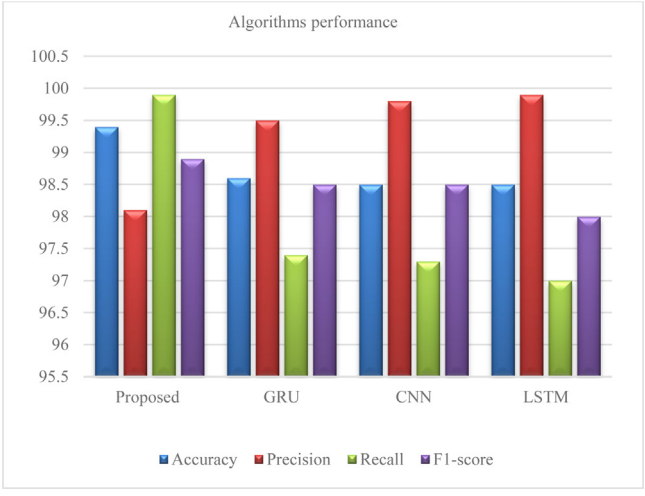


Fig. 8. Overall performance comparison of the considered algorithms.

learning-based intrusion detection algorithm. As a result, we proposed an algorithm for intrusion detection in Smart Grid, by hybridizing CNN and GRU algorithms. In evaluating the efficacy of our proposed algorithm, the accuracy, precision, recall, and f1-score, are evaluated to strengthen the SCADA system's security framework and make it more resistant to DDoS attacks. Using the CICIDSS2017 dataset, we carried out a thorough systematic simulation using MATLAB 2021a. We used the supervised machine learning approach after normalizing the data. Results demonstrate that the proposed algorithm can classify cyberattacks with a 99.7% accuracy and a detection rate of 99.9%, outperforming the accuracy and the detection rate of the comparative existing intrusion detection techniques. In general, the proposed algorithm can improve network intrusion detection performance.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Agarwal, A., Khari, M., & Singh, R. (2021). Detection of DDOS attack using deep learning model in cloud storage application. *Wireless Personal Communication*, http://dx.doi.org/10.1007/s11277-021-08271-z.

Ahakonye, L. A. C., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2021). Efficient classification of enciphered SCADA network traffic in smart factory using decision tree algorithm. *IEEE Access*, *9*, 154892–154901. http://dx.doi.org/10.1109/ACCESS.2021.3127560.

Al-Emadi, S., Al-Mohannadi, A., & Al-Senaid, F. (2020). Using deep learning techniques for network intrusion detection. In *2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT)* (pp. 171–176). http://dx.doi.org/10.1109/ICIoT48696.2020.9089524.

Albulayhi, K., & Sheldon, F. T. (2021). An adaptive deep-ensemble anomaly-based intrusion detection system for the internet of things. http://dx.doi.org/10.1109/AIIoT52608.2021.9454168, 0187-0196.

Aldossary, L. A., Ali, M., & Alasaadi, A. (2021). Securing SCADA systems against cyber-attacks using artificial intelligence. In *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 739–745). http://dx.doi.org/10.1109/3ICT53449.2021.9581394.

Alhaidari, F. A., & AL-Dahasi, E. M. (2019). New approach to determine ddos attack patterns on SCADA system using machine learning. In *2019 international conference on computer and information sciences* (pp. 1–6). http://dx.doi.org/10.1109/ICCISci.2019.8716432.

Almgren, M. (2018). Building a national testbed for research and training on SCADA security (short paper). In *13th international conference, CRITIS 2018, Kaunas, Lithuania*. Springer.

Almomani, I., Alkhayer, A., & El-Shafai, W. (2022). An automated vision-based deep learning model for efficient detection of android malware attacks. *IEEE Access*, *10*, 2700–2720. http://dx.doi.org/10.1109/ACCESS.2022.3140341.

Attia, M., Sedjelmaci, H., Senouci, S. M., & Aglzim, E.-H. (2015). A new intrusion detection approach against lethal attacks in the smart grid: temporal and spatial based detections. In *2015 global information infrastructure and networking symposium* (pp. 1–3). http://dx.doi.org/10.1109/GIIS.2015.7347186.

Chen, X., Zhang, L., Liu, Y., & Tang, C. (2018). Ensemble learning methods for power system cyber-attack detection. In *2018 IEEE 3rd international conference on cloud computing and big data analysis* (pp. 613–616). http://dx.doi.org/10.1109/ICCCBDA.2018.8386588.

Cherifi, T., & Hamami, L. (2018). A practical implementation of unconditional security for the IEC 60780 — 5 — 101 SCADA protocol. *International Journal of Critical Infrastructure Protection*, *20*, 68–84.

de Figueiredo, H. F. M., Ferst, M. K., & Denardin, G. W. (2019). An overview about detection of cyber-attacks on power SCADA systems. In *2019 IEEE 15th Brazilian power electronics conference and 5th IEEE southern power electronics conference (COBEP/SPEC)* (pp. 1–6). http://dx.doi.org/10.1109/COBEP/SPEC44138.2019.9065353.

Diaba, S. Y., Shafie-khah, M., & Elmusrati, M. (2022). On the performance metrics for cyber–physical attack detection in smart grid. *Soft Computing*, http://dx.doi.org/10.1007/s00500-022-06761-1.

Elgargouri, A., Virrankoski, R., & Elmusrati, M. (2015). IEC 61850 based smart grid security. In *2015 IEEE international conference on industrial technology* (pp. 2461–2465). http://dx.doi.org/10.1109/ICIT.2015.7125460.

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning algorithms for anomaly detection. In *2020 international conference on cyber security and protection of digital services (cyber security)* (pp. 1–8). http://dx.doi.org/10.1109/CyberSecurity49315.2020.9138871.

Farrukh, Y. A., Ahmad, Z., Khan, I., & Elavarasan, R. M. (2021). A sequential supervised machine learning approach for cyber attack detection in a smart grid system. In *2021 north American power symposium* (pp. 1–6). http://dx.doi.org/10.1109/NAPS52732.2021.9654767.

Fatani, A., Dahou, A., Al-qaness, M. A. A., Lu, S., & Abd Elaziz, M. (2022). Advanced feature extraction and selection approach using deep learning and aquila optimizer for IoT intrusion detection system. *Sensors*, *22*, 140. http://dx.doi.org/10.3390/s22010140.

Ferrag, M. A., & Maglaras, L. (2019). DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Transactions on Engineering Management*, *67*(4), 1285–1297.

Fouladi, R. F., Ermiş, O., & Anarim, E. (2022). A ddos attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN. *Computer Networks*, *214*, Article 109140.

Fu, R., Huang, X., Xue, Y., Wu, Y., Tang, Y., & Yue, D. (2019). Security assessment for cyber physical distribution power system under intrusion attacks. *IEEE Access*, *7*, 75615–75628. http://dx.doi.org/10.1109/ACCESS.2018.2855752.

Gao, J., Li, J., Jiang, H., Li, Y., & Quan, H. (2020). A new detection approach against attack/intrusion in measurement and control system with fins protocol. In *2020 Chinese automation congress* (pp. 3691–3696). http://dx.doi.org/10.1109/CAC51589.2020.9327136.

Graves, A., & Schmidhuber, J. (2005). Framewise phoneme classification with bidirectional LSTM and other neural network architectures. *Neural Networks*, *18*, 5–6.

Hai-He, T. (2018). Intrusion detection method based on improved neural network. In *2018 international conference on smart grid and electrical automation* (pp. 151–154). http://dx.doi.org/10.1109/ICSGEA.2018.00045.

Hosseinzadehtaher, M., Khan, A., Shadm, M. B., & Abu-Rub, H. (2020). Anomaly detection in distribution power system based on a condition monitoring vector and ultra- short demand forecasting. In *2020 IEEE CyberPELS (CyberPELS)* (pp. 1–6). http://dx.doi.org/10.1109/CyberPELS49534.2020.9311534.

Hu, C., Yan, J., & Liu, X. (2020). Adaptive feature boosting of multi-sourced deep autoencoders for smart grid intrusion detection. In *2020 IEEE power & energy society general meeting* (pp. 1–5). http://dx.doi.org/10.1109/PESGM41954.2020.9281934.

Huang, K., Li, S., Deng, W., Yu, Z., & Ma, L. (2022). Structure inference of networked system with the synergy of deep residual network and fully connected layer network. *Neural Networks*, *145*.

Ismail, et al. (2022). A machine learning-based classification and prediction technique for DDoS attacks. *IEEE Access*, *10*, 21443–21454. http://dx.doi.org/10.1109/ACCESS.2022.3152577.

Jaiganesh, V., Sumathi, P., & Mangayarkarasi, S. (2013). An analysis of intrusion detection system using back propagation neural network. In *2013 international conference on information communication and embedded systems* (pp. 232–236). http://dx.doi.org/10.1109/ICICES.2013.6508202.

Jiang, Y., Xu, A., Zhang, Y., Hong, C., & Cai, X. (2020). Anticipate fault sets generation methods for cyber physical power system considering cyber-attacks. In *2020 12th IEEE PES Asia-Pacific power and energy engineering conference* (pp. 1–5). http://dx.doi.org/10.1109/APPEEC48164.2020.9220404.

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, *84*, 225–238.

Khan, R. U., Zhang, X., Alazab, M., & Kumar, R. (2019). An improved convolutional neural network model for intrusion detection in networks. In *2019 cybersecurity and cyberforensics conference* (pp. 74–77). http://dx.doi.org/10.1109/CCC.2019.000-6.

Khoei, T. T., Aissou, G., Hu, W. C., & Kaabouch, N. (2021). Ensemble learning methods for anomaly intrusion detection system in smart grid. In *2021 IEEE international conference on electro information technology* (pp. 129–135). IEEE.

Komyakov, A. A., Erbes, V. V., & Ivanchenko, V. I. (2015). Application of artificial neural networks for electric load forecasting on railway transport. In *2015 IEEE 15th international conference on environment and electrical engineering* (pp. 43–46). http://dx.doi.org/10.1109/EEEIC.2015.7165296.

Koutsandria, G., Muthukumar, V., Parvania, M., Peisert, S., McParl, C., & Scaglione, A. (2014). A hybrid network IDS for protective digital relays in the power transmission grid. In *2014 IEEE international conference on smart grid communications (SmartGridComm)* (pp. 908–913). http://dx.doi.org/10.1109/SmartGridComm.2014.7007764.

Lee, J. M., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access*, *8*, 62954–62968. http://dx.doi.org/10.1109/ACCESS.2020.2983179.

Li, D., Guo, H., Zhou, J., Zhou, L., & Wong, J. W. (2019). SCADAWall: A CPI-enabled firewall model for SCADA security. *Computers & Security*, [ISSN: 0167-4048] *80*, 134–154.

Li, X., & Hedman, K. W. (2020). Enhancing power system cyber-security with systematic two-stage detection strategy. *IEEE Transactions on Power Systems*, *35*(2), 1549–1561. http://dx.doi.org/10.1109/TPWRS.2019.2942333.

Liang, H., Ye, C., Zhou, Y., & Yang, H. (2021). Anomaly detection based on edge computing framework for AMI. In *2021 IEEE international conference on electrical engineering and mechatronics technology* (pp. 385–390). http://dx.doi.org/10.1109/ICEEMT52412.2021.9601888.

Lin, W. H., Lin, H. C., Wang, P., Wu, B. H., & Tsai, J. Y. (2018). Using convolutional neural networks to network intrusion detection for cyber threats. In *2018 IEEE international conference on applied system invention* (pp. 1107–1110). http://dx.doi.org/10.1109/ICASI.2018.8394474.

Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power systems: A fast solution. *IEEE Transactions on Smart Grid*, *8*(2), 1023–1025. http://dx.doi.org/10.1109/TSG.2016.2623983.

Lopez Perez, R., Adamsky, F., Soua, R., & Engel, T. (2018). Machine learning for reliable network attack detection in SCADA systems. In *2018 17th IEEE international conference on trust, security and privacy in computing and communications/ 12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 633–638). http://dx.doi.org/10.1109/TrustCom/BigDataSE.2018.00094.A.

Mahmud, R., Vallakati, R., Mukherjee, A., Ranganathan, P., & Nejadpak, A. (2015). A survey on smart grid metering infrastructures: Threats and solutions. In *2015 IEEE international conference on electro/information technology* (pp. 386–391). http://dx.doi.org/10.1109/EIT.2015.7293374.

Mohan, S. N., Ravikumar, G., & Govindarasu, M. (2020). Distributed intrusion detection system using semantic-based rules for SCADA in smart grid. In *2020 IEEE/PES transmission and distribution conference and exposition (T & D)* (pp. 1–5). http://dx.doi.org/10.1109/TD39804.2020.9299960.

Oyewole, P. A., & Jayaweera, D. (2020). Power system security with cyber-physical power system operation. *IEEE Access*, *8*, 179970–179982. http://dx.doi.org/10.1109/ACCESS.2020.3028222.

Peng, Y. (2020). Application of convolutional neural network in intrusion detection. In *2020 international conference on advance in ambient computing and intelligence* (pp. 169–172). http://dx.doi.org/10.1109/ICAACI50733.2020.00043.

Peng, W., Kong, X., Peng, G., Li, X., & Wang, Z. (2019). Network intrusion detection based on deep learning. In *2019 international conference on communications, information system and computer engineering* (pp. 431–435). http://dx.doi.org/10.1109/CISCE.2019.00102.

Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2018). An anomaly-based intrusion detection system for the smart grid based on CART decision tree. In *2018 global information infrastructure and networking symposium* (pp. 1–5). http://dx.doi.org/10.1109/GIIS.2018.8635743.

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks*, *61*.

Sharafaldin, I., Habibi, A. L., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *ICISSP*.

Shum, J., & Malki, H. A. (2008). Network intrusion detection system using neural networks. In *2008 fourth international conference on natural computation* (pp. 242–246). http://dx.doi.org/10.1109/ICNC.2008.900.

Singh, V. K., Ebrahem, H., & Govindarasu, M. (2018). Security evaluation of two intrusion detection systems in smart grid SCADA environment. In *2018 north American power symposium* (pp. 1–6). http://dx.doi.org/10.1109/NAPS.2018.8600548.

Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Transactions on Network and Service Management*, *18*(2), 1137–1151. http://dx.doi.org/10.1109/TNSM.2021.3078381.

Subasi, A., et al. (2018). Intrusion detection in smart grid using data mining techniques. In *2018 21st Saudi computer society national computer conference* (pp. 1–6). http://dx.doi.org/10.1109/NCG.2018.8593124.

Sun, Y., Guan, X., Liu, T., & Liu, Y. (2013). A cyber–physical monitoring system for attack detection in smart grid. In *2013 IEEE conference on computer communications workshops (INFOCOM WKSHPS)* (pp. 33–34). http://dx.doi.org/10.1109/INFCOMW.2013.6970712.

Suppitaksakul, C., & Saelee, V. (2009). Application of artificial neural networks for electrical losses estimation in three-phase transformer. In *2009 6th international conference on electrical engineering/electronics, computer, telecommunications and information technology* (pp. 248–251). http://dx.doi.org/10.1109/ECTICON.2009.5137002.

Talha, B., & Ray, A. (2016). A framework for MAC layer wireless intrusion detection & response for smart grid applications. In *2016 IEEE 14th international conference on industrial informatics* (pp. 598–605). http://dx.doi.org/10.1109/INDIN.2016.7819232.

Ullah, I., & Mahmoud, Q. H. (2017). An intrusion detection framework for the smart grid. In *2017 IEEE 30th Canadian conference on electrical and computer engineering* (pp. 1–5). http://dx.doi.org/10.1109/CCECE.2017.7946654.

Valdes, A., Macwan, R., & Backes, M. (2016). Anomaly detection in electrical substation circuits via unsupervised machine learning. In *2016 IEEE 17th international conference on information reuse and integration* (pp. 500–505). http://dx.doi.org/10.1109/IRI.2016.74.

Vijayanand, R., Devaraj, D., & Kannapiran, B. (2019). A novel deep learning based intrusion detection system for smart meter communication network. In *2019 IEEE international conference on intelligent techniques in control, optimization and signal processing* (pp. 1–3). http://dx.doi.org/10.1109/INCOS45849.2019.8951344.

Xu, Y. (2020). A review of cyber security risks of power systems: from static to dynamic false data attacks. *Protection and Control of Modern Power Systems*, *5*, 19. http://dx.doi.org/10.1186/s41601-020-00164-w.

Yang, L., Liu, J., & Zhang, Y. (2019). An intelligent security defensive model of SCADA based on multi-agent in oil and gas fields. *International Journal of Pattern Recognition and Artificial Intelligence*, *34*, http://dx.doi.org/10.1142/S021800142059003X.

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Pranggono, B., & Wang, H. F. (2013). Intrusion detection system for IEC 60870 − 5 − 104 based SCADA networks. In *2013 IEEE power & energy society general meeting* (pp. 1–5). http://dx.doi.org/10.1109/PESMG.2013.6672100.

Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., & Mihet-Popa, L. (2020). Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access*, *8*, 151019–151064. http://dx.doi.org/10.1109/ACCESS.2020.3016826.

Zhao, J., Chen, M., & Luo, Q. (2011). Research of intrusion detection system based on neural networks. In *2011 IEEE 3rd international conference on communication software and networks* (pp. 174–178). http://dx.doi.org/10.1109/ICCSN.2011.6013688.