A Hybrid IDS using Machine Learning and Semantic Rules for Modern Power Systems to Detect Cyber-Attacks

MSc Research Project
Cyber Security

Harsh Dharmendra Patel
Student ID: X21141932

School of Computing
National College of Ireland

Supervisor: Prof. Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Harsh Dharmendra Patel		
Student ID:	X21141932		
Programme:	MSC in Cybersecurity	**Year:**	2022-2023
Module:	Research Project		
Supervisor:	Mr. Jawad Salahuddin		
Submission Due Date:	1st February 2023		
Project Title:	A Hybrid IDS using Machine Learning and Semantic Rules for Power System to Detect Cyber-Attacks		
Word Count:	**7353**	**Page Count : 21**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Harsh Dharmendra Patel

Date: 31st January 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Hybrid IDS using Machine Learning and Semantic Rules for Modern Power System to Detect Cyber-Attacks

Harsh Dharmendra Patel
X21141932

Abstract

The evolution of power systems into modern power systems or smart grids has provided a huge benefit. Smart grids have made the working and operation of the power grids more efficient but a major problem that accompanies this shift is the unavoidable threat of cyber-attacks as the smart grids are connected to networks and like all networks, these are exposed to cyber-attacks. So, it is important to create a system that can detect cyber-attacks on smart power grid networks. In the approach proposed here intrusions or attacks in the smart power grid systems will be detected using machine learning algorithms and a second method which uses semantic rules for Intrusion detection system (IDS) to detect cyberattacks. The machine learning algorithms like Random Forest (RF), Decision Tree (DT) and Artificial Neural Networks (ANN) will be used for detecting intrusions in networks and semantic rule-based intrusion detection system (IDS) based on Snort tool will be used to detect network intrusions. A Snort tool is used hers as it can be used to setup rules for detecting any malicious activities in the network. The machine learning classifiers will be trained using the data in the NSL-KDD and Edge IIoT dataset. The important features from the dataset will be used for training the machine learning algorithms and these important features will be selected using the analysis of variance (ANOVA) feature selection technique. The performance of the machine learning classifiers will be evaluated by computing the accuracy and the performance of the Snort will be evaluated by generating attacks on the computing device in which the Snort is installed. The machine learning algorithm with the best accuracy is used for creating a desktop application which is able to detect network intrusions based on the network features given as input. Two desktop applications will be created based on both datasets. It was observed from the results of this approach that the intrusions in smart power grid networks is effectively detected by both the machine learning classifiers and Snort.

Keywords- Intrusion Detection System, Machine Learning, Snort, Power Systems, Cyber-attacks.

1 Introduction

The power systems have naturally evolved from their traditional forms according to the changing times. A power system can be considered modern if it has a “smart” element attached to it. The smart power grids have a cyber-physical system (CPS) incorporated into them. Cyber and communication infrastructure are integrated with physical power distribution and transmission system to form the modern power system (Mohammadpourfard et al., 2021). Smart grids have helped in increasing the reliability of the power system and have made the power systems highly efficient. But being regularly connected to the internet for data communication has made the smart power grids susceptible to cyber-attacks (Shefaei et al., 2021). Two kinds of attacks can happen to a smart power system, cyber-attacks, and physical attacks. Each kind of attack have clearly defined objectives they are trying to accomplish (Majidi, Hadayeghparast and Karimipour, 2022). Physical attacks focus on the physical parts of the power grid for damaging and altering the working of the power grid and the network topology associated with the grid. The cyber-attacks mainly focus on several aspects like remote terminal units (RTUs), data communications infrastructure, supervisory control, and data acquisition (SCADA) systems and equipment connected to the internet and used for measuring (Figure (1)). The cyber-attacks affect the working of the power grid by fooling the network operators (Konstantinou et al., 2021).

The cyber-attacks are very dangerous and may compromise the entire working of the grid, and these power grids may be highly important as they may be responsible for providing energy to many people and industries. There have been many instances in the past that have demonstrated the devastating effects of cyber-attacks on power grids. A cyber-attack by the USA on a gas pipeline software in Siberia resulted in a huge explosion(Musleh, Chen and Dong, 2019). A Slammer worm attacked the David-Besse nuclear plant's control system which resulted in the display of the control system not functioning for 5 hours(F. Pasqualetti, F. Dorfler and F. Bullo, 2015). The Stuxnet was also a highly dangerous worm that attacked the Siemens SCADA located in the USA. it also attacked the nuclear plants in Iran (MIDDLETON, A,2016). There are also different kinds of cyber-attacks that may be used for attacking a smart power grid. So, with the threat of a cyber-attack always looming and the significance of smart power grids in society, it is necessary to create a system to detect cyber-attacks in smart power grids for making the grids more secure for ensuring their proper working.

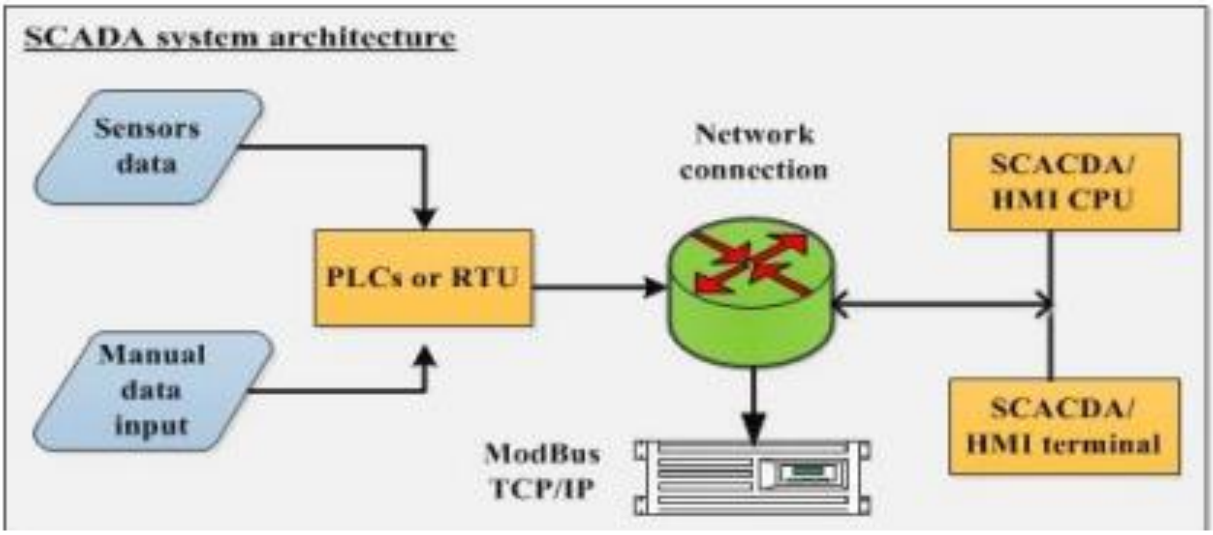

Figure (1): Basic architecture of SCADA systems (Keshk et al., 2017).

Intrusion detection systems (IDS) have been designed based on a number of techniques for detecting intrusions in networks and one major technique based on which IDS' have been developed is machine learning. Machine learning has proven to be an effective technique in detecting intrusions in networks (Buczak and Guven, 2016; Xin et al., 2018; Agrawal and Agrawal, 2015). For detecting cyber-attacks or intrusions in a network, machine learning models can be trained using data associated with networks and network intrusions or cyber-attacks. These trained models will be able to find out if an intrusion has occurred in the network based on the values of the attributes or the features associated with networks. Another technique frequently used for detection is the identification of network intrusions based on semantic rules. One such network IDS(NIDS) is Snort (Sagala, 2015). It is classic NIDS which is open source and has the capability to perform network traffic analysis and packet logging in real-time in computer systems connected to a network by utilizing content matching, searching and protocol analysis (Aickelin, Twycross and Roberts, 2007; Tasneem, Kumar and Sharma, 2018). The Snort has also proven to be very effective in detecting cyber-attacks in networks in real-time So, for providing security to smart power grid systems that uses machine learning and Snort separately can be used for detecting cyber-attacks.

1.1 Research question

- Will machine learning techniques and semantic rules be effective in detecting cyber-attacks in smart power grids?
- How will the performance of the machine learning model and semantic rules-based system in detecting cyber-attacks in smart power grids be evaluated?

1.2 Aims

- Create a system that uses machine learning models for detecting cyber-attacks in networks.
- Implement semantic rules in Snort for detecting cyber-attacks in a device connected to a network.
- Create a desktop application that is able to detect cyber-attacks in networks based on the network features.

The following sections make up the report:

‘Introduction’: The background details about the need for an intrusion detection system in smart power grids, the research questions, and aim will be provided in this section.

‘Literature review’: The literature related to the existing systems that perform intrusion detection based on machine learning models and snort will be studied here.

‘Methodology’: The data collected and used in this approach, the techniques used for processing the data, and other major methods for the development of the system will be discussed in this section.

‘Design and implementation: The specifications of the frameworks used in this approach and the implementation details of the final form of the system developed here will be discussed in these sections.

‘Evaluation’: The results obtained from the NIDS developed here will be discussed here.

‘Discussion’: The main findings revealed from the results will be discussed here.

‘Conclusion and future enhancement’: The concluding details about the NIDS developed here will be discussed in this section. The main methods used, and the results obtained will be discussed. The enhancements that can be made to the system in the future will also be discussed in this section.

2 Related Work

IDS based on machine learning models, Snort, and existing IDS in smart power grids will be studied here.

2.1 IDS using machine learning and Snort

A NIDS that uses the two-stage classifier based on the RepTree algorithm and protocols subset is proposed in (Belouch, El and Idhammad, 2017). The NSL-KDD and UNSW-NB15 data sets were used in this approach. A multiclass algorithm is then used for detecting the type of attack found in the anomalies. Feature extraction was performed here and an accuracy of 89.85% when the NSL-KDD data set was used. It was observed from this approach that the feature selection was effective in decreasing the training time of the model and improving its accuracy. The NSL-KDD dataset was used in this approach and is found to be effective as the machine learning models achieve good accuracy in intrusion detection. The main limitation of this approach is that the classifications made by the system for the UDP, and other protocols were not accurate.

The performances of Naïve Bayes, Support vector machine (SVM), Random Forest (RF), and Decision Tree (DT) in detecting network intrusions are evaluated in (Belouch, El Hadaj, and Idhammad, 2018). The UNSW-NB15 dataset is used in this approach, and it was observed from the results of this approach that the RF classifier showcased the best performance with an accuracy of 97.49%. The main limitation of this approach is that the time for training taken by the models is greater as no feature selection method was used in this approach.
The importance of the accuracy of a machine learning model in intrusion detection was discussed in (Ahmad et al., 2018). The approach determined the accuracy for evaluating the performances of the SVM, extreme learning machine (ELM), and RF in detecting network intrusions. The NSL-KDD data was used in this approach, and it was found that the ELM showcased the best performance as it achieved an accuracy of 99.5 %. The main limitation of the approach is that only three machine learning models are used in this approach and more effective machine learning models which may have a better performance than ELM are not considered.

Different classes of intrusions were detected using machine learning algorithms in (Zala et al., 2020). The NSL-KDD dataset was used in this approach and feature selection was performed so that the training time of the machine learning models decreased. The SVM, Naïve Bayes (NB), RF, decision tree(DT), k-nearest neighbour (knn), and logistic regression (LR) was used in this approach, and it was found that the knn exhibited the best performance with an accuracy of 86%. The effectiveness of the machine learning models in detecting intrusions are gain evident from the results of this approach. The main limitation of this approach is that it could only find out the best machine learning model in intrusion detection by comparing six models and no new findings were revealed from the study.

Ensemble learning was used for the development of an intrusion detection system in (Shakeela,s et al., 2020). The DT classifier was used in this approach and the feature selection was performed using the Analysis of Variance (ANOVA) F-test. The accuracy of the DT for detecting different kinds of network intrusions were computed separately and it was found that the system developed here achieved an accuracy of 99.64% in detecting the DoS, 99.56% in detecting the Probe, 97.92% in detecting the R2L and 99.64% in detecting the U2R attacks. This approach shows that the ANOVA technique is effective for selecting important features in IDS. The main limitation of this approach is that it is not able to detect unknown attacks in a network and the system is not able to handle a large number of features, also the significance of the features was not explored in this approach.

An IDS was developed using the Artificial Neural Network (ANN) in (P and D, 2010). The KDD cup 99 dataset is used in this approach. The detection is performed in two different ways in this approach. In the frits approach the ANN is trained using the feature selected using the Mutual information(MI) method and in the second approach, the ANN is trained using the reduced features. The accuracies of both the approaches are computed and it is observed that the ANN-MI approach achieves an accuracy of 99.98% when the ANN is trained using the features selected by the MI method and when the feature reduction is used, it achieves an accuracy of 81.57%. The main limitation of the approach is that it has not provided significant findings to prove that it is suitable for real-time applications even though it has been stated in the literature that the system developed was suited for real-time applications.

An intrusion detection and prevention system(IDPS) based on Snort was proposed in (Tasneem, Kumar and Sharma, 2018). The effectiveness of the Snort in detecting intrusions in a network is discussed in this approach. The main limitation of this approach is that it does not specify or define any methods for computing the detection rate or FPR when the Snort is used for intrusion detection.

The Snort is used as a tool for intrusion detection in (Gaddam and Nandhini, 2017). A level-based architecture was proposed in this approach for detecting unknown and known attacks. The effectiveness of the architecture proposed in this approach is proved by integrating the architecture with the help of Snort using Code refactoring. The main limitation of this approach was that the other techniques for improving the efficiency of the IDS based on Snort were not discussed in this approach.

2.2 Intrusion detection in modern power systems

Machine learning algorithms were used for detecting False Data Injection Attacks (FDIA) occurring in smart grids (Kumar, Saxena and Choi, 2021). Feature selection methods were used in this approach for achieving high accuracies in detection. A number of machine learning algorithms were used in this approach for determining the one with the best performance. From the results of this approach, it was seen that the highest accuracy was achieved by the RF with an accuracy of 92% when the machine learning algorithm is trained using the train-test split method.

Malicious network traffic in SCADA was detected using machine learning methods in (Maglaras and Jiang, 2014). The One-class SVM(OCSVM) is used in this approach for detecting intrusions and the algorithm does not use any labels or information about the kind of anomaly that it has to expect for detection. It can be observed from the results of this

approach that the system achieves an accuracy of 98.87% in detecting intrusions. The main limitation of the approach is that the effectiveness of the system against network attacks like Man in the Middle (MITM), honeypot, and SYN Flooding is not evaluated in this approach.
Intrusions are detected in a power grid as multiple-class, trinary-class, and binary-class using the system proposed in (Yu et al., 2022). The ANN is used in this approach for detecting intrusions and the Gray wolf algorithm (GWA) is used for evolving the training of the ANN. The dataset used in this approach is from the Mississippi State Laboratory in the United States. The system is observed to achieve an accuracy of 96% in detecting multi-class attacks. It was revealed from the results of this approach that the ANN was highly effective in detecting network attacks in power grids.

Attacks on Cyber-Physical Power Systems (CPPS) are detected using physical and cyber data fusion using a data link in (Wang et al., 2021). The two-step principal component analysis (PCA) is used for the classification of the operating status of the system. The classification is performed in this approach using the cost-sensitive gradient boosting decision tree (CS-GBDT). The normal operation of the system is identified at an accuracy of 99% and the improper operation is identified at an accuracy of 98%. The main limitation of this approach is that it is not able to detect attacks in real-time.

Cyber-attacks in power systems were detected using machine learning algorithms in (Borges Hink et al., 2014). Data from 15 datasets that contained data that belonged to different kinds of attacks were used in this approach. There are some limitations associated with this approach the first one is that the results of the approach were not evaluated using a very large set of data. The approach also does not study the methods for training the models, methods for generating data with labels etc.

An approach for detecting FDIA is proposed in (Yang et al., 2018). The system uses one-Class SVM, Isolation forest, Robust covariance, and Local outlier factor methods based on machine learning for detecting the intrusions. From the results of the approach, it can be seen that the best accuracy is achieved by the one-Class SVM with an accuracy of 99.03% when the contamination rate is 0.1 and when the contamination rate is 0.2 the best performance is achieved by the Robust Covariance with an accuracy of 95.79%. The main limitation of this approach is that the density of data used in this approach has led to the results of the approach being misrepresented.

The role of the Industrial Internet of Things (IIoT) in developing smart grids is defined in (Yao et al., 2019). In this approach, the machine learning algorithms NB, LR, DT, RF, and LightGBM are used for detecting intrusions. The highest accuracy is achieved by the LightGBM with an accuracy of 93.2%. From the results of this study, the data from the IIoT can be considered as the data from the modern power system as it is used for creating power grids. The main limitation of this approach is that it only focuses on intrusion detection IIoT-based power grids or environments and no other kinds of modern power grids or systems.
Hybrid classifiers for intrusion detection in smart grids (Song et al., 2021). The NSL-KDD dataset is used in this approach and is observed to be very effective for training classifiers for detecting intrusions in power grids. The long short-term memory(LSTM) and extreme gradient boosting(XGBoost) classifiers are used in this approach.

The signature-based rules from Snort and Quickdraw were used for evaluating cyber security in SCADA in (Vávra and Hromada, 2016) . The rule-based intrusion detection of the Snort was found to be effective in detecting intrusions in SCADA based on the results of the approach in (Craig Valli , 2009). The Snort was again found to be effective in detecting intrusions in SCADA networks. The honeypot technologies were also used along with the Snort in this approach.

2.3 Summary

From the study of the existing literature, machine learning algorithms are highly effective in the development of intrusion detection systems including intrusion detection in modern power systems. From the findings of the existing literature, Snort was also observed to be effective in detecting intrusions in normal networks and modern power systems. The NSL-KDD dataset was also observed to be effective in training machine-learning models for detecting intrusions in networks. It was observed from the findings of the approach that the data from the IIoT edge network can be considered identical to the data from smart power grids. The Snort was also observed to be highly effective in detecting intrusions in normal networks and SCADA networks.

From the studies of the existing literature, no significant research gap was observed between the system proposed here and the existing systems. But based on the literature studied here no approach used the Snort and machine learning algorithms for detecting intrusions in a modern power system, together, even though the Snort and machine learning algorithms are used separately in the approach proposed here. Also, no existing approach was observed to use the data from IIoT edge networks for training machine learning algorithms to perform intrusion detection in modern power grids. So, the system proposed here will use the data from the IIoT edge networks for training the machine learning algorithms to perform intrusion detection in modern power grids and the system will also use both the Snort and machine learning algorithms for detecting intrusions.

3 Research Methodology

3.1 Overall working

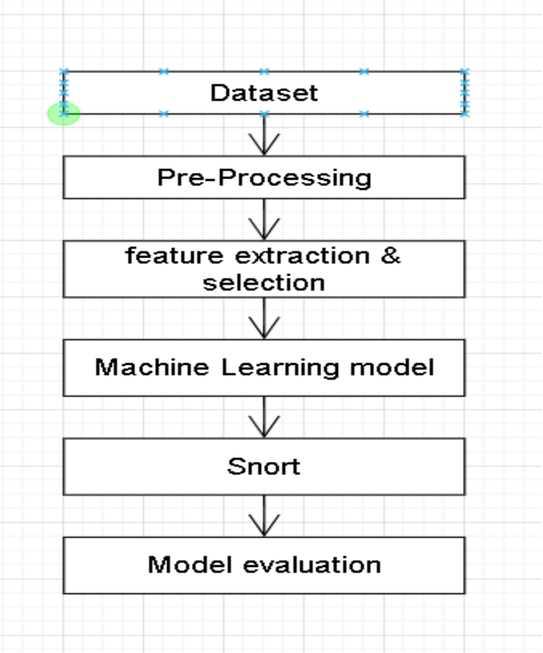

Figure (2): Research Structure.

The system developed here will be used for detecting attacks in a smart power grid network. The Snort and machine learning algorithms will be used separately for detecting the attacks in the network. The DT, RF, and ANN will be trained separately using the data in two different datasets, NSL-KDD and Edge IIoT, for detecting intrusions or attacks in the network, while the rules will be defined for the Snort for detecting attacks in networks. Both the machine learning algorithms and the Snort will be able to detect the attack and the type of attack on a network. The performance of the machine learning algorithms and Snort in detecting intrusions will be evaluated.

3.2 Dataset

The machine learning algorithms will be trained separately using the data in two different datasets. The two datasets used here are the NSL-KDD and Edge IIoT datasets.

3.2.1 NSL-KDD

The NSL-KDD dataset will contain different data which corresponds to different networks. The data will be the different features associated with the network and the label or class associated with the network. The dataset initially will not contain any column names that specify the type of feature values present in a particular column. The labels in the dataset either correspond to a normal network with the label 'normal' or a network in which a DDoS attack has occurred. The names of labels corresponding to the network in which the DDoS attack occurs will be denoted by the names of the subcategories of the DDoS attack.

3.2.2 Edge IIoT dataset

This dataset contains data from networks associated with IoT and IIoT applications. The data associated with the features of different networks will be present in the different columns and the labels or classes of the networks will be present in the column 'Attack_type'. The dataset contains data about a large number of networks in which different types of attacks have occurred and all of the attacks present in the dataset are not required for the system being developed here.

3.3 Pre-processing

The datasets are pre-processed so that both datasets are converted into a suitable form for training the machine learning algorithms.

3.3.1 NSL-KDD dataset

Column names must be added to the dataset so that the machine learning classifiers can learn what the data in a particular column represents. The rows of the dataset will represent the different networks and the columns of the dataset will represent the features corresponding to each network. The columns are names added to the columns in the dataset. The labels or classes of the networks will be present as string values and these values have to be converted to a numerical values. This is done to make sure that the training of the machine learning algorithms is effective as these algorithms perform better when handling numerical values. In this dataset, data associated with only normal networks and networks in which DDoS attacks have occurred is present. So, the labels which have the value 'normal' is replaced with 0 and all the other values of the labels are replaced with 1 as they represent DDoS attacks. The columns 'attack' and 'level' are dropped. Now columns other than the 'label' column will contain string values, so the string values in all these columns are replaced with numerical values.

3.3.2 Edge IIoT dataset

The unwanted columns are removed from the dataset. For developing the system proposed here only the labels 'DDoS_UDP', 'DDoS_ICMP', 'DDoS_HTTP', 'DDoS_TCP', 'MITM', and 'SQL_injection' representing different attacks, and the label 'normal' are required all the rows corresponding to labels other than these are removed. Now all the string values in the dataset are converted to numerical values. The labels are converted into numerical values in a way that all different sub-categories of the DDoS attacks are assigned the value 1, the 'MITM' attacks are assigned the value 2, the 'SQL_injection' is assigned the value 3, and the label with the value 'normal' is assigned the value 0. After this, the string or text values in all the other columns are also replaced with numerical values. Any remaining null values present in the dataset are also removed.

3.4 Feature selection

The best features from both datasets are selected for training the machine learning algorithms and the feature selection is performed using the ANOVA method. The best feature scores of the features in both the datasets are computed and the best 15 features from the NSL-KDD and the best 14 features from the Edge IIoT datasets are selected. Two new data frames (.CSV files) are created, one using the best 15 features from the NSL-KDD dataset and the other using the best 14 features from the Edge IIoT dataset.

3.5 Training machine learning algorithms

Before training the machine learning algorithms the data associated with features and labels from the two datasets will be separated and stored in two different variables. The data from the two datasets will also be split into a training set and a testing set. Before training the machine learning classifiers the data must be balanced and standardized. Data balancing is done because the data of one particular class in both datasets is greater than all the other classes. So, if the machine learning classifiers are training using this imbalanced data the output or the prediction by the machine learning classifiers will be biased towards the class that is greater in number in the dataset. The data balancing is performed using the 'SMOTE' technique. Standardization is performed on the data from making sure that the values of all the features lie in a common range because if the values of the different features lie in different ranges the smaller ranges of values tend to be overlooked by the machine learning algorithms and the results of the machine learning algorithms will be affected. So, standardization is performed using the 'Standard Scaler' technique.

After data balancing and scaling the data in the dataset are used for training the machine learning classifiers. The DT and RF classifiers are loaded and initialized while the ANN is created using different dense layers. Then all three classifiers are trained using the data in the dataset and the trained classifiers are saved.

3.6 Snort

IDS rules can be created in the Snort. Several rules for IDS are predefined in the Snort and among these pre-defined rules, the rule for detecting the DoS attack is already defined. The Snort is mainly used for detecting DDoS, SSH, and FTP attacks. Custom rules can also be defined for detecting attacks that are required apart from the predefined rules. The rules in the Snort are defined using the port number and IP address of the network which is sending data to the system in which the Snort is set up and the port number and IP address of the system in which the Snort is set up, the message that should be displayed as the alert when a particular attack occurs is also defined in the rules. The rules for detecting the different kinds of DDoS attacks are defined in the Snort. The rules for detecting the FTP and SSH are also defined. For the rule of the FTP, the port number of the system is defined as 21 and for the SSH attack, the port number of the system is defined as 22. The rules for the detection of the required attacks are defined in the Snort.

3.7 Evaluation of the machine learning classifiers and the Snort

The performances of the machine learning classifiers are evaluated by computing the accuracy achieved by each classifier in detecting the attacks in the smart grid networks. The performance of the Snort in detecting attacks will be evaluated based on the attacks created based on the different commands.

3.8 Salient features of the power system

The main reason we have studied the power system is that they consist of many other systems which can be vulnerable to cyberattacks. One of these systems is the SCADA system which is used for communication between power system and the other communication system such as remote computer. As it uses communication layer for communicating between the master which is power system and other remote computers, hence they are more vulnerable to cyberattacks. Therefore, snort tool can be useful for detection of these attacks.

4 Design Specification

The IDS based on the machine learning classifiers are implemented using Python. The RF classifier and DT classifier are loaded from the 'sklearn' library. The dense layer for creating the ANN architecture is loaded from the 'TensorFlow' or 'tf' library. The IDS will be created as a desktop application, and it will be designed and developed using the 'Tkinter' library. A separate desktop application has been created for both the dataset.

For setting up the Snort the Snort tool is installed in a computing device. Now for evaluating the performance of the Snort it has to be subjected to different kinds of attacks. Here, the same computing device will be used as the device which is attacked and the device which is performing the attack. This is achieved by installing Ubuntu and Kali Linux on a single computing device. The Snort will be installed on the Ubuntu OS and the attacks will be performed from the Kali Linux.

5 Implementation

The IDS created based on the machine learning classifiers is in the form of a desktop application. Two desktop applications will be created for the two datasets. Both desktop applications will consist of a login interface in which a default username and password are provided for logging in and reaching the interface where the intrusion detection takes place. Firstly, the desktop application developed based on the NSL-KDD will be discussed. The interface of the desktop application will consist of 15 spaces for providing inputs, these inputs correspond to the 15 features associated with the networks. The inputs are read and given as inputs to the machine learning classifier achieving the best accuracy when trained using the NSL-KDD dataset. If the values of the features given as input correspond to a network in which an attack has occurred, then the text 'DDoS Attack Detected' will be displayed and if the network is normal then the text 'Normal' will be displayed.

Now for the desktop application developed based on the Edge IIoT dataset. The interface of the desktop application will consist of 14 spaces for providing inputs, these inputs correspond to the 14 features associated with the networks. The inputs are read and given as inputs to the machine learning classifier achieving the best accuracy when trained using the Edge IIoT dataset. The system will display the type of attack detected based on the input values. The different attacks will be specified using the texts, ‘DDoS Attack Detected’, ‘MITM Attack Detected’, and ‘FDIA Attack Detected’ and if there is no attack ‘Normal’ will be displayed in the interface of the desktop application.

The Snort will be run on Ubuntu and the attacks will be generated from the Kali Linux on the same computing device the Snort on detecting the attacks will specify the kind of attack occurring on the network based on the alerts set for each kind of network when the rules are defined in the Snort.

6 Evaluation

6.1 Performance of the machine learning classifiers trained using NSL-KDD

The accuracies of the machine learning classifiers trained using the NSL-KDD dataset are computed.

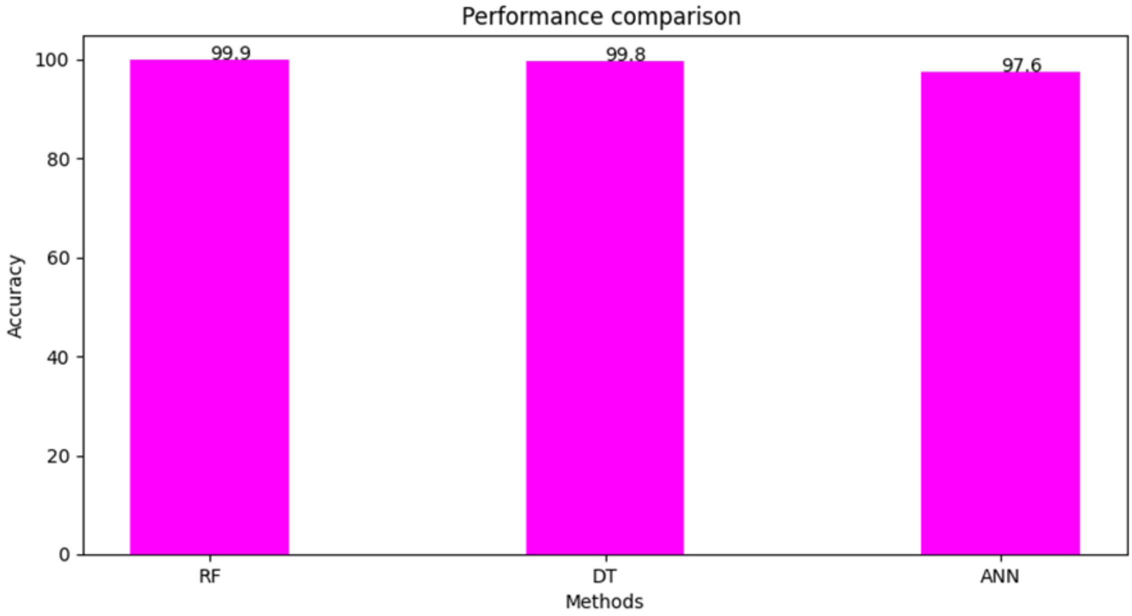

Figure (3): The accuracies achieved by the machine learning classifiers when trained using the NSL-KDD dataset.

It can be observed that the best accuracy is achieved by the RF classifier as it achieves an accuracy of 99.9%(Figure (3)).

6.2 Performance of the machine learning classifiers trained using Edge IIot dataset

The accuracies of the machine learning classifiers trained using the Edge IIoT dataset , are computed.

Figure (4): The accuracies achieved by the machine learning classifiers when trained using the Edge IIoT dataset.

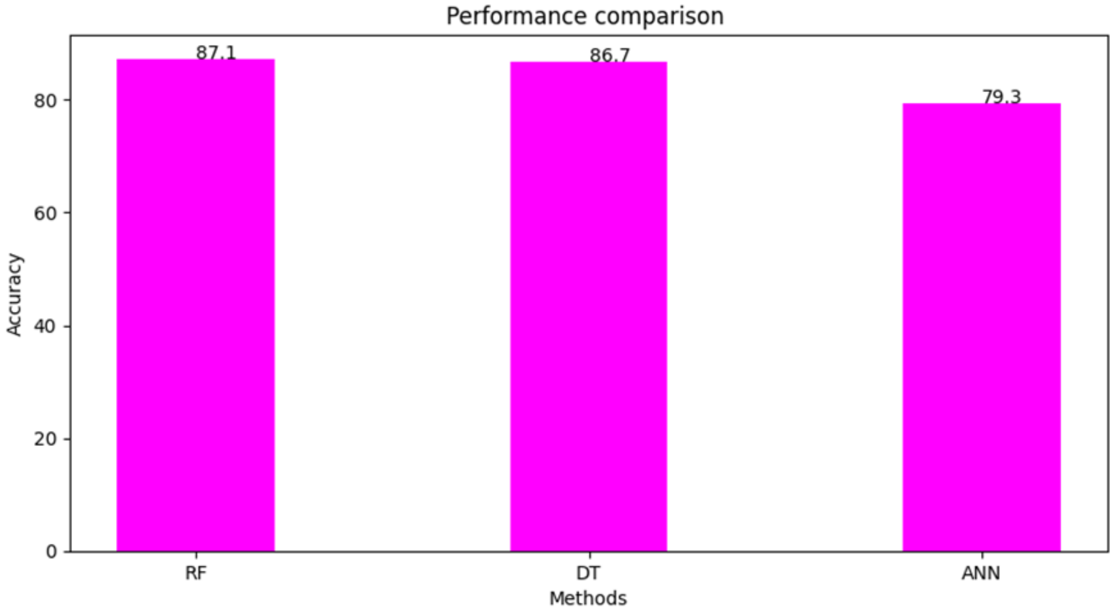

Figure (4): The accuracies achieved by the machine learning classifiers when trained using the Edge IIoT dataset.

It can be observed that the best accuracy is achieved by the RF classifier as it achieves an accuracy of 87.1%(Figure (3)).

6.3 Performance Metrics

This is used to detect the effectiveness of the given machine-learning techniques. This is done by evaluating many assessments in the two-dimensional matrix, which is represented by the confusion matrix.

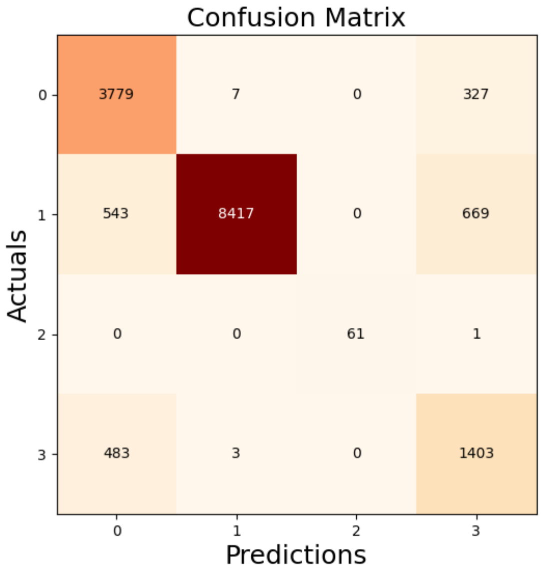

Figure (5): Confusion matrix of RF for Edge-IIoT dataset

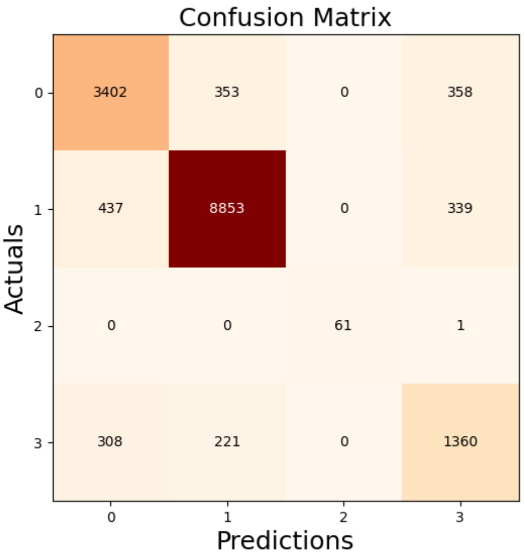

Figure (6): Confusion matrix of DT for Edge-IIoT dataset

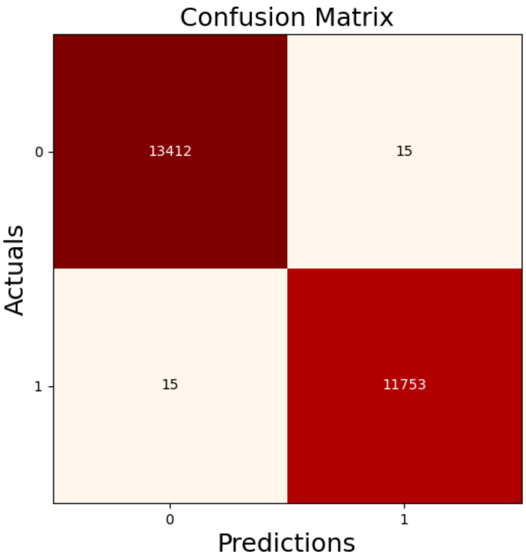

Figure (7): Confusion matrix of RF for NSL-KDD dataset

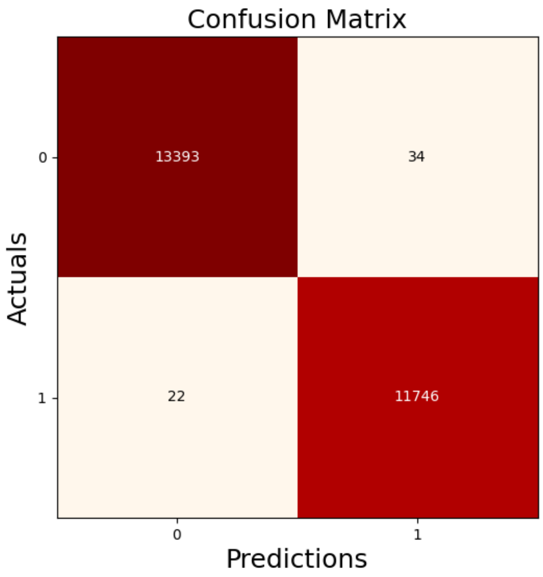

Figure (8): Confusion matrix of DT for NSL-KDDdataset

6.4 Accuracy

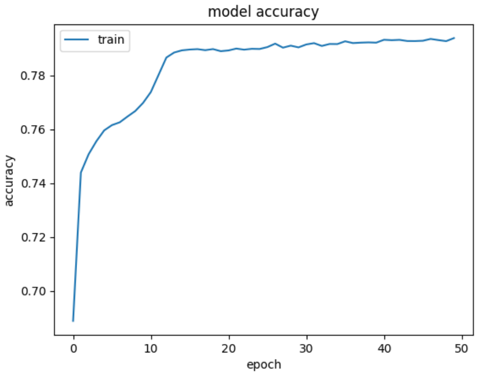

Figure (9): The model accuracy Edge-IIoT dataset

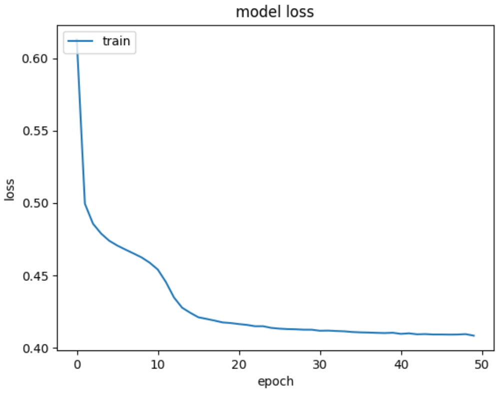

Figure (10): The model loss Edge-IIoT dataset

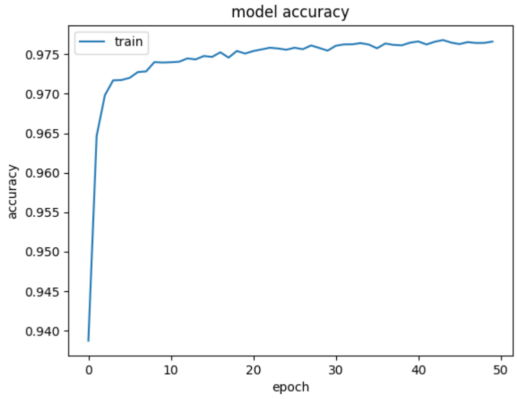

Figure (11): The model accuracy NSL-KDD dataset

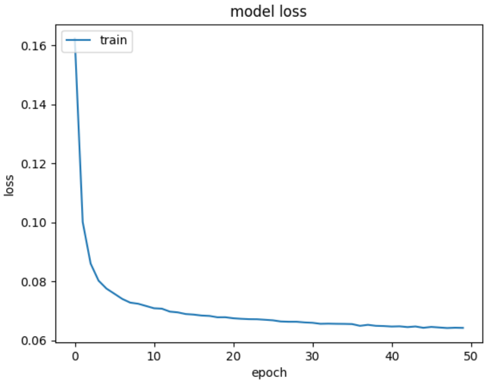

Figure (12): The model loss NSL-KDD dataset

6.5 Snort

The Snort is evaluated by using the command for generating the SSH, FTP, Ping, Nap, and DDoS attacks these attacks are generated from the Kali Linux and applied on the Snort installed in Ubuntu of the computer device.

Discussion

The findings from the existing literature revealed that machine learning algorithms are effective in detecting network intrusions from smart power grids which are supported by the finding from the results obtained here as the performance of the machine learning models in detecting attacks was effective on the data from both the datasets NSL-KDD and Edge IIoT although the performances of the machine learning classifiers were lower when using the data from the Edge IIoT this may be due to the presence different classes of intrusions present in the Edge IIoT dataset, it also may be due to the fact that the Edge IIoT dataset contained the data from the IoT and IIoT systems. The approach performed here is comparable to some of the existing literature studied here. It was observed from the results of Kumar, Saxena and Choi (2021) that RF is effective in detecting intrusions in power grids which is in line with the results of the approach here as the RF is observed to achieve the best performance. The findings from Maglaras and Jiang (2014) revealed that machine learning classifiers are effective in detecting intrusions which is in line with the approach proposed here. The finding from Yu et al. (2022) showed that ANN is effective in detecting intrusions in smart power grid networks this finding is partly supported by the findings from the approach performed here as the performance of the ANN was low when it was trained using the Edge IIoT dataset but the datasets used by Yu et al. (2022) is different from the Edge IIoT dataset which may be the reason for the performance of the ANN decreasing. The findings from Vávra and Hromada (2016) and Craig Valli (2009) showed the effectiveness of the Snort in detecting intrusions in SCADA networks which is supported by the results of the approach performed here but the Snort here was not tested in a SCADA network but the attacks normally occurring in the SACDA networks were detected by the Snort.

System	Accuracy (in %)
Kumar, Saxena and Choi, 2021	92%
Maglaras and Jiang, 2014	98.87%
Yu et al., 2022	96%
System developed here using NSL-KDD(RF)	99.9%

Table (1): The accuracies of the existing systems studied here and the system developed here

It can be observed that the system developed here achieves an accuracy greater than the existing systems studied here(Table (1)). The system has some limitations. One main limitation of the system is that the performance of the Snort is evaluated by using only a limited number of attacks that may occur on a smart power grid network. The performances of the machine learning classifiers are reduced when the classifiers are trained using the Edge IIoT dataset the underlying reason for this is also not explored in this approach.

7 Conclusion and Future Work

The system for detecting intrusions in smart power grid networks is successfully developed here. The first research question of this approach is answered here as the attacks in a smart power grid network are effectively detected by machine learning algorithms and Semantic rules-based system as the RF, DT, and ANN algorithms are able to detect the intrusions which has been shown by creating separate desktop application for both the dataset and the Semantic rules-based Snort is also able to detect intrusions effectively. The second research question is also answered as the performances of the machine learning algorithms were evaluated by computing the accuracy of the machine learning algorithms and the performance of the Snort was evaluated by simulating attacks on a computing device that contained the Snort. The machine learning algorithms were trained using the NSL-KDD data and the Edge IIoT dataset and it was observed that the best accuracy was achieved by the RF with values of 99.9% and 87.1% respectively for the NSL-KDD and Edge IIoT datasets.

In the future deep learning, methods can be used instead of machine learning methods for enhancing the performance of detecting intrusions in a smart grid network. The Snort can be evaluated by using more attacks based on the smart grid network for getting a better idea about its performance.

References

Agrawal, S. and Agrawal, J. (2015). Survey on Anomaly Detection using Data Mining Techniques. Procedia Computer Science, 60, pp.708–713. doi:10.1016/j.procs.2015.08.220.

Ahmad, I., Basheri, M., Iqbal, M.J. and Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. IEEE Access, 6, pp.33789–33795. doi:10.1109/access.2018.2841987.

Aickelin, U., Twycross, J. and Roberts, T.H. (2007). Rule generalisation in intrusion detection systems using SNORT. International Journal of Electronic Security and Digital Forensics, 1(1), p.101. doi:10.1504/ijesdf.2007.013596.

Belouch, M., El Hadaj, S. and Idhammad, M. (2018). Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Computer Science, 127, pp.1–6. doi:10.1016/j.procs.2018.01.091.

Belouch, M., El, S. and Idhammad, M. (2017). A Two-Stage Classifier Approach using RepTree Algorithm for Network Intrusion Detection. International Journal of Advanced Computer Science and Applications, 8(6). doi:10.14569/ijacsa.2017.080651.

Borges Hink, R.C., Beaver, J.M., Buckner, M.A., Morris, T., Adhikari, U. and Pan, S. (2014). Machine learning for power system disturbance and cyber-attack discrimination. 2014 7th International Symposium on Resilient Control Systems (ISRCS). doi:10.1109/isrcs.2014.6900095.

Buczak, A.L. and Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), pp.1153–1176. doi:10.1109/comst.2015.2494502.

F. Pasqualetti, F. Dorfler and F. Bullo.(2015).Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems. IEEE Control Systems, 35(1), pp.110–127. doi:10.1109/mcs.2014.2364725.

Gaddam, R. and Nandhini, M. (2017). An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. [online] IEEE Xplore. doi:10.1109/ICICCT.2017.7975177.

Keshk, M., Moustafa, N., Sitnikova, E. and Creech, G. (2017). Privacy Preservation Intrusion Detection Technique for SCADA Systems. [online] Available at: https://arxiv.org/ftp/arxiv/papers/1711/1711.02828.pdf [Accessed 5 Dec. 2022].

Kumar, A., Saxena, N. and Choi, B.J. (2021). Machine Learning Algorithm for Detection of False Data Injection Attack in Power System. 2021 International Conference on Information Networking (ICOIN). doi:10.1109/icoin50884.2021.9333913.

Maglaras, L.A. and Jiang, J. (2014). Intrusion detection in SCADA systems using machine learning techniques. 2014 Science and Information Conference. doi:10.1109/sai.2014.6918252.

Majidi, S.H., Hadayeghparast, S. and Karimipour, H. (2022). FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid. International Journal of Critical Infrastructure Protection, 37, p.100508. doi:10.1016/j.ijcip.2022.100508.

MIDDLETON, A. (2016). Stuxnet: The World's First Cyber... Boomerang? Interstate - Journal of International Affairs [Online], 2015/2016. Available: http://www.inquiriesjournal.com/a?id=1343

Mohammadpourfard, M., Genc, I., Lakshminarayana, S. and Konstantinou, C. (2021). Attack Detection and Localization in Smart Grid with Image-based Deep Learning. [online] Available at: https://arxiv.org/pdf/2110.11007.pdf [Accessed 3 Dec. 2022].

Mohammadpourfard, M., Khalili, A., Genc, I. and Konstantinou, C. (2021). Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. Sustainable Cities and Society, p.103116. doi:10.1016/j.scs.2021.103116.

Musleh, A.S., Chen, G. and Dong, Z.Y. (2019). A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. IEEE Transactions on Smart Grid, pp.1–1. doi:10.1109/tsg.2019.2949998.

P, G.K. and D, D. (2010). INTRUSION DETECTION USING ARTIFICIAL NEURAL NETWORK WITH REDUCED INPUT FEATURES. ICTACT Journal on Soft Computing, 1(1), pp.30–36. doi:10.21917/ijsc.2010.0005.

Sagala, A. (2015). Automatic SNORT IDS rule generation based on honeypot log. [online] IEEE Xplore. doi:10.1109/ICITEED.2015.7409013.

Shaikh Shakeela, N Sai Shankar, P Mohan Reddy, T Kavya Tulasi, and M Mahesh Koneru.(2020).Optimal Ensemble Learning Based on Distinctive Feature Selection by Univariate ANOVA-F Statistics for IDS.INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, VOL. 67, NO. 2, PP. 267-275. Available online: https://journals.pan.pl/Content/118896/PDF/39_2752_Shakeela_sk.pdf

Shefaei, A., Mohammadpourfard, M., Mohammadi-ivatloo, B. and Weng, Y. (2021). Revealing a New Vulnerability of Distributed State Estimation: A Data Integrity Attack and an Unsupervised Detection Algorithm. IEEE Transactions on Control of Network Systems, [online] pp.1–1. doi:10.1109/TCNS.2021.3091631.

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

Tasneem, A., Kumar, A. and Sharma, S. (2018). Intrusion Detection Prevention System using SNORT. International Journal of Computer Applications, 181(32), pp.21–24. doi:10.5120/ijca2018918280.

Tasneem, A., Kumar, A. and Sharma, S. (2018). Intrusion Detection Prevention System using SNORT. International Journal of Computer Applications, 181(32), pp.21–24. doi:10.5120/ijca2018918280.

Valli, Craig. (2009). Snort IDS for SCADA Networks.. 618-621. Available online : https://www.researchgate.net/publication/221200018_Snort_IDS_for_SCADA_Networks.

Vávra, J. and Hromada, M. (2016). Comparison of the Intrusion Detection System Rules in Relation with the SCADA Systems. Advances in Intelligent Systems and Computing, pp.159–169. doi:10.1007/978-3-319-33622-0_15.

Wang, L., Xu, P., Qu, Z., Bo, X., Dong, Y., Zhang, Z. and Li, Y. (2021). Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link. Frontiers in Energy Research, 9. doi:10.3389/fenrg.2021.666130.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 6, pp.35365–35381. doi:10.1109/access.2018.2836950.

Yang, C., Wang, Y., Zhou, Y., Ruan, J. and Liu, W. (2018). False Data Injection Attacks Detection in Power System Using Machine Learning Method. Journal of Computer and Communications, 06(11), pp.276–286. doi:10.4236/jcc.2018.611025.

Yao, H., Gao, P., Zhang, P., Wang, J., Jiang, C. and Lu, L. (2019). Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection. IEEE Network, 33(5), pp.75–81. doi:10.1109/mnet.001.1800479.

Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D. and Yang, C. (2022). An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning. Frontiers in Energy Research, 10. doi:10.3389/fenrg.2022.903370.

Zala, J., Panchal, A., Thakkar, A., Prajapati, B. and Puvar, P. (2020). Intrusion Detection System using Machine Learning. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp.61–71. doi:10.32628/cseit2062166.