e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

ATTACK CLASSIFICATION IN A POWER SYSTEM USING MACHINE LEARNING AND ARTIFICIAL NEURAL NETWORK

Uday Singh[*1], Robin Sharma[*2]

[*1]Masters Of Engineering In Computer Engineering, University Of Guelph, Guelph, Ontario, Canada.
[*2]Masters Of Engineering In Systems & Computing University Of Guelph, Guelph, Ontario, Canada.

ABSTRACT

Attacks to electricity grids need to be classified appropriately. Such classification offers the chance to determine the best steps to address them. Essentially, establishing rigid controls before attacks happen is deemed to be desirable. It contributes significantly towards reducing the general vulnerability of systems. According to the available data, this paper has classified the types of attacks into three categories (Attack, No Event, and Natural). We have achieved significant results using Machine Learning (ML) algorithms and Artificial Neural Networks (ANN). At last, we have compared the score for each of the applied methods.

Keywords: Electricity Grids, Machine Learning (ML), Artificial Neural Network (ANN), Intrusion Detection System (IDS).

I. INTRODUCTION

An Intrusion Detection System (IDS) is a software system that detects network traffic and any suspicious and abnormal activity that can primarily violate the policy. Not all unauthorized activities or unauthorized users have the intention to harm the system or device [1]. When IDS detects any unusual activities, it reports to the Control Room to look into the matter.

In the Power System dataset, there is the need to look into the attributes from the power system framework, as shown in Fig. 1.

The specification-based Intrusion Detection Systems (IDS) classifies system behaviours over time as either normal or an intrusion. The hardware required in an IDS can be seen in the Fig. 2. The insight is generally essential in guiding systems to determine whether a given issue is problematic and needs attention [1]. In addition, insight is critical concerning the available guidance on the improvements necessary for the system's proper functioning. Essentially, there is a high chance of the best outcomes being attained with respect to the system's running.

Common paths within the system generally dictate the signature for each scenario [1]. It helps describe the scenario with the need to establish the impact that it might have on the system. It is also important to determine the adjustments which enable the system to protect itself effectively.

Some attacks are only a probable threat that has not yet occurred, while others are the real threat [1]. For example, where an IDS has detected a threat and acts upon it before it damages the power grid, it is deemed a probable attack. Under this situation, it had the chance of causing adverse outcomes but never did. On the other hand, where the attack is not easily detected and ends up causing damage, it is an actual attack.

Thus, the aim is usually to ensure that the IDS has developed in a way that offers it the chance to ward off any potential attacks before they cause any harm to the grid [1]. Therefore, this concept has its importance in creating desired effects with respect to protecting the system; it contributes effectively towards protecting the system.

This approach makes the system better as the system has to identify the possible elements that may negatively contribute to its situation [1]. Moreover, this process establishes the necessary improvements that have to be adopted with the changing situation. Therefore, it contributes towards attaining the desired effects.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

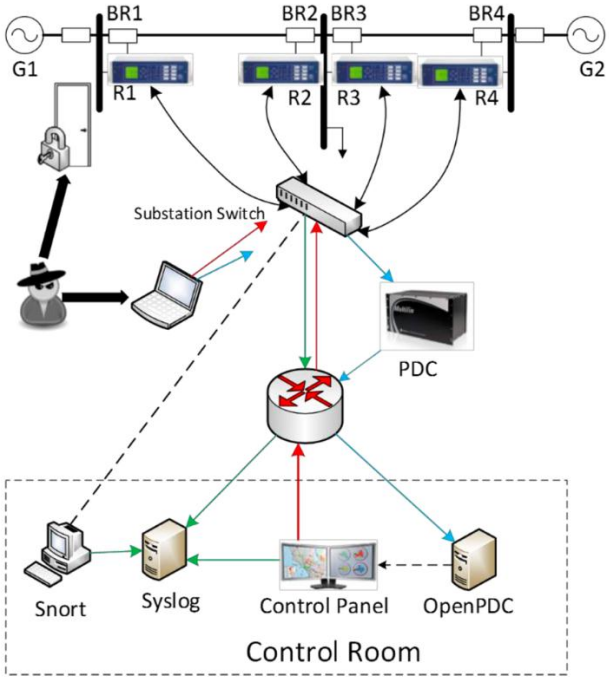

Fig 1: Power System dataset[2]

In this paper, we had 15 datasets with 128 parameters as features, and for each phasor measurement unit (PMU), there were 29 types of measurement [2], as shown in Table 1. The bifurcation of the triple dataset is, Attack, No Event, and Neutral. Furthermore, we had applied ML algorithms and a few variations of the ANN algorithm and finally compared the performances for all of them.

Table 1. Features in the datasets[2].

Feature	Description
PA1:VH – PA3:VH	Phase A - C Voltage Phase Angle
PM1: V – PM3: V	Phase A - C Voltage Phase Magnitude
PA4:IH – PA6:IH	Phase A - C Current Phase Angle
PM4: I – PM6: I	Phase A - C Current Phase Magnitude
PA7:VH – PA9:VH	Pos. – Neg. – Zero Voltage Phase Angle
PM7: V – PM9: V	Pos. – Neg. – Zero Voltage Phase Magnitude
PA10:VH - PA12:VH	Pos. – Neg. – Zero Current Phase Angle
PM10: V - PM12: V	Pos. – Neg. – Zero Current Phase Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
PA:Z	Appearance Impedance for relays
PA:ZH	Appearance Impedance Angle for relays
S	Status Flag for relays

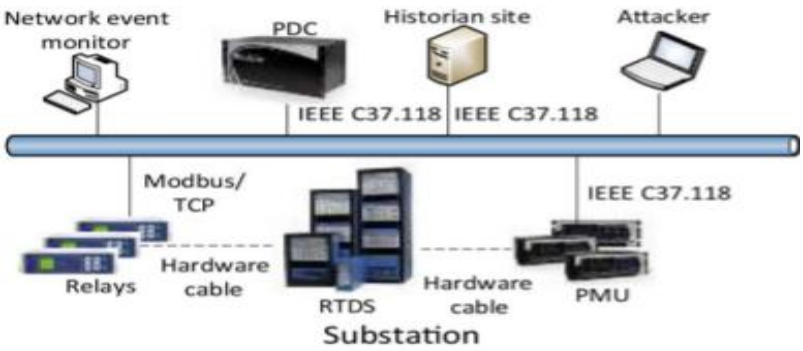

Fig 2: Hardware for IDS [3]

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

II. BACKGROUND

Power system attacks often come from various sources. For example, these could be from insiders, amateur hackers, criminal organizations, political activists, terrorists or governments. Therefore, the protective systems need to be developed in a way that they can quickly identify and deal with any simple attacks as well as the complicated ones[3].

Essentially, it is crucial to ensure the stability of the systems with the need to enable them to be more outstanding with respect to the activities that are entailed within. The approach generally means that such systems are bound to attain the ability to function effectively. In the process, there is the ease of establishing the areas that are performing well with respect to the presented situations. Therefore, it is possible to determine the appropriate mechanisms that need to be considered to ensure the system's desired stability.

Cyber-attacks on power installations may appear to be a real nuisance. For example, the fact that they might cause a negative decline to the system's performance shows that they harm the ability of people to access power [4]. The situation also limits the ability of people to go about their usual ways of life. Essentially, there is the indication that these challenges prevent the system from attaining the necessary levels of stability that would, otherwise, be linked to the same.

Moreover, strategies adopted with the need to address the problem are essential enough [3]. Significantly, they offer the chance for the necessary improvements to be made in a way that enables power systems to control themselves effectively. The concept also reduces the chances of people lacking access to power.

One scenario is the short-circuiting fault; it pertains to the short in the power line [4]. It can happen at one location or in multiple locations. The situation can happen due to a cyberattack that aims to make the system appear to have an internal problem.

Another form of attack could be through data injection. In this case, it is generally concerned with the flow of the data is directed to the system. Such data corrupts, makes the system act in a way that is different from normal [4]. In this process, the invalid data running through the system has a high risk of disruptions in the power grid.

For instance, there could be a relay setting change, also known as a direct attack on a system. It pertains to a change in the electricity relays signals. The negative impact on the relay signals is bound to be of significant harm, as it can potentially impact the transmission process, resulting in a power outage.

There are different types of attacks possible on power systems. One of them is a binary attack in which it introduces malicious code that changes how a power system should operate. Therefore, it is bound to disrupt the system, which might end up as a power outage [5]. In addition, sometimes, the binary attack could be covertly incorporated into the system in a way that would, otherwise, make it difficult to detect and address. As a result, it continues to project significant damage to the system until it is detected and dealt with.

There is also the multi-class attack. This form of attack could be either natural, intentional or one that results from normal operations. Natural attacks are often brutal to prevent as they result from situations beyond control [5]. For example, floods can be one of the causes, among others. In light of attacks that result from normal operations, it is necessary for the activities entailed within to be appropriately revamped. Such an approach is deemed to be imperative with respect to improving the whole situation. Therefore, the operations manager to continue as deemed appropriate with respect to ensuring that the desired outcomes are attained. The process is generally important with respect to minimizing the chances of adverse outcomes on the system due to operations challenges. Essentially, all the activities are likely to happen effectively with the need to attaining the desired effects.

Further, attack events should be appropriately assessed. The aim is to establish the causes of these attacks. In this process, there is the ease of establishing the necessary aspects deemed important to minimize the outcomes that may be attained. In addition, there is the comfort of adopting the desired mechanisms that may eventually lead to the system's protection.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

III. OBJECTIVE

The main objective is to train the model using Machine Learning algorithms and an Artificial neural network to predict whether the power system is under attack or not. In order to achieve that, we will be performing the data preprocessing, which includes data cleaning, normalizing the data, dealing with NAN values, oversampling & undersampling for imbalanced data and finally fitting into the classification algorithms for ML and then on ANN.

IV. METHODOLOGY

In this paper, we had the Power system's dataset, and the methodology followed for getting our result can be seen in Fig.3. So first, we looked into the data size for all 15 datasets and combined them in one data frame.

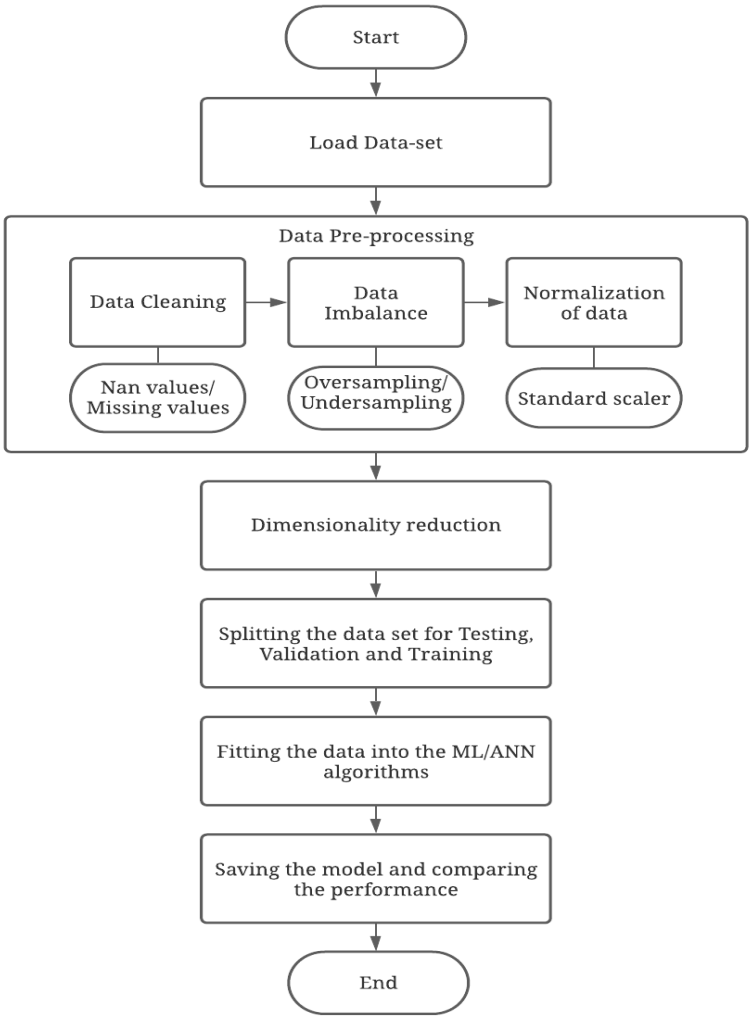

Fig 3: Methodology for training the model

A. Data Preprocessing

In data preprocessing, we started to clean the unwanted/invalid data present in the dataset; first, we looked into the zero values as there were no NaN values; as a result, we dropped all the columns which had more than 10,000 points as zero values. After that, we removed the rows having zeros values by converting them into NaN values and dropping them. Finally, we had a clean data set, and then we separated the features and target as 'X' and 'y'. adding to this, we made the targets binary i.e. No Event = 0, Natural = 1, and attack = 2.

B. Dimensionality Reduction

We made the dimensionality reduction by using the Low Variance method as we were getting bad results from PCA (Principal Component Analysis); in this, we dropped the columns having a variance less than ten,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

indicating that it has a low impact on training the model. Thus, after completing this step, we had our final parameters. Furthermore, the data is then split into Training (70%), Testing (20%) and Validation (10%).

C. Data Balancing

Now comes the problem of data imbalance; in the dataset, we had 51359 points for attack, 16202 for Natural and 4396 points for No Event, as shown in Fig. 4. A data imbalance refers to a "classification problem where the number of observations per class is not equally distributed" [6].

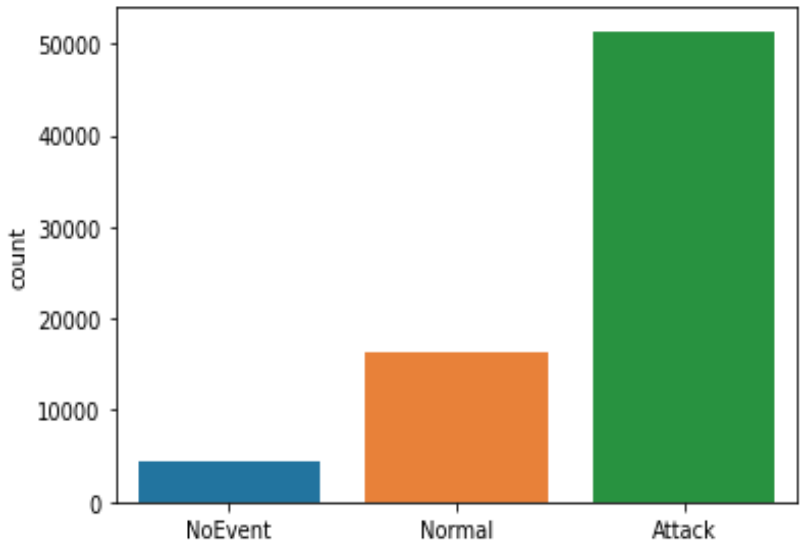

Fig 4: Imbalanced classes in the data-set

So, the countermeasure to solve this issue was to use oversampling; the method used is SMOTE (Synthetic Minority Oversampling Technique). It is a K- nearest algorithm which synthetic puts values near the original class values with the K= 5. As a result, we get balanced points for all classes, as seen in Fig. 5. Moreover, after getting our data balanced and cleaned, we normalized the data using the standard scaler algorithm.

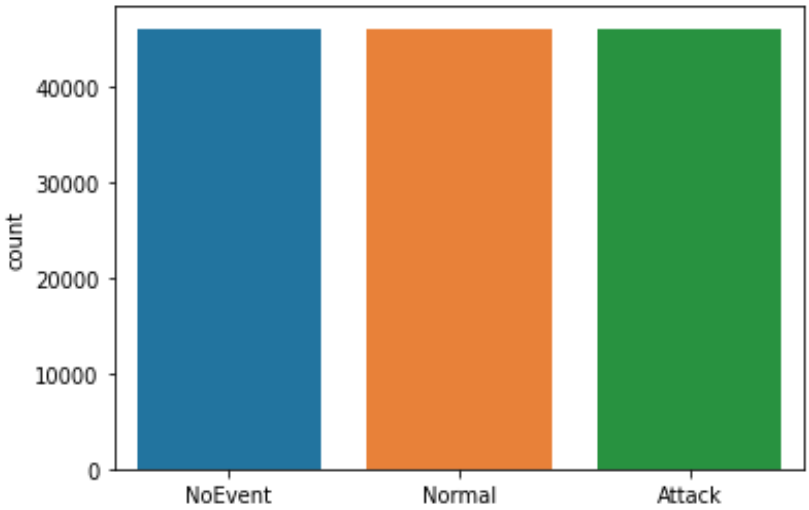

Fig 5: Balanced data-set for all classes

D. Outlier Rejection

We also did the outlier rejection for our dataset using the quantile method. Unfortunately, the model training was not up to the mark as the outliers getting rejected were valuable points and losing them was not an option. Furthermore, as we can compare in Fig. 6 and Fig. 7, the upper cluster was taken into account, whereas the lower cluster was rejected and came out as a data loss. Adding to this, we did train the model using this dataset; however, the model performance was significantly lower than non- rejected outlier data.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

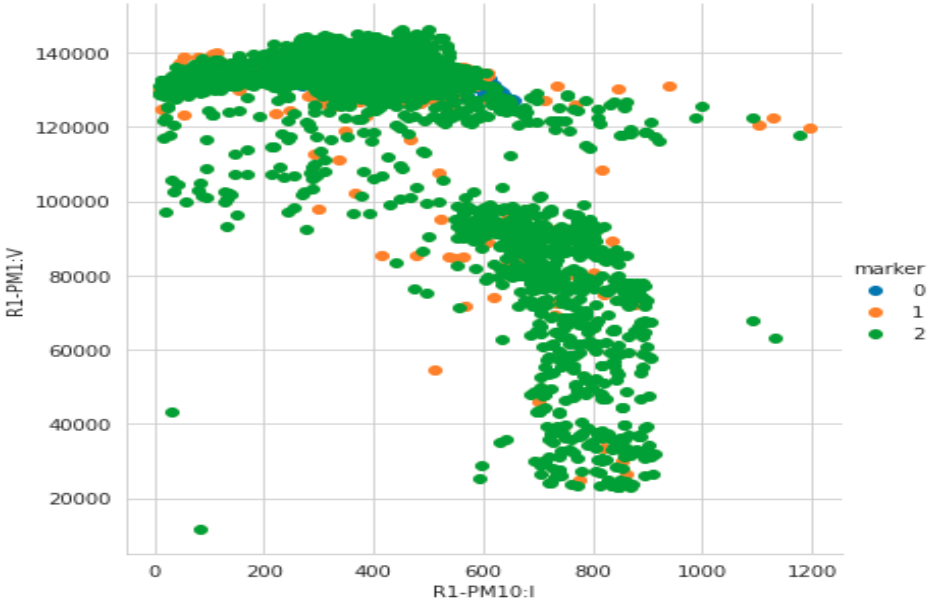

Fig 6: The whole data-set

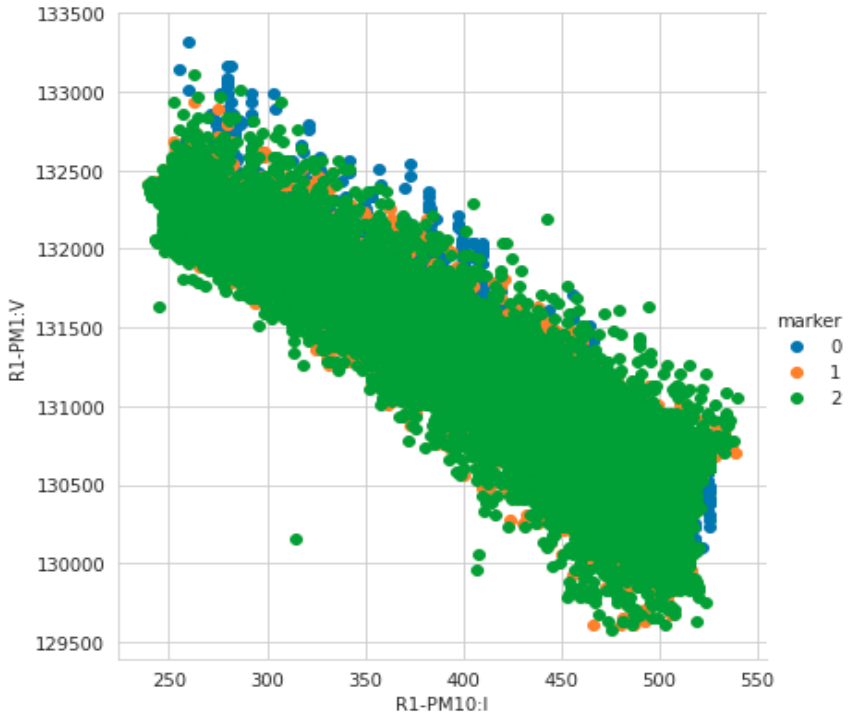

Fig 7: The data-set after outlier rejection

E. Model Training

Finally, we fitted our features onto the classification ML algorithms and lastly onto the ANN. The algorithms we tested on are:

1. SVM (Support Vector Machine)
2. KNN (K Nearest Neighbour)
3. Decision Tree
4. Naive Bayes
5. Random Forest
6. ANN

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

After training the model, we saved it using a library called pickles, and for ANN, we used one of the Keras libraries named model_from_yaml and saved the weights in the file format of HDF5.

V. RESULTS

After applying the algorithms, the results, we obtained are as follows:

A. SVM (Support Vector Machine)

SVM gave the lowest performance. In here, we had two kernels; one was 'RBF,' and the other was 'Linear,' both had the lowest accuracies.

The accuracy for SVM using RBF has been shown in Fig. 8 and for linear in Fig. 9.

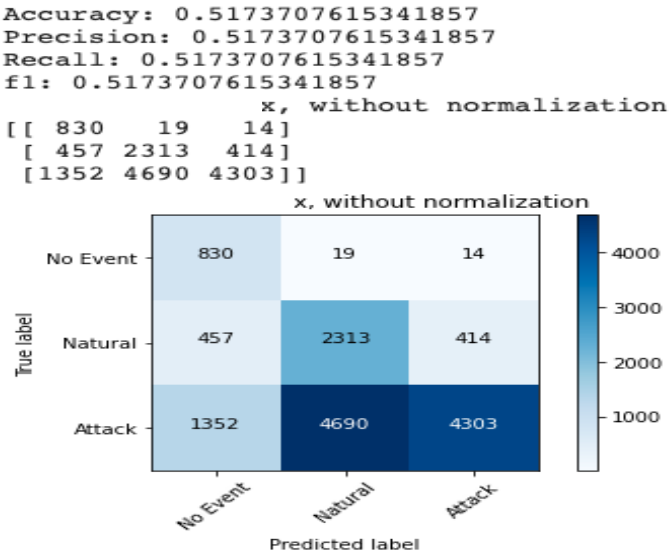

Fig 8: SVM using rbf Kernel

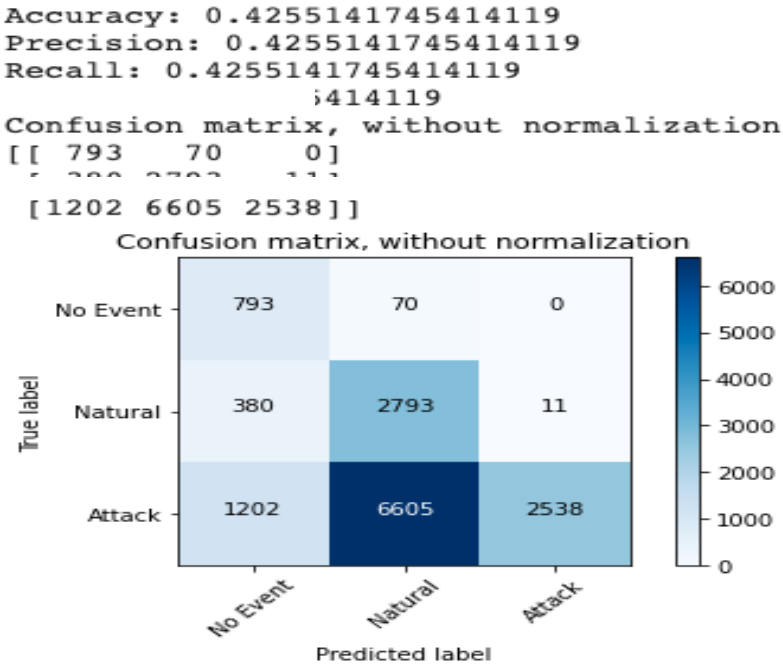

Fig 9: SVM using linear Kernel

B. KNN (K Nearest Neighbour)

In KNN, we looped over various values of K (from 1-14) and selected the one with the best accuracy as we have the results, as shown in Fig. 10.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

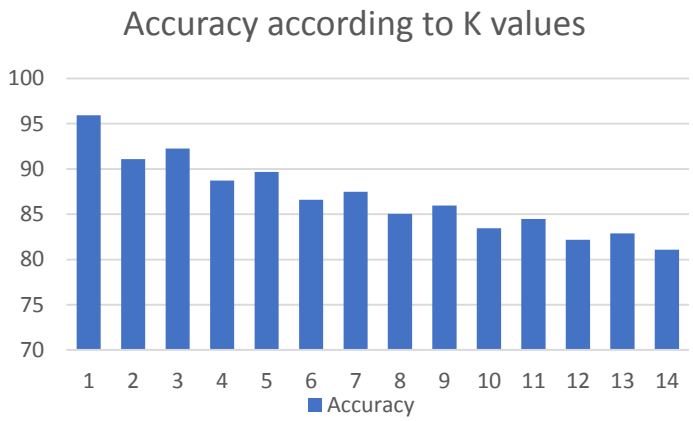

Fig 10: Accuracy with respect to K

As K = 1 has the highest accuracy but is a deficient number, we selected K = 3 and the result can be seen in Fig. 11.

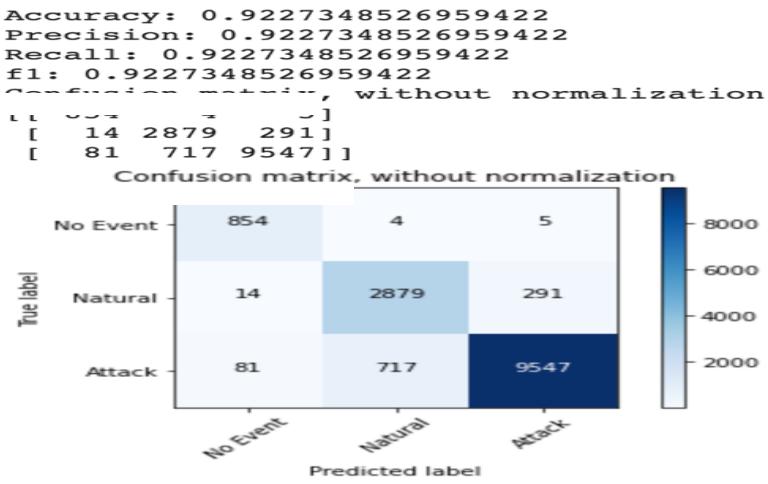

Fig 11: KNN accuracy when K =3

C. Decision Tree

The decision tree gave a good performance, and the accuracy can be seen in Fig. 12, and the importance given to each parameter by the algorithm can be seen in Fig. 13.

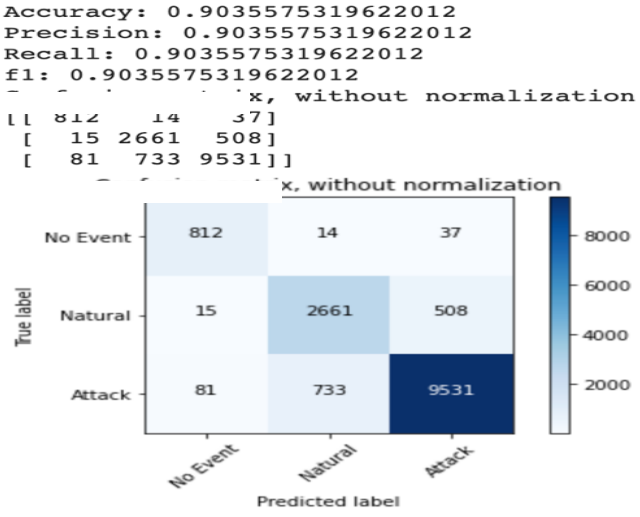

Fig 12: Accuracy of Decision Tree

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

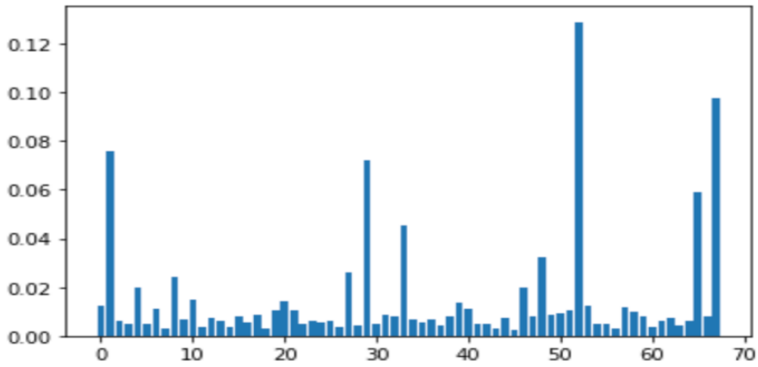

Fig 13: Importance given to each parameters by Decision Tree

D. Naive Bayes

Naive Bayes gave the worst performance of all the algorithms for reference; the result is shown in Fig. 14.

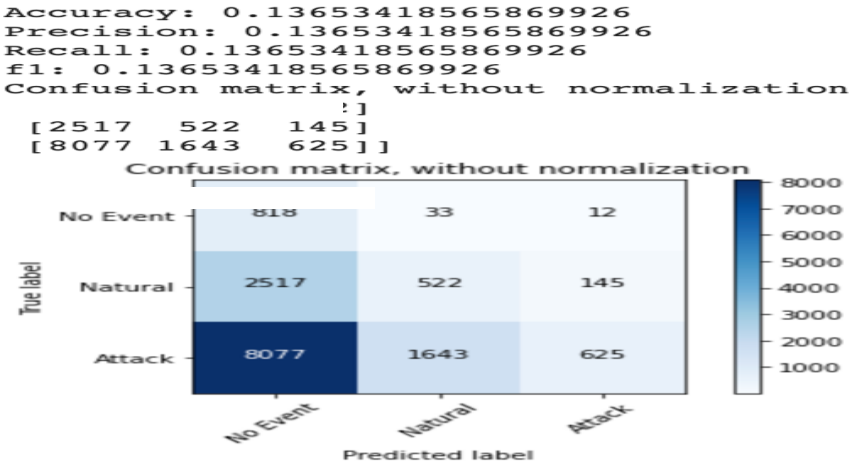

Fig 14: Accuracy of Naive Bayes

E. Random Forest

The Random Forest gave the best performance among all the algorithms. The result can be seen in Fig. 15, plus the importance given to each feature can be observed in Fig. 16.

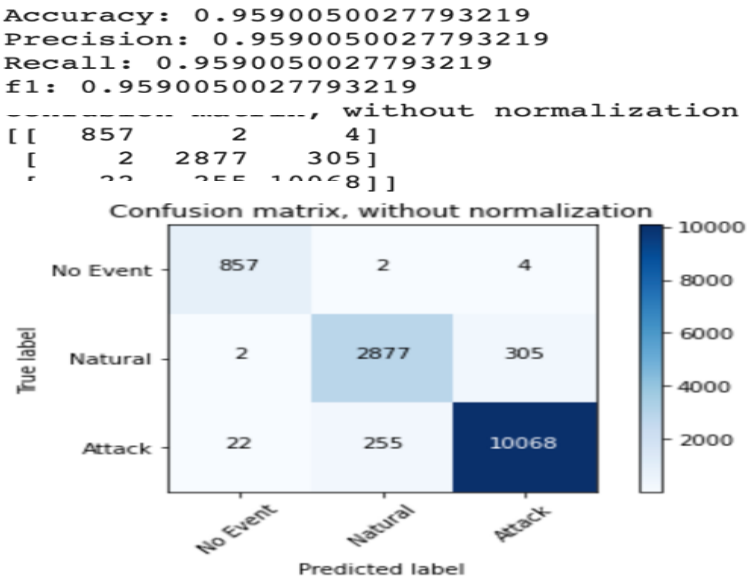

Fig 15: Accuracy of Random Forest

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

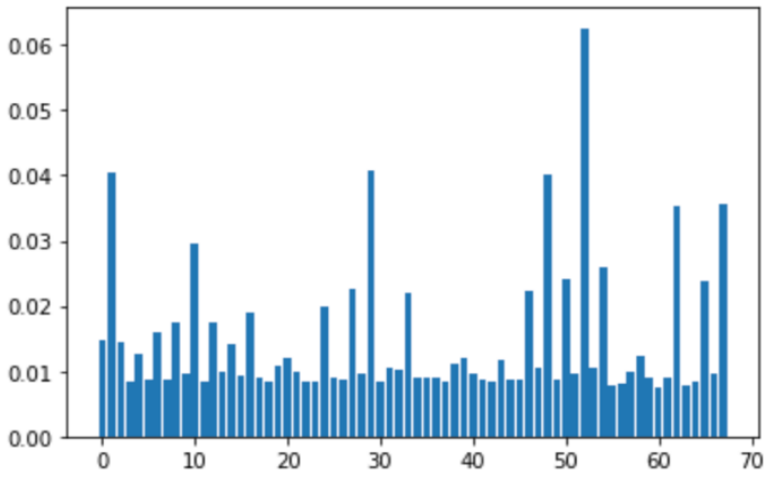

Fig 16: Importance given to each parameters by Random Forest

F. Artificial Neural Network (ANN)

In ANN, we have tried the hit and trial method using various activation functions on the hidden layers, changing batch size and loss function. Adding to this, we selected fully connected layers as 128, 64, 16, and 3, with the first three layers having an activation function as 'relu' and for the last layer, we used 'sigmoid.' Furthermore, the loss function used is 'mse' (mean square error) with the optimizer as 'adam.' Finally, after training multiple models, we have got a maximum of 85% accuracy:

1. The layered architecture can be seen in Fig. 17.
2. The epoch loss vs validation and epoch accuracy vs validation can be seen in Fig. 18 and 19
3. The accuracy can be seen in Fig. 20.

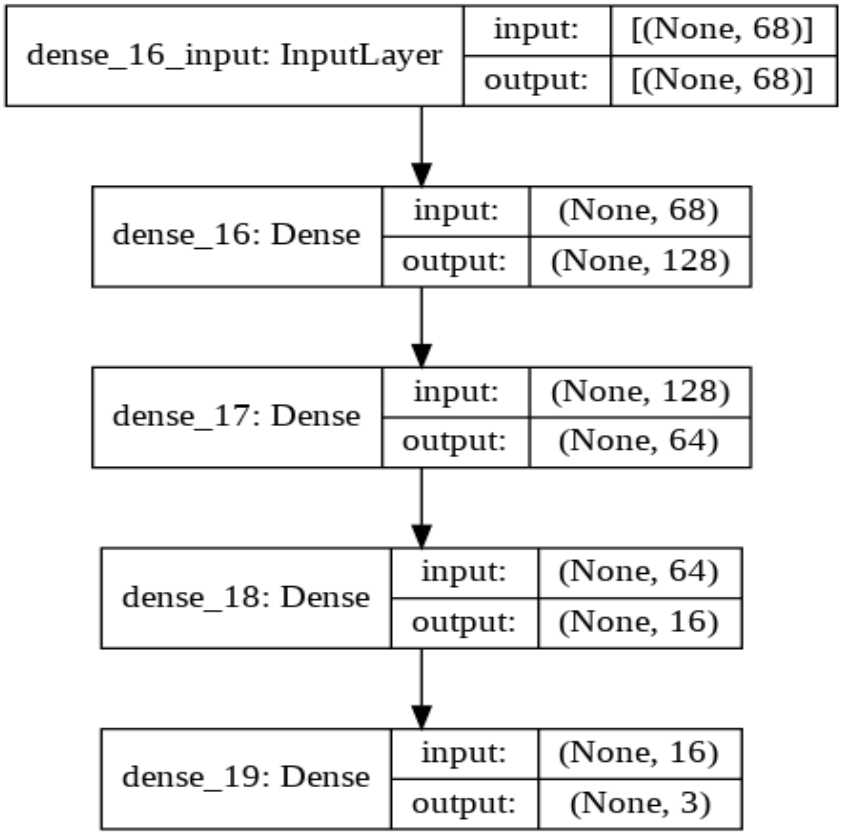

Fig 17: Layer architecture for ANN

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

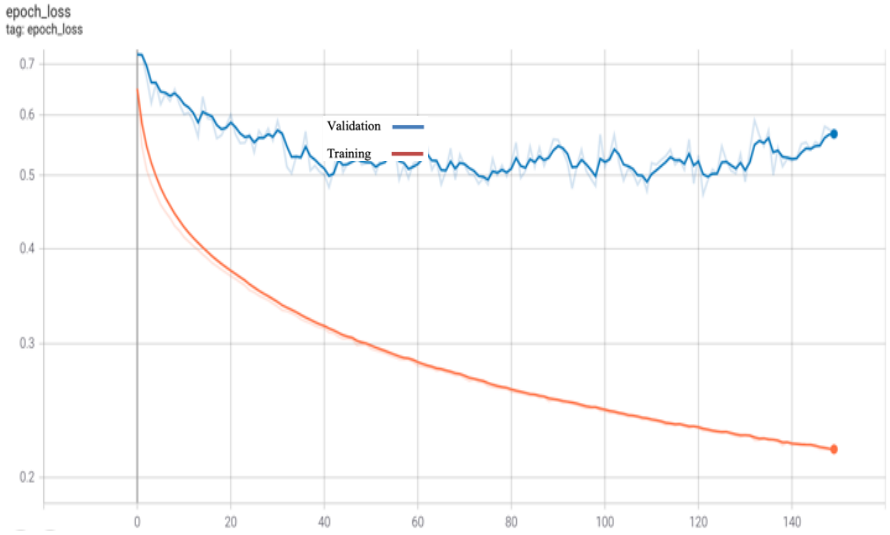

Fig 18: Epoch loss vs validation for ANN

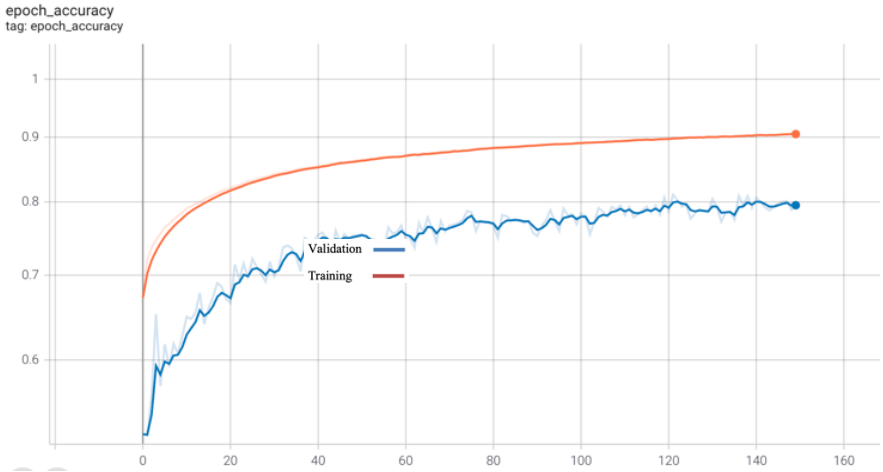

Fig 19: Epoch Accuracy vs validation for ANN

```
Accuracy: 0.8510978321289605
Precision: 0.8510978321289605
Recall: 0.8510978321289605
f1: 0.8510978321289605
Saved model to disk
Confusion matrix, without normalization
[[ 852    5    6]
 [  21 2744  419]
```

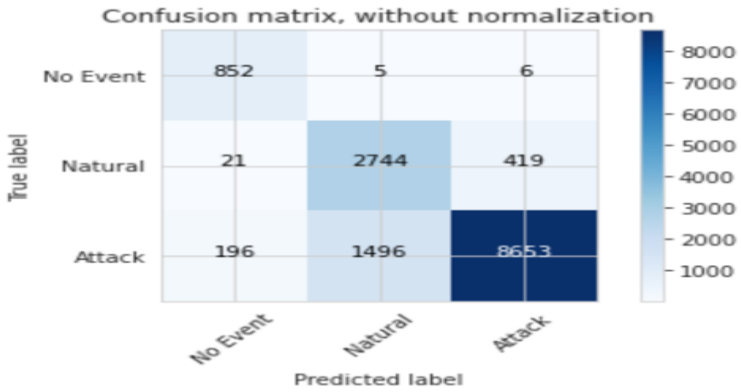

Fig 20: Accuracy for the ANN

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

G. Final comparison

In this section, we have compared the accuracies for all the models which we have trained. The graphical comparison can be witnessed in Fig. 21.

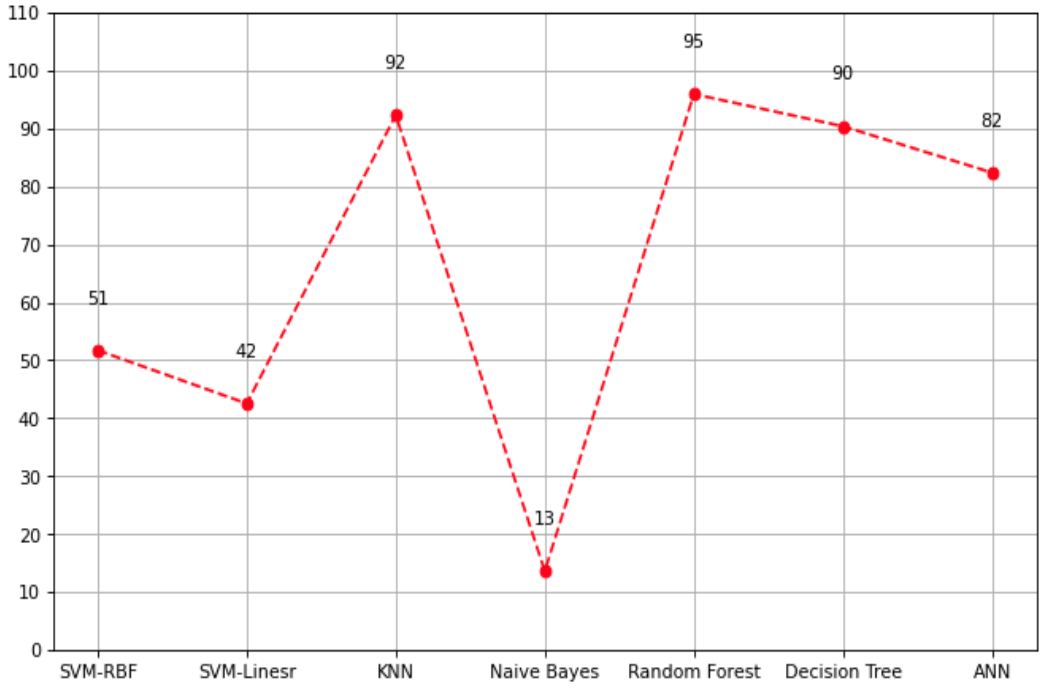

Fig 21: Final comparison for all models.

VI. COUNTERMESURES

Several countermeasures can be applied to avoid an attack. One of them entails the use of Wide Area Monitoring Systems (WAMS) [5]. The use of these systems generally enables organizations to cooperate to have real-time monitoring of electric power systems. The mechanism enables companies to focus more on identifying potential threats to the system to address them in a timely fashion. In the process, it deals with the problem because it leads to power disruptions. The monitoring of power systems is also vital in identifying any vulnerabilities linked to the system. In the process, the necessary adjustments could be made to the system to work effectively. It could help to ward off potential attacks.

Electricity companies can also use IDS. These systems are originally used on an IT system to detect activities that violate the security policy. There are two types of these systems. These include; Anomaly-based Intrusion Detection and Misuse-based Intrusion Detection. The Anomaly-based IDS is usually preferred owing to its ability to detect zero-day intrusions. However, the downside of the system is that it has a high rate of false positives. This case typically occurs due to some normal behaviours, not relevant aspects that would otherwise be described as expected [5]. Therefore, it describes some normal behaviours as intrusions. It creates a major challenge as system adjustments are prompted to occur when there is no intrusion that needs to be acted upon.

Essentially, the system needs protection against the adverse effects linked to this software to prevent negative outcomes from the situation. However, to counter the problem associated with the Anomaly-based IDS, the specification-based IDS was introduced. This system is important for creating the desired level of accuracy concerning the identification of any anomalies[5]. It would be necessary to identify the causes that are an indication of a breach. As a result, the system will be creating a positive change in line with addressing the problem identified. The reduction in the case of false positives would also be significant in safeguarding the number of resources that go into the whole process.

Another countermeasure would entail the use of a Bayesian network. This network offers precise semantics that provides the chance to extract the necessary knowledge. Moreover, it provides the ease to establish how

well a system is working [5]. Thus, a system can work effectively in the process, especially considering the improvements they make to the system to boost its performance effectively.

Decision trees and Random Forest are also deemed necessary for establishing the strategies that may need to be applied with the need to improve the performance of a system. In the process, there is the ease of adopting the necessary improvements. Therefore, it contributes towards creating the best outcomes.

VII. CONCLUSION

We have concluded that random forest gives the best accuracy in order to predict whether there is an attack on the power system or not. Furthermore, the model could be implemented in such a way that it can predict a streamline of data and identify if attacks are being initialized in real-time.

FUTURE WORK

We think the model for ANN could have been better if we had pre-trained the model or reduced the dimensions. Moreover, there is a possibility that we could have got better outlier rejection if we had used one of the library functions of sklearn named Isolation Forest. Adding to this, it might have helped in increasing the accuracy for both ANN and ML models.

VIII. REFERENCE

[1] S. Pan, T. Morris, and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104–3113, Nov. 2015, doi: 10.1109/TSG.2015.2409775.

[2] "Power System Attack Datasets-Mississippi State".

[3] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 650–662, Jun. 2015, doi: 10.1109/TII.2015.2420951.

[4] S. Pan, T. Morris, and U. Adhikari, "A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System," 2015.

[5] R. Borges, J. M. Beaver, M. Buckner, and T. Morris, "Machine Learning for Power System Disturbance and Cyber-attack Discrimination", doi: 10.1109/ISRCS.2014.6900095.

[6] B. Krawczyk, "Learning from imbalanced data: open challenges and future directions," Progress in Artificial Intelligence, vol. 5, no. 4, pp. 221–232, Nov. 2016, doi: 10.1007/S13748-016-0094-0.