IJIEMR Transactions, online available on 27th Nov 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 11

DOI: 10.48047/IJIEMR/V11/ISSUE 11/22

Title ICT DEVICES PROTECTION IN SMART GRID

Volume 11, ISSUE 11, Pages: 139-144

Paper Authors

G.SURESH, Dr. V.UMA RANI

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ICT DEVICES PROTECTION IN SMART GRID

G.SURESH[1], Dr. V.UMA RANI[2]

[*1]Student, M.Tech (CNIS), School of Information Technology, JNTU Hyderabad, Hyderabad, India

[*2]Professor of CSE, School of Information Technology, JNTU Hyderabad, Hyderabad, India

ABSTRACT: Recent developments in the cyber-physical smart grid (CPSG) have made a variety of new information and communication technology-based devices possible (ICT). However, the threat of cyber-physical attacks is on the rise against these ICT-enabled gadgets. This study offers a unified state-space model that allows for the successful generalization of cyber-physical attack and defense models by concentrating on the physical layer of the CPSG. The target components of the current cyber-physical attacks are categorized. The state-of-the-art in the field, including data driven approaches, is then presented through a number of operational and informational defense approaches. When looking for system attacks, we use a variety of machine learning algorithms. Finally, we talk about the cyber-physical security of the smart grid's difficulties and potential future opportunities.

Keywords *– K- Nearest Neighbors (KNN); Logistic Regression (LR); Support Vector Machine (SVM).*

1 INTRODUCTN

Cyber-physical systems (CPSs) are intelligent systems with engineered networks of physical and computer components interacting with one another. Systems that are deeply interconnected and integrated add new capabilities to support technological advancement in vital infrastructures like water networks, transportation, home automation, and healthcare. A CPS includes intricate control, awareness, computing, and communication systems. The potential difficulties for the security and resilience of CPSs have been highlighted by the complexity and variability. The challenge of the bulk physical layer's interconnection protection from any innate physical vulnerabilities

2 LITERATURE SURVEY

Cyber–physical system security for the electric power grid:

In order to create a reliable smart grid, it is important to comprehend the potential effects of successful cyber attacks. Evaluation of the grid's reliance on its cyber infrastructure and its capacity to withstand potential breakdowns are necessary for estimating the impact of a realistic attack. To assess the suitability of the smart grid, more investigation into the cyber-physical relationships within it is required, as well as a detailed examination of potential attack vectors. cyber security initiatives In order to avoid, mitigate, and tolerate cyber attacks, this study emphasizes the importance of cyber infrastructure security in conjunction with power application security. In order to assess risk based on the security of both the physical power applications and the underlying cyber infrastructure, a layered methodology is developed. A classification is provided to show the interdependencies between the communication and computations that need to be secured from cyber attack and the cyber-physical controls necessary to support the smart grid. The presentation then discusses ongoing research projects designed to improve the application and infrastructure security of the smart grid. Finally, in order to enable future research, present problems are identified..

. A small Belarusian company called VirusBlockAda's security experts discovered harmful software (malware) that infected USB memory sticks on June 17th, 2010. 1 A flurry of activity in the computer security field emerged in the months that followed, showing that this finding had only pinpointed one element of the Stuxnet computer worm. This software was made primarily to attack industrial machinery. Many in the media conjectured that Stuxnet's ultimate objective was to attack Iranian nuclear facilities once it was revealed that the majority of infections were found Additionally, the Iranian Fuel Enrichment Plant (FEP) at Natanz decommissioned its centrifuges for no apparent reason, 3 in Iran. When Iranian

President Mahmoud Ahmadinejad publicly stated that a computer worm caused issues for a "small number of our [nuclear] centrifuges" in November 2010, some of these fears were confirmed. Stuxnet has already been described as "unprecedented," "an evolution leap," and "the type of danger we want to never see again" by reputable specialists in the field of computer security. 8 In this essay, I contend that Stuxnet profoundly alters the character of cyber warfare and that it represents a revolution in military affairs (RMA) 9 in the virtual world. This assertion is supported by four factors: Stuxnet was the first instance of a cyberattack targeting industrial machinery, and there is evidence that the worm was successful in

Considering False Data Injection Attacks in Light of the 2015 Ukraine Blackout

An adversary conducts a coordinated, stealthy hack of measurements from electricity grid sensors in a false data injection attack (FDIA), hoping to avoid detection by the power system's bad data detection module. A successful FDIA may prompt the system operator to make decisions that compromise the power system's ability to function physically or profitably. In this letter, we discuss possible FDIAs-related ramifications of the late-2015 Ukraine Blackout incident.

Cyber security issues for advanced metering infrastructure (ami):

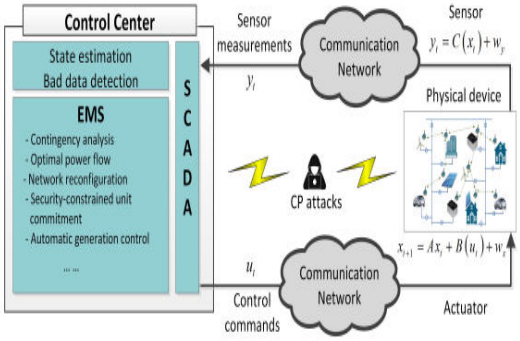
Many stakeholders, including utilities, regulators, energy markets, and a society concerned with energy conservation and mitigating the effects of global warming, are becoming more and more interested in advanced metering infrastructure (AMI). Many companies are working on AMI technologies, which are quickly replacing the older Automated Meter Reading (AMR) technologies. Some of these suppliers are metering manufacturers, communications service providers, and back-office Meter Data Management (MDM) IT vendors. The cyber security of AMI systems has not yet received much attention in this frenzy of excitement. Typically, the response is, "Oh, of course, we'll encrypt everything; that'll make everything secure." This response suggests a lack of awareness of the potential security risks posed by AMI, a technology that will affect the vast majority of homes as well as almost all commercial and industrial clients.

Security and privacy challenges in the smart grid:

The switch to smart grid technologies is one of the biggest revolutions the electrical system has ever through. Customers and providers may manage and produce power more effectively thanks to this new grid. The smart grid raises fresh security issues, as with many new technology. The current of worldwide smart grid deployments, their operational, ecological, and financial justifications, as well as the potential causes and expenses of security failures, are all discussed in this article. The secuhority issues that upcoming deployments would almost certainly encounter could be addressed by future projects.

3 Methodlogy

The ability of smart grids to repair themselves can be actively assisted by electricity customers. Some smart cities employ this smart grid to regulate the opening and closing of doors, the consumption of electricity, and other operations. The smart grid system is open to intrusions from dishonest users who want to spread or introduce incorrect information. If this occurs, the smart grid would work improperly and incur huge losses in revenue. By analysing historical data from the past, machine learning algorithms may predict the future. In order to detect bogus injection attacks paired with observed data, these algorithms are skilled in spotting unobserved information mixed with observed information.



4 IMPLEMENTATION

ALGORITHMS

The Perceptron, KNN, SVM, and Logistic Regression machine learning algorithms were employed by the author to carry out this study.

PERCEPTRON ALGORITHM:

For binary classification tasks, the Perceptron is a linear machine learning technique.

1. It might be regarded as one of the earliest and most basic varieties of artificial neural networks.

2. It is unquestionably not "deep" learning, but it is a crucial stepping stone.

3. It can learn a linear separation in feature space for two-class classification tasks quickly, similar to logistic regression, however unlike logistic regression, it uses the stochastic gradient descent optimization approach and does not forecast calibrated probability.

The Perceptron algorithm is a machine learning approach for binary classification with two classes. It belongs to a class of neural network models, maybe the most basic one. an individual node or neuron that takes in a row of data as input

KNN ALGORITHM:

The supervised machine learning technique known as the k-nearest neighbours (KNN) can be used to handle classification and regression issues. It is straightforward and simple to implement. A set of input values are used by machine learning models to forecast output values. One of the simplest machine learning algorithms, KNN is primarily employed for categorization. The classification of the data point is based on the classification of its neighbour. Based on the similarity score of the previously stored data points, KNN categorises the new data points. If we have a dataset of tomatoes and bananas, as an illustration. Similar metrics like form and colour will be stored by KNN. When a new object is delivered, its shape and colour (red or yellow) are compared to see if they are identical**.**

SVM:

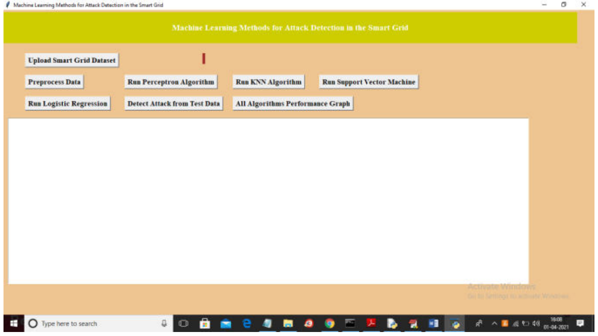
. An approach for supervised machine learning called SVM can be applied to classification or regression issues. Your data is transformed using a method known as the kernel trick, and based on these modifications, it determines the best border between the potential outputs. The kernel trick alters the data you supply it with. You put in some fantastic attributes that you believe will create a fantastic classifier, and some data that you no longer recognise comes out. It resembles unravelling a DNA strand in certain ways. After going through the kernel technique, the initially harmless-appearing vector of data unravels and compounds itself into a considerably larger set of data that is difficult to comprehend by glancing at a spreadsheet. However, this is where the magic happens; by enlarging the dataset, your classes' boundaries are now more evident, and the SVM method can generate a hyperplane that is much more optimal.

LOGISTIC REGRESSION:

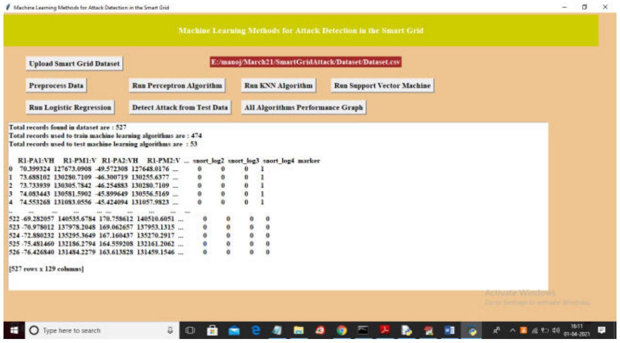
A supervised learning approach called logistic regression is used to forecast a dependent categorical target variable. In essence, logistic regression may be able to aid if you need to categorise a vast quantity of data. When determining if bank customers are likely to fail on their debts, logistic regression may be utilised. This is a formula a bank uses to determine whether or not to lend to a customer and to determine how much money it will lend to those who have already been found to be creditworthy. The bank will take into account a number of variables while making this calculation. This logistic model has lend as its target, and using the predicted likelihood of default, The decision to take the risk of lending to each consumer rests with the lender. These elements, which are sometimes referred to as characteristics or independent variables, may include things like credit score, income level, age, marital status, employment status, gender, the area where one currently resides, and educational background. In addition, insurance corporations and medical researchers frequently employ logistic regression. Researchers would include various patient behaviours and genetic predispositions as predictive factors in order to quantify cancer risks. Age, race, weight, smoking, drinking, exercise habits, general medical history, family history of cancer, and place of residence and employment, taking into account environmental factors, would all be taken into consideration to determine whether or not a patient is at a high risk of developing cancer. Regression with logit is

5 EXPERIMENT RESULTS

Double-clicking the "run.bat" file will open the project and display the screen below**.**

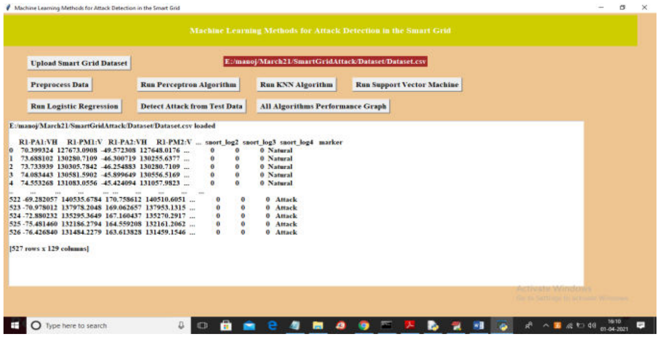

Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph

dataset Click the "Upload Smart Grid Dataset" button in the previous screen to upload.


Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph

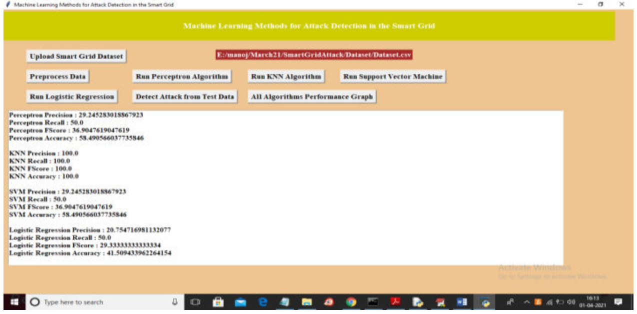
```
Total records found in dataset are : 527
Total records used to train machine learning algorithms are : 474
Total records used to test machine learning algorithms are  : 53

    R1-PA1:VH    R1-PM1:V   R1-PA2:VH    R1-PM2:V  ...  snort_log2  snort_log3  snort_log4  marker
0    70.399324  127673.0908  -49.572308  127648.0176  ...        0          0          0      1
1    73.688102  130280.7109  -46.300719  130255.6377  ...        0          0          0      1
2    73.733939  130305.7842  -46.254883  130280.7109  ...        0          0          0      1
3    74.083443  130581.5902  -45.899649  130556.5169  ...        0          0          0      1
4    74.553268  131083.0556  -45.424094  131057.9823  ...        0          0          0      1
..         ...          ...         ...          ...  ...      ...        ...        ...    ...
522 -69.282057  140535.6784  170.758612  140510.6051  ...        0          0          0      0
523 -70.978012  137978.2048  169.062657  137953.1315  ...        0          0          0      0
524 -72.880232  135295.3649  167.160437  135270.2917  ...        0          0          0      0
525 -75.481460  132186.2794  164.559208  132161.2062  ...        0          0          0      0
526 -76.426840  131484.2279  163.613828  131459.1546  ...        0          0          0      0

[527 rows x 129 columns]
```

The "Dataset.csv" file is being selected and uploaded on the screen above. Next, click "Open" to load the dataset and display the screen below.


Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph

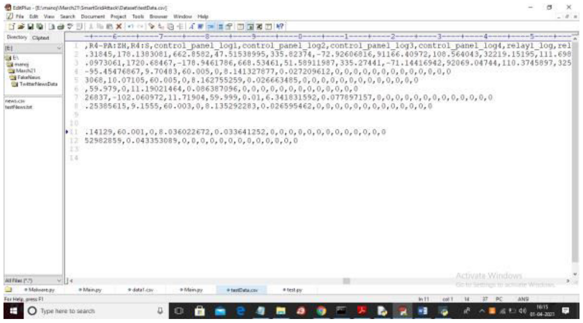
```
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv loaded

    R1-PA1:VH    R1-PM1:V   R1-PA2:VH    R1-PM2:V  ...  snort_log2  snort_log3  snort_log4   marker
0    70.399324  127673.0908  -49.572308  127648.0176  ...        0          0          0  Natural
1    73.688102  130280.7109  -46.300719  130255.6377  ...        0          0          0  Natural
2    73.733939  130305.7842  -46.254883  130280.7109  ...        0          0          0  Natural
3    74.083443  130581.5902  -45.899649  130556.5169  ...        0          0          0  Natural
4    74.553268  131083.0556  -45.424094  131057.9823  ...        0          0          0  Natural
..         ...          ...         ...          ...  ...      ...        ...        ...      ...
522 -69.282057  140535.6784  170.758612  140510.6051  ...        0          0          0   Attack
523 -70.978012  137978.2048  169.062657  137953.1315  ...        0          0          0   Attack
524 -72.880232  135295.3649  167.160437  135270.2917  ...        0          0          0   Attack
525 -75.481460  132186.2794  164.559208  132161.2062  ...        0          0          0   Attack
526 -76.426840  131484.2279  163.613828  131459.1546  ...        0          0          0   Attack

[527 rows x 129 columns]
```

The dataset is loaded in the page above, and non-numeric values are displayed there. To replace these with numeric values, click on "Preprocess Data. The dataset in the above screen's first three lines contains a total of 527 records, and the application uses 474 of those records to train machine learning (ML) and 53 of those records to test the accuracy of that learning. All string values and missing values have been replaced with numeric values. In order to train the perceptron algorithm on the prepared dataset and determine its accuracy, click the "Run Perceptron Algorithm" button.


Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph

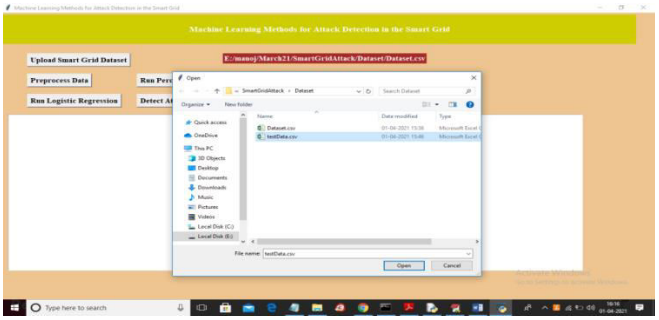
```
Perceptron Precision : 29.245283018867923
Perceptron Recall : 50.0
Perceptron FScore : 36.9047619047619
Perceptron Accuracy : 58.490566037735846

KNN Precision : 100.0
KNN Recall : 100.0
KNN FScore : 100.0
KNN Accuracy : 100.0

SVM Precision : 29.245283018867923
SVM Recall : 50.0
SVM FScore : 36.9047619047619
SVM Accuracy : 58.490566037735846

Logistic Regression Precision : 20.754716981132077
Logistic Regression Recall : 50.0
Logistic Regression FScore : 29.333333333333334
Logistic Regression Accuracy : 41.509433962264154
```

I selected all four algorithms in the screen above, and the accuracy, precision, recall, and FSCORE of each algorithm appeared. KNN is the overall algorithm with the best performance results. The ML algorithm will now predict whether to classify the uploaded test data as normal or attack. In the test data shown below, vector values can be seen, but no class labels are present. This class label will be predicted by ML.

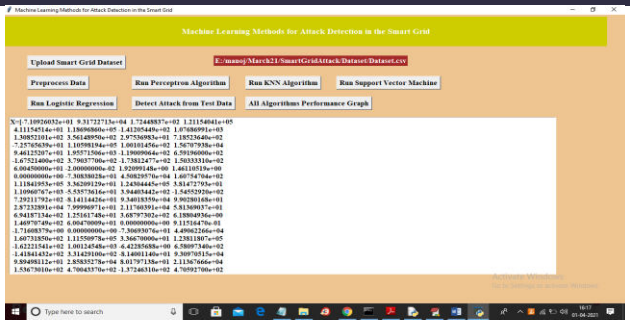

File Edit View Search Document Project Tools Browser Window Help
Cliptext

```
,R4-PA:ZH,R4:S,control_panel_log1,control_panel_log2,control_panel_log3,control_panel_log4,relay1_log,rel
.31845,178.1383081,662.8582,47.51538995,335.82374,-72.92606816,91166.40972,108.564043,32219.15195,111.698
.0973061,1720.68467,-178.9461786,668.53461,51.58911987,335.27441,-71.14416942,92069.04744,110.3745897,325
-95.45476867,9.70483,60.005,0,8.141327877,0.027209612,0,0,0,0,0,0,0,0,0,0,0,0
3068,10.07105,60.005,0,8.162755259,0.026663485,0,0,0,0,0,0,0,0,0,0,0,0
,59.979,0,11.19021464,0.086387096,0,0,0,0,0,0,0,0,0,0,0,0
26837,-102.060972,11.71904,59.999,0.01,6.341831592,0.077897157,0,0,0,0,0,0,0,0,0,0,0,0
.25385615,9.1555,60.003,0,8.135292283,0.026595462,0,0,0,0,0,0,0,0,0,0,0,0


.14129,60.001,0,8.036022672,0.033641252,0,0,0,0,0,0,0,0,0,0,0,0
52982855,0.043353089,0,0,0,0,0,0,0,0,0,0,0,0
```

We don't have a class label for natural or attack in the test dataset screen shown above. Once we submit the dataset to the programme, machine learning will predict the class label for each record. To access the screen below, click the 'Detect Attack from Test Data' button.

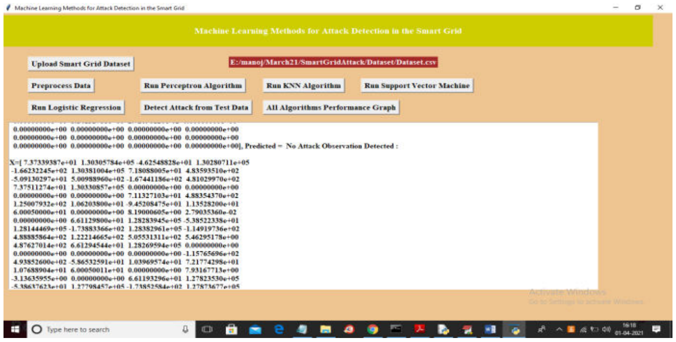

Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Logistic Regression
Open
Dataset.csv
testData.csv
File name: testData.csv
Open
Cancel

The "testData.csv" file can be selected, uploaded, and then clicked to get the results shown below.


Machine Learning Methods for Attack Detection in the Smart Grid
Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph
Type here to search

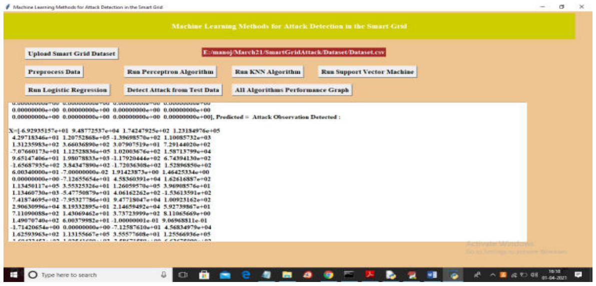
```
X=[-7.10926032e+01  9.31722713e+04  1.72448837e+02  1.21154041e+05
  4.11154514e+01  1.18696860e+05 -1.41205449e+02  1.07686991e+03
  1.30852101e+02  3.56148950e+02  2.97536983e+01  7.18523640e+02
 -7.25765639e+01  1.10598194e+05  1.00101456e+02  1.56707938e+04
  9.46125207e+01  1.95571506e+03 -1.19009064e+02  6.59196000e+02
 -1.67521400e+02  3.79037700e+02 -1.73812477e+02  1.50333310e+02
  6.00450000e+01 -2.00000000e-02  1.92099148e+00  1.46110519e+00
  0.00000000e+00 -7.30838028e+01  4.50829570e+04  1.60754704e+02
  1.11841953e+05  3.36209129e+01  1.24304445e+05  3.81472793e+01
  1.10960767e+03 -5.53573616e+01  3.94403442e+02 -1.54552920e+02
  7.29211792e+02 -8.14114426e+01  9.34018359e+04  9.90280168e+01
  2.87232891e+04  7.99996971e+01  2.11760391e+04  5.81369037e+01
  6.94187134e+02  1.25161748e+01  3.68797302e+02  6.18804936e+00
  1.46970749e+02  6.00470009e+01  0.00000000e+00  9.11516470e-01
 -1.71608379e+00  0.00000000e+00 -7.30693076e+01  4.49062266e+04
  1.60731850e+02  1.11550978e+05  3.36670000e+01  1.23811807e+05
 -1.62221541e+02  1.00124548e+03 -6.42285688e+00  6.58097340e+02
 -1.41841432e+02  3.31429100e+02 -8.14001140e+01  9.30970515e+04
  9.89498112e+01  2.85835278e+04  8.01797138e+01  2.11367666e+04
  1.53673010e+02  4.70043370e+02 -1.37246310e+02  4.70592700e+02
```

Grid vector values are shown in square brackets in the above-screen textarea; after the square brackets, the anticipated outcome is shown in the below-screen textarea On the screen above, we can see the anticipated outcome as observed ATTACK observation values.

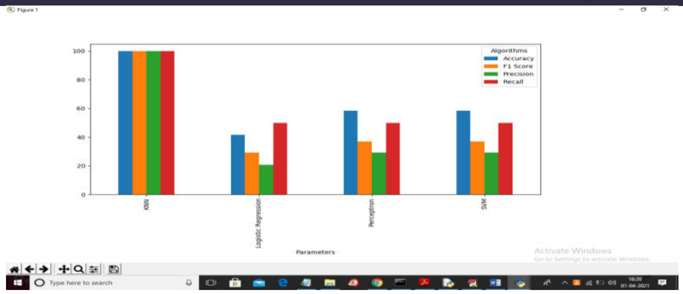

Machine Learning Methods for Attack Detection in the Smart Grid
Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph
Type here to search

```
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00], Predicted =  No Attack Observation Detected :

X=[ 7.37339387e+01  1.30305784e+05 -4.62548828e+01  1.30280711e+05
 -1.66232245e+02  1.30381004e+05  7.18088005e+01  4.83593510e+02
 -5.09130297e+01  5.00988960e+02 -1.67441186e+02  4.81029970e+02
  7.37511274e+01  1.30330857e+05  0.00000000e+00  0.00000000e+00
  0.00000000e+00  0.00000000e+00  7.11327103e+01  4.88354370e+02
  1.25007932e+02  1.06203800e+01 -9.45208475e+01  1.13528200e+01
  6.00050000e+01  0.00000000e+00  8.19000605e+00  2.79035360e-02
  0.00000000e+00  6.61129800e+01  1.28283945e+05 -5.38522338e+01
  1.28144469e+05 -1.73883366e+02  1.28382961e+05 -1.14919736e+02
  4.88885864e+02  1.22214665e+02  5.05531311e+02  5.46295178e+00
  4.87627014e+02  6.61294544e+01  1.28269594e+05  0.00000000e+00
  0.00000000e+00  0.00000000e+00  0.00000000e+00 -1.15765696e+02
  4.93852600e+02 -5.86532591e+01  1.03969574e+01  7.21774298e+01
  1.07688904e+01  6.00050011e+01  0.00000000e+00  7.93167713e+00
 -3.13635955e+00  0.00000000e+00  6.61193296e+01  1.27823530e+05
 -5.38637623e+01  1.27798457e+05 -1.73852584e+02  1.27873677e+05
```

On the screen above, we can see that there were no attacks identified for the fourth record. Scroll down to view the forecast results for each record. To access the graph below, click the "All Algorithms Performance Graph" button.


Machine Learning Methods for Attack Detection in the Smart Grid
Machine Learning Methods for Attack Detection in the Smart Grid
Upload Smart Grid Dataset
E:/manoj/March21/SmartGridAttack/Dataset/Dataset.csv
Preprocess Data
Run Perceptron Algorithm
Run KNN Algorithm
Run Support Vector Machine
Run Logistic Regression
Detect Attack from Test Data
All Algorithms Performance Graph
Type here to search

```
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00], Predicted =  Attack Observation Detected :

X=[-6.92935157e+01  9.48772537e+04  1.74247925e+02  1.23184976e+05
  4.29718346e+01  1.20752868e+05 -1.39698570e+02  1.10085732e+03
  1.31235983e+02  3.66036890e+02  3.07907519e+01  7.29144020e+02
 -7.07660173e+01  1.12528836e+05  1.02003676e+02  1.58713799e+04
  9.65147406e+01  1.98078833e+03 -1.17920444e+02  6.74394130e+02
 -1.65687935e+02  3.84347890e+02 -1.72036308e+02  1.52896850e+02
  6.00340000e+01 -7.00000000e-02  1.91423873e+00  1.46425334e+00
  0.00000000e+00 -7.12655654e+01  4.58360391e+04  1.62616887e+02
  1.13450117e+05  3.55325326e+01  1.26059570e+05  3.96908576e+01
  1.13460730e+03 -5.47750879e+01  4.06162262e+02 -1.53613591e+02
  7.41874695e+02 -7.95327786e+01  9.47718047e+04  1.00923162e+02
  2.90630996e+04  8.19332895e+01  2.14659492e+04  5.92739867e+01
  7.11090058e+02  1.43069462e+01  3.73723999e+02  8.11065669e+00
  1.49070740e+02  6.00379982e+01 -1.00000001e-01  9.06968811e-01
 -1.71420654e+00  0.00000000e+00 -7.12587610e+01  4.56834979e+04
  1.62593963e+02  1.13155667e+05  3.55577608e+01  1.25566936e+05
```



For each method, the y-axis in the above graph shows accuracy, precision, recall, and FSCORE. Based on this graph, we can conclude that KNN produced

6 CONCLUSION & FUTURE SCOPE

This project offers a CPPS operating model and fixes the related vulnerabilities that an attacker might exploit. On the basis of the CPPS paradigm, we categorise the current attack strategies used against various components. The state-of-the-art in the field was reviewed and categorised using the most innovative operational defence strategies, which included everything from the state estimation based detector to new moving target defence and watermarking techniques. Significant attack surfaces are introduced, along with a wide range of opportunities and problems, as smart grid technologies spread and more physical objects are connected to the cyber-physical infrastructures. The examination into the cyber-physical security of smart grids revealed four difficulties. Our poll reveals information about the need for future study into a new set of cyber-physical security issues.
s better results.

REFERENCES

[1] C.-P. S. P. W. Group et al., “Framework for cyber-physical systems: Volume 1, overview, version 1.0,” NIST Special Publication, pp. 1500– 201, 2017.

[2] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” IET Cyber-Physical Systems: Theory Applications, vol. 1, no. 1, pp. 13–27, 2016.

[3] G. Loukas, “1 - a cyber-physical world,” in CyberPhysical Attacks, G. Loukas, Ed. Boston: ButterworthHeinemann, 2015, pp. 1 – 19. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128012901000011

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," vol. 100, no. 1, pp. 210–224. [Online]. Available: http://ieeexplore.ieee.org/document/6032699/

[5] T. C. Reed, At the abyss: an insider's history of the Cold War. Presidio Press, 2005.

[6] T. L. Hardy, Software and System Safety. AuthorHouse, 2012.