DETECTING ELECTRICAL THEFT IN SMART GRIDS USING MACHINE LEARNING

[1] K.Venkata Ramaiah, Associate Professor, Department of CSE, Chalapathi Institute of Technology, Guntur.
[2] Yechuri Bhavyasri, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[3] Pabolu Lakhsmi Manasa, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[4] Mupparaju Anusha, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[5] Valeti Chanakya Siva Phanish, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.

Abstract: Electricity theft is a global problem that negatively affects both utility companies and electricity users. It destabilizes the economic development of utility companies, causes electric hazards and impacts the high cost of energy for users. The development of smart grids plays an important role in electricity theft detection since they generate massive data that includes customer consumption data which, through machine learning and deep learning techniques, can be utilized to detect electricity theft. This paper introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach. We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features. We improve the electricity theft detection performance by optimizing hyper parameters using a Bayesian optimizer and we employ an adaptive moment estimation optimizer to carry out experiments using different values of key parameters to determine the optimal settings that achieve the best accuracy. Lastly, we show the competitiveness of our method in comparison with other methods evaluated on the same dataset. On validation, we obtained 97% area under the curve (AUC), which is 1% higher than the best AUC in existing works, and 91.8% accuracy, which is the second-best on the benchmark.

1. INTRODUCTION

ELECTRICITY theft is a problem that affects utility companies worldwide. More than $96 billion is lost by utility companies worldwide due to Non-Technical Losses (NTLs) every year, of which electricity theft is the major contributor [1]. In sub-Saharan Africa, 50% of generated energy is stolen, as reported by World Bank [2]. The ultimate goal of electricity thieves is to consume energy without being billed by utility companies [3], or pay the bills amounting to less than the consumed amount [4]. As a result, utility companies suffer a huge revenue loss due to electricity theft. [5] reports that in 2015, India lost $16.2 billion, Brazil lost $10.5 billion and Russia lost $5.1 billion. It is estimated that approximately $1.31 billion (R20 billion) revenue loss incurred by South Africa (through Eskom) per year is due to electricity theft [2].Apart from revenue loss, electricity theft has a direct negative impact on the stability and reliability of power grids [3]. It can lead to surging electricity, electrical systems overload and public safety threats such as electric shocks [4]. It also has a direct impact on energy tariff increases, which affect all customers [3]. Implementation of smart grids comes with many opportunities to solve the electricity theft problem [4]. Smart grids are usually composed of traditional power grids, smart meters and sensors, computing facilities to monitor and control grids, etc., all connected through the communication network [6]. Smart meters and sensors collect data such as electricity usage, grid status, electricity price, etc. [6]. Many Utilities sought to curb electricity theft in traditional grids by examining meters' installation and configurations, checking whether the power line is bypassed, etc. [4]. These methods are expensive, inefficient and cannot detect cyber attacks [4], [7]. Recently, researchers have worked towards detecting electricity theft by utilizing machine learning classification techniques using readily available smart meters data. These theft detection methods have proved to be of relatively lower costs [8]. However, existing classification techniques consider time-domain features and do not regard frequency-domain features, thereby limiting their performance. Regardless of the fact that there is active ongoing research on electricity theft detection, electricity theft is still a problem. The major cause of delay in solving this problem may be that smart grids deployment is realized in developed nations while developing nations are lagging behind [9]. The challenges of deploying smart grids include the lack of communication infrastructure and users' privacy concerns over data reported by the smart meters [10]. However, [10] reports that smart meters are being considered by many developed and developing countries with aims that include solving NTLs. [11] predicted smart grids global market to triple in size between 2017 and 2023, with the following key regions leading smart grids deployment: North America, Europe and Asia. In this paper, we present an effective electricity theft detection method based on carefully extracted and selected features in Deep Neural Network (DNN)-based classification approach. We show that employing frequency-domain features as opposed to using time-domain features alone enhances classi_cation performance. We use a realistic electricity consumption dataset released by State Grid Corporation of China (SGCC) accessible at [12]. The dataset consists of electricity consumption data taken from January 2014 to October 2016.

2. LITERATURE SURVEY

2.1 Q. Louw and P. Bokoro, ``An alternative technique for the detection and mitigation of electricity theft in South Africa,'' SAIEE Afr. Res. J., vol. 110, no. 4, pp. 209_216, Dec. 2019. [3] M.Anwar, N. Javaid, A. Khalid, M. Imran, and M. Shoaib, ``Electricity theft detection using pipeline in machine learning,'' in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020, pp. 2138_2142

Electricity theft and illicit ground surface conductor connections are widespread in South Africa. This phenomena not only causes revenue loss and equipment damage, but it also poses a life-threatening hazard. Despite decades of research into non- technical losses, no general solution has been given due to the problem's complexity. This research studies the use of zero-sequence current-based detection as a mitigation approach for dealing with unauthorized ground surface conductor connections. The validity of this technique, as well as its influence on seasonal changes in soil resistivity, is demonstrated by simulation and experimental data.

2.2 Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, ``Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids,'' IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1606_1615,Apr. 2018.

Power grids suffer as a result of electricity theft. Due to the abundance of data generated by smart grids, smart grids can assist in addressing the issue of electricity theft by integrating energy and information flows. Because energy thieves have an unusual pattern of using electricity, data analysis on smart grid data can be helpful in identifying thefts. However, due to the fact that the majority of them were conducted on one-dimensional (1-D) electricity consumption data and failed to capture the periodicity of electricity consumption, the existing methods have poor detection accuracy of electricity theft.

To address the aforementioned concerns, we initially propose a novel electricity-theft detection method based on the wide and deep CNN model in this paper. In particular, there are two parts to the wide and deep CNN model: the deep CNN component in addition to the wide component. Based on 2-D electricity consumption data, the deep CNN component is able to precisely identify the periodicity of normal usage and the nonperiodicity of electricity theft. In the meantime, 1-D electricity consumption data's global characteristics can be captured by the wide component. Consequently, the wide and deep CNN model can perform exceptionally well in electricity-theft detection. Extensive testing on a real-world dataset demonstrates that the wide and deep CNN model performs better than other methods currently in use.

3. EXISTING SYSTEM

Electricity theft is a global problem that negatively affects both utility companies and electricity users. It destabilizes the economic development of utility companies, causes electric hazards and impacts the high cost of energy for users. The development of smart grids plays an important role in electricity theft detection since they generate massive data that includes customer consumption data which, through machine learning and deep learning techniques, can be utilized to detect electricity theft. This paper introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach. We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features.

DISADVANTAGES OF EXISTING SYSTEM

- An existing system not implemented dnn-based electricity theft detection method.
- An existing system not implemented hyperbolic tangent activation function.

4. PROPOSED SYSTEM

In propose paper we propose a novel DNN classification-based electricity theft detection method using comprehensive time-domain features. We further propose using frequency-domain features to enhance performance. We employ Principal Component Analysis (PCA) to perform classification with reduced feature space and compare the results with classification done with all input features to interpret the results and simplify the future training process. We further use the Minimum Redundancy Maximum Relevance (mRMR) scheme to identify the most significant features and validate the importance of frequency-domain features over time-domain features for detecting electricity theft. We optimize the hyper parameters of the model for overall improved performance using a Bayesian optimizer. We further employ an adaptive moment estimation (Adam) optimizer to determine the best ranges of values of the other key parameters that can be used to achieve good results with optimal model training speed. Lastly, we show 1% improvement in AUC and competitive accuracy of our model in comparison to other data-driven electricity theft detection methods in the literature evaluated on the same dataset.

ADVANTAGES

- High Accuracy for detecting electricity theft detection.

SYSTEM ARCHITECTURE

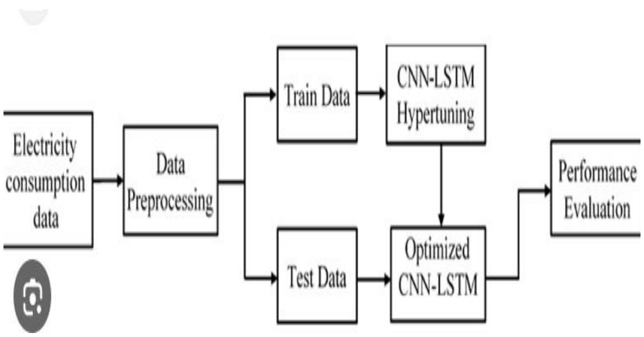
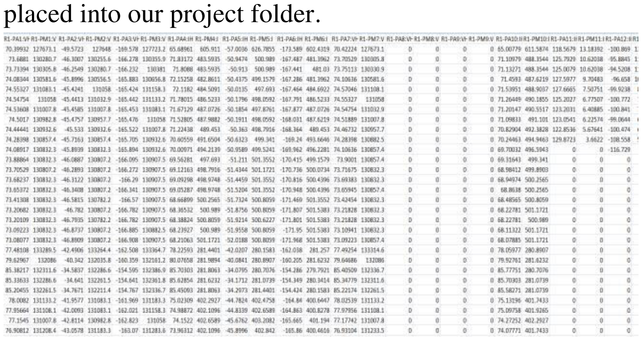


Fig 1: System Architecture

5. DATASET:

We can collect the dataset from the kaggle.com site and placed into our project folder.



R1-PA1:VH	R1-PM1:V	R1-PA2:VH	R1-PM2:V	R1-PA3:VH	R1-PM3:V	R1-PA4:IH	R1-PM4:I	R1-PA5:IH	R1-PM5:I	R1-PA6:IH	R1-PM6:I	R1-PA7:VH	R1-PM7:V	R1-PA8:VH	R1-PM8:V	R1-PA9:VH	R1-PM9:V	R1-PA10:IH	R1-PM10:I	R1-PA11:IH	R1-PM11:I	R1-PA12:IH
70.39932	127673.1	-49.5723	127648	-169.578	127723.2	65.68961	605.911	-57.0036	626.7855	-173.589	602.4319	70.42224	127673.1	0	0	0	0	65.00779	611.5874	118.5679	13.18392	-100.869
73.6881	130280.7	-46.3007	130255.6	-166.278	130355.9	71.83172	483.5935	-50.9474	500.989	-167.487	481.3962	73.70529	130305.8	0	0	0	0	71.10979	488.3544	125.7929	10.62038	-95.8845
73.73394	130305.8	-46.2549	130280.7	-166.232	130381	71.8088	483.5935	-50.913	500.989	-167.441	481.03	73.75113	130330.9	0	0	0	0	71.13271	488.3544	125.0079	10.62038	-94.5208
74.08344	130581.6	-45.8996	130556.5	-165.883	130656.8	72.15258	482.8611	-50.4375	499.1579	-167.286	481.3962	74.10636	130581.6	0	0	0	0	71.4593	487.6219	127.5977	9.70483	-96.658
74.55327	131083.1	-45.4241	131058	-165.424	131158.3	72.1182	484.5091	-50.0135	497.693	-167.464	484.6922	74.57046	131108.1	0	0	0	0	71.53951	488.9037	127.6665	7.50751	-99.9238
74.54754	131058	-45.4413	131032.9	-165.442	131133.2	71.78015	486.5233	-50.1796	498.0592	-167.791	486.5233	74.55327	131058	0	0	0	0	71.26449	490.1855	125.2027	6.77507	-100.772
74.53608	131007.8	-45.4585	131007.8	-165.453	131083.1	71.67129	487.0726	-50.1854	497.8761	-167.877	487.0726	74.54754	131032.9	0	0	0	0	71.20147	490.5517	123.2031	6.40885	-100.841
74.5017	130982.8	-45.4757	130957.7	-165.476	131058	71.52805	487.9882	-50.1911	498.0592	-168.031	487.6219	74.51889	131007.8	0	0	0	0	71.09833	491.101	123.0541	6.22574	-99.0644
74.44441	130932.6	-45.533	130932.6	-165.522	131007.8	71.22438	489.453	-50.363	498.7916	-168.364	489.453	74.46732	130957.7	0	0	0	0	70.82904	492.3828	122.8536	5.67641	-100.474
74.28398	130857.4	-45.7163	130857.4	-165.705	130932.6	70.60559	491.6504	-50.6323	499.341	-169.24	493.6646	74.28398	130882.5	0	0	0	0	70.24463	494.9463	129.8723	3.6622	-108.558
74.08917	130832.3	-45.8939	130832.3	-165.894	130932.6	70.00971	494.2139	-50.9589	499.5241	-169.962	496.2281	74.10636	130857.4	0	0	0	0	69.70032	496.5943	0	0	-116.729
73.88864	130832.3	-46.0887	130807.2	-166.095	130907.5	69.56281	497.693	-51.211	501.3552	-170.415	499.1579	73.9001	130857.4	0	0	0	0	69.31643	499.341	0	0	0
73.70529	130807.2	-46.2893	130807.2	-166.272	130907.5	69.12163	498.7916	-51.4344	501.1721	-170.736	500.0734	73.71675	130832.3	0	0	0	0	68.98412	499.8903	0	0	0
73.68237	130832.3	-46.3122	130807.2	-166.29	130907.5	69.09298	498.9748	-51.4459	501.3552	-170.816	500.4396	73.69383	130832.3	0	0	0	0	68.94974	500.2565	0	0	0
73.65372	130832.3	-46.3408	130807.2	-166.341	130907.5	69.05287	498.9748	-51.5204	501.3552	-170.948	500.4396	73.65945	130857.4	0	0	0	0	68.8638	500.2565	0	0	0
73.41308	130832.3	-46.5815	130782.2	-166.57	130907.5	68.66899	500.2565	-51.7324	500.8059	-171.469	501.3552	73.42454	130832.3	0	0	0	0	68.48565	500.8059	0	0	0
73.20682	130832.3	-46.782	130807.2	-166.782	130907.5	68.36532	500.989	-51.8756	500.8059	-171.807	501.5383	73.21828	130832.3	0	0	0	0	68.22781	501.1721	0	0	0
73.20109	130832.3	-46.7935	130782.2	-166.782	130907.5	68.38824	500.8059	-51.9214	500.6227	-171.801	501.5383	73.21828	130832.3	0	0	0	0	68.22781	500.989	0	0	0
73.09223	130832.3	-46.8737	130807.2	-166.885	130882.5	68.23927	500.989	-51.9558	500.8059	-171.95	501.5383	73.10941	130832.3	0	0	0	0	68.11322	501.1721	0	0	0
73.08077	130832.3	-46.8909	130807.2	-166.908	130907.5	68.21063	501.1721	-52.0188	500.8059	-171.968	501.5383	73.09223	130857.4	0	0	0	0	68.07885	501.1721	0	0	0
77.48108	133289.5	-42.4906	133264.4	-162.508	133364.7	78.22593	281.4401	-42.0207	280.1583	-162.038	281.257	77.49254	133314.6	0	0	0	0	78.05977	280.8907	0	0	0
79.62967	132086	-40.342	132035.8	-160.359	132161.2	80.07658	281.9894	-40.0841	280.8907	-160.205	281.6232	79.64686	132086	0	0	0	0	79.92761	281.6232	0	0	0
85.38217	132311.6	-34.5837	132286.6	-154.595	132386.9	85.70303	281.8063	-34.0795	280.7076	-154.286	279.7921	85.40509	132336.7	0	0	0	0	85.77751	280.7076	0	0	0
85.33633	132286.6	-34.641	132261.5	-154.641	132361.8	85.62854	281.6232	-34.1712	281.0739	-154.349	280.3414	85.34779	132311.6	0	0	0	0	85.70303	281.0739	0	0	0
85.20455	132261.5	-34.7671	132211.4	-154.767	132336.7	85.45093	281.8063	-34.2073	281.4401	-154.424	280.1583	85.22174	132261.5	0	0	0	0	85.58271	281.0739	0	0	0
78.0082	131133.2	-41.9577	131083.1	-161.969	131183.3	75.02309	402.2927	-44.7824	402.4758	-164.84	400.6447	78.02539	131133.2	0	0	0	0	75.13196	401.7433	0	0	0
77.95664	131108.1	-42.0093	131083.1	-162.021	131158.3	74.98872	402.1096	-44.8339	402.6589	-164.863	400.8278	77.97956	131108.1	0	0	0	0	75.09758	401.9265	0	0	0
77.1545	131007.8	-42.8114	130982.8	-162.823	131058	74.1522	402.6589	-45.6762	403.2082	-165.665	401.194	77.17742	131007.8	0	0	0	0	74.27252	402.2927	0	0	0
76.90812	131208.4	-43.0578	131183.3	-163.07	131283.6	73.96312	402.1096	-45.8996	402.842	-165.86	400.4616	76.93104	131233.5	0	0	0	0	74.07771	401.7433	0	0	0
76.67894	131509.3	-43.287	131484.2	-163.299	131584.5	73.75113	401.0109	-46.0773	401.9265	-165.957	399.9122	76.69613	131534.4	0	0	0	0	73.90583	401.0109	0	0	0

Table 5.1: Electricity data

6. UML DIAGRAMS

1. CLASS DIAGRAM

The cornerstone of event-driven data exploration is the class outline. Both broad practical verification of the application's precision and fine-grained demonstration of the model translation into software code rely on its availability. Class graphs are another data visualisation option.

The core components, application involvement, and class changes are all represented by comparable classes in the class diagram. Classes with three-participant boxes are referred to be "incorporated into the framework," and each class has three different locations:

• The techniques or actions that the class may use or reject are depicted at the bottom.

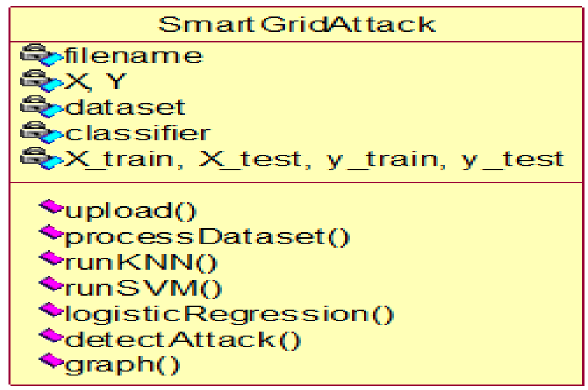


Fig 6.1 shows the class diagram of the project

2. USECASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

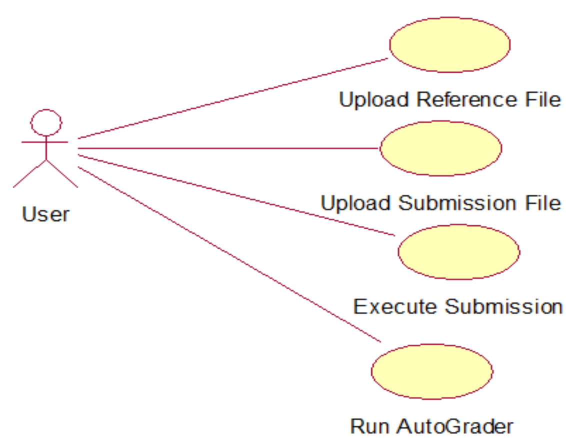


Fig 6.2 Shows the Use case Diagram

3. SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

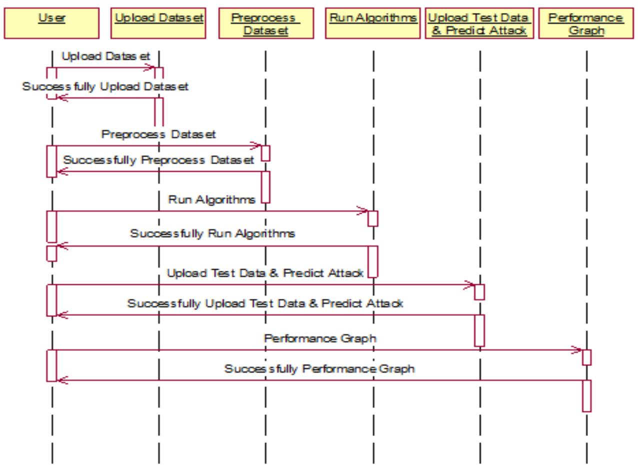


Fig 6.3 Shows the Sequence Diagram

7. RESULTS

7.1 Output Screens

Fig 7.1 Upload the Dataset

In above screen click on 'Upload Smart Grid Dataset' button and upload dataset

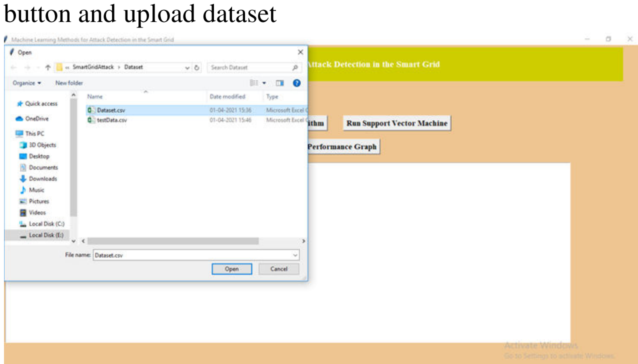


Fig 7.2 Uploading the Dataset File

In above screen we are selecting and uploading 'Dataset.csv' file and then click on 'Open' button to load dataset and to get below screen

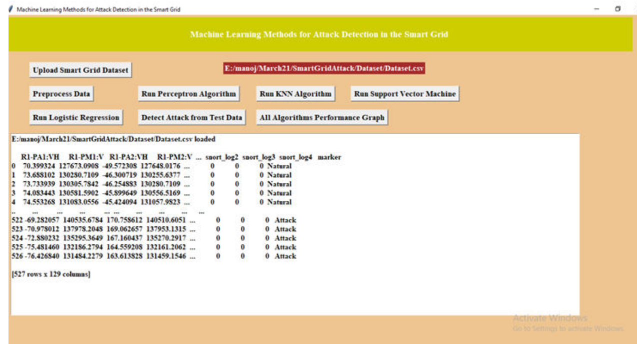


Fig 7.3 Preprocess the dataset

In above screen dataset loaded and we can see above dataset showing non-numeric values and to replace them click on 'Preprocess Data' to replace with numeric values

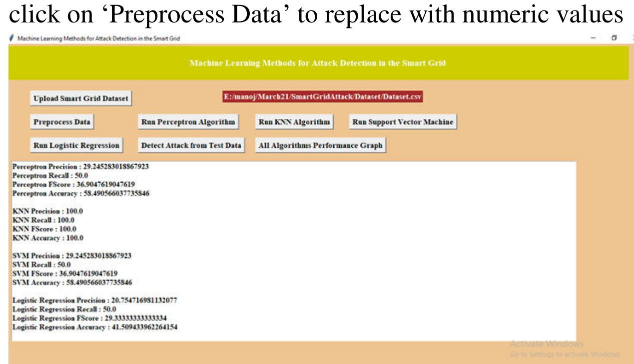


Fig 7.4 Run the KNN Algorithm

In above screen I clicked on all 4 algorithms button and then we got accuracy, precision, recall and FSCORE of each algorithm and in all algorithm KNN is giving better performance result. Now we can upload test data and then ML algorithm will predict class label as normal or attack. In below test data we can see we have vector values but we don't have class label and this class label will be predicted by ML

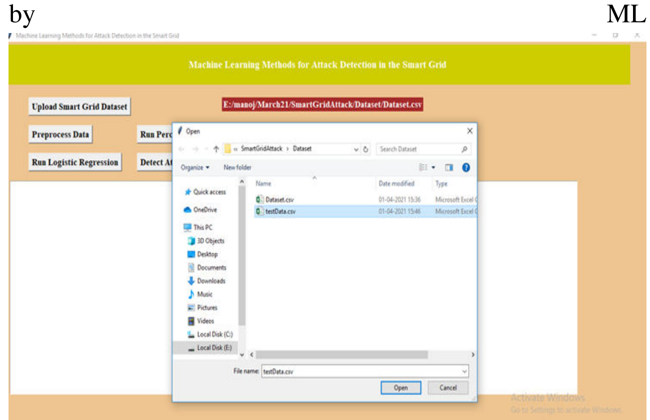


Fig 7.5 Upload the test.csv file

In above screen selecting and uploading 'testData.csv' file and then click on 'Open' button to get below result

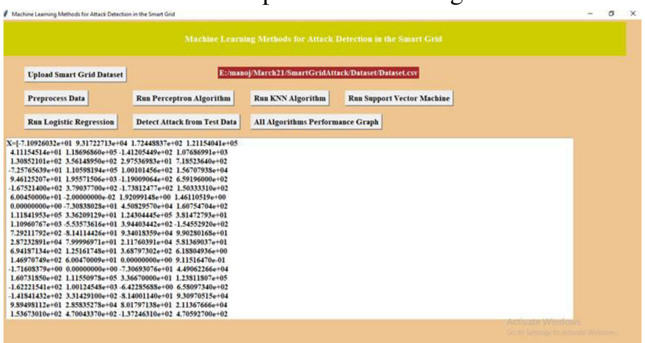


Fig 7.6 Detection Accuracy

In above screen in square bracket we have grid vector values and after square bracket we can see predicted result as below screen and to see predicted result

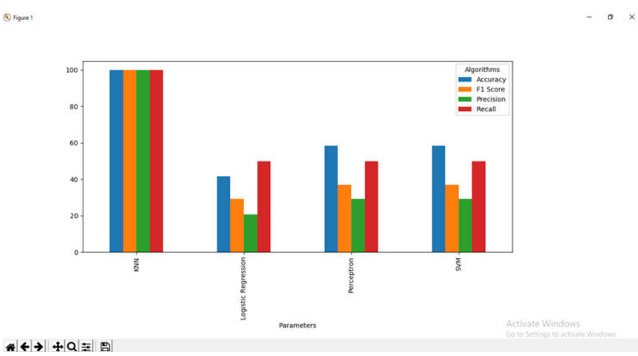


Fig 7.7 Accuracy Comparison Graph

In above graph x-axis represents algorithm name and y-axis represents accuracy, precision, recall and FSCORE for each algorithm and from above graph we can say KNN is giving better result

8. CONCLUSION

The attack detection problem has been reformulated as a machine learning problem and the performance of supervised, semisupervised, classifier and feature space fusion, and online learning algorithms have been analyzed for different attack scenarios. In a supervised binary classification problem, the attacked and secure measurements are labeled in two separate classes. In the experiments, we have observed that the state-of-the-art machine learning algorithms perform better than the well-known attack detection algorithms that employ an SVE approach for the detection of both observable and unobservable attacks. We have observed that the perceptron is less sensitive and the k-NN is more sensitive to the system size than the other algorithms. In addition, the imbalanced data problem affects the performance of the k-NN. Therefore, k-NN may perform better in small-sized systems and worse in large-sized systems when compared to other algorithms.

9. REFERENCES

[1] C. Rudin et al., "Machine learning for the New York City power grid," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 2, pp. 328–345, Feb. 2012.

[2] R. N. Anderson, A. Boulanger, W. B. Powell, and W. Scott, "Adaptive stochastic control for the smart grid," Proc. IEEE, vol. 99, no. 6, pp. 1098–1115, Jun. 2011.

[3] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, Sep./Oct. 2011.

[4] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[5] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1306–1318, Jul. 2013. This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination. OZAY et al.: MACHINE LEARNING METHODS FOR ATTACK DETECTION IN THE SMART GRID 13

[6] A. Abur and A. G. Expósito, Power System State Estimation: Theory and Implementation. New York, NY, USA: Marcel Dekker, 2004.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. 16th ACM Conf. Comput. Commun. Secur., Chicago, IL, USA, Nov. 2009, pp. 21–32. [8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[9] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the North American electric power infrastructure," IEEE Syst. J., vol. 6, no. 4, pp. 616–626, Dec. 2012.

[10] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[11] E. J. Candès and T. Tao, “Decoding by linear programming,” IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[12] D. L. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[13] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, “Smarter security in the smart grid,” in Proc. 3rd IEEE Int. Conf. Smart Grid Commun., Tainan, Taiwan, Nov. 2012, pp. 312–317. [14] L. Saitta, A. Giordana, and A. Cornuéjols, Phase Transitions in Machine Learning. New York, NY, USA: Cambridge Univ. Press, 2011.

[15] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, “Distributed models for sparse attack construction and state vector estimation in the smart grid,” in Proc. 3rd IEEE Int. Conf. Smart Grid Commun., Tainan, Taiwan, Nov. 2012, pp. 306–311.

[16] O. Bousquet, S. Boucheron, and G. Lugosi, “Introduction to statistical learning theory,” in Advanced Lectures on Machine Learning, O. Bousquet, U. von Luxburg, and G. Rätsch, Eds. Berlin, Germany: Springer-Verlag, 2004.

[17] S. Kulkarni and G. Harman, An Elementary Introduction to Statistical Learning Theory. Hoboken, NJ, USA: Wiley, 2011.

[18] Q. Wang, S. R. Kulkarni, and S. Verdú, “Divergence estimation for multidimensional densities via k-nearest-neighbor distances,” IEEE Trans. Inf. Theory, vol. 55, no. 5, pp. 2392–2405, May 2009.

[19] S. Theodoridis and K. Koutroumbas, Pattern Recognition. Orlando, FL, USA: Academic, 2006.

[20] R. D. Duda, P. E. Hart, and D. G. Stork, Pattern Classification. New York, NY, USA: Wiley, 2001.