ISSN No:-2456-2165

Detection and Location of a Cyber Attack in an Active Distribution System

Dr. A. Manjula, M.Sai Prasad, B. Pragnya, D. Sahithya, K. Pranay, K. Avinash, M. Pradeep
[1,2]Associate Professor, [3,4,5,6,7]Student
Department of CSE, Jyothishmathi Institute of Technology and Science, Telangana

Abstract:- Creating a cyber security strategy for active distribution systems is challenging due to the integration of distributed renewable energy source. This essay presents a methodology for adaptive hierarchical cyber-attack localisation and detection for distributed active distribution systems utilising electrical waveform analysis. The foundation for cyber attack detection is a sequential deep learning model, which enables the detection of even the tiniest cyberattacks. The two-stage approach first estimates the cyber-attack sub-region before localising the specified cyber-attack within it. For the "coarse" localization of hierarchical cyber-attacks, we propose a modified spectral clustering-based method of network partitioning. Second, it is recommended to use a normalised impact score based on waveform statistical metrics to further pinpoint the location of a cyber attack by defining various waveform features.Finally, a detailed quantitative evaluation using two case studies shows that the proposed framework produces good estimation results when compared to established and cutting-edge approaches.

Keywords:- *SVM, Random Forest, Gradient Boosting, Logistic Regression, Cyber Attack Detection.*

I. INTRODUCTION

Cyber-attacks have become more sophisticated in recent years, particularly those that target systems that store or handle sensitive information. As vital information or services depend on critical national infrastructures, protecting them from cyberattacks becomes a significant problem for both corporations and countries. Intrusion detection systems (IDS) are utilised as a secondary line of defence in addition to current preventive security techniques like access restriction and authentication.IDS is able to differentiate between legitimate conduct and malicious behaviour based on a set of specified rules or patterns[1].

Power electronics converters are more susceptible to cyber/physical attacks as a result of their rising use in Internet of Things (IoT) enabled applications, such as smart grids. Because there is a dearth of cyber knowledge within the power electronics industry, it is more important than ever to create techniques for power electronics converters to detect and identify cyber/physical attacks in many safety-critical applications. These malicious assaults have the potential to cause catastrophic failure and severe financial loss if they are not identified in the early stages [2]. Employing extensive smart metre data, a hierarchical architecture for anomaly detection in smart grids. The suggested methodology is intended to identify anomalies at several smart grid levels, including as the transmission, substation, and distribution levels [3].

Modern electric vehicles' power train systems' cyber-physical security (EVs). The paper discusses the weaknesses and difficulties of EV power train systems, including intrusions on the communication networks, electric motor control, and battery management system [4]. Using support vector machines, a hierarchical intrusion detection system (IDS) for industrial control networks (SVMs). The suggested approach is intended to identify and categorise various intrusion types, such as reconnaissance assaults, DoS attacks, and data modification attacks. The models distinguish between typical and aberrant network behaviour using a variety of parameters, including packet size and frequency [5] a data-driven technique based on synchronised phasor measurement for locating single-phase grounding faults in distribution networks. The suggested approach makes use of the synchronised phasor data to determine the fault's location and kind as well as to calculate the fault resistance [6] a smart system that uses deep learning to detect fake data injection assaults in real time in smart grids. In order to identify aberrant changes brought on by bogus data injection assaults and learn the temporal patterns of the power system data, the suggested approach makesa use of neural network with long short-term memory (LSTM) [7].

II. RELATED WORK

A cutting-edge intrusion detection system (IDS) incorporating the REP Tree, JRip algorithm, and Forest PA classifier approaches, all of which are founded on decision trees and rules-based ideas. Characteristics from the initial data set as well as the results of the first and second classifiers are inputs for the third classifier. Using the CICIDS2017 dataset, which was proposed by Mehmood et al [1], the experimental results show that the suggested IDS is superior to current state-of-the-art approaches in terms of precision, rate of detection, frequency of false alarms, and time overhead.Distribution power grid security is at risk from both physical and digital attacks. Photovoltaics (PVs), one of the burgeoning renewable energy sources, introduces new potential vulnerabilities. In this paper, an existing system creates a novel high-dimensional data-driven cyber physical attack detection and identification (HCADI) approach based on the electric waveform data collected by waveform sensors in the distribution power networks and was proposed by F. Li, R. Xiewt. al [2].

ISSN No:-2456-2165

Smart grids (SGs) must be monitored and controlled in real time if power utilities are to increase operational efficiency and reliability. We create a real-time anomaly detection system that is based on data gathered from smart metres (SM) installed at customers' homes. The approach is intended to identify unusual occurrences and circumstances at both the lateral and consumer levels. We put forth a generative model for anomaly identification that considers both the network's hierarchical structure and the information gathered from SMs,was proposed by Li, G., Lu, Z et al [3].

Power electronics systems have become more susceptible to cyber-physical attacks as a result of their increased use in Internet of Things (IoT) enabled applications, such connected electric automobiles (EVs). In response to this expanding need, the IEEE Power Electronics Society recently established a cyber-physical security initiative (PELS). The hypothesis advanced by J. Ye, L. Guo, and others [4] that linked electric vehicles would experience a higher cyber-physical security concern when connectivity grows as a result of Vehicle-to-everything (V2X) and the number of electronic control units.

With the advancement of information technology, standard Ethernet is gradually being used in industrial control systems. It dismantles the ICS's built-in isolation but lacks any security features. For modern ICS, a customised intrusion detection system (IDS) that is closely associated to a particular industrial scenario is required. On the one hand, this study describes many attack strategies, such as our inventive forging assault and penetration attacks. On the other hand, we offer a hierarchical IDS that has both a model for anomaly detection and a model for traffic forecasting. The autoregressive integrated moving average (ARIMA)-based traffic prediction model can predict the short-term traffic of the ICS network and may reliably identify infiltration attacks in response to abnormal changes in traffic patterns. Raza [5] suggested using the anomaly detection model.Power systems' single-phase grounding faults are influenced by a number of variables as a result of the expanding sizes and rising complexity of these systems. We suggest a modified approach using synchronised phasor measurement to capitalise on big data in power systems. The data-driven approach is used to locate and identify single-phase grounding faults, proving the connection between eigenvalues and power system state that B. Wang et al. [6] proposed.

The use of computer and communications intelligence greatly raises the standard of smart grid monitoring and control. The reliance on information technology dramatically increases the susceptibility to destructive attacks. False data injection (FDI), a data integrity attack, is currently posing a severe danger to the supervisory control and data acquisition system. As suggested by Y. He et al. [7], we employ deep learning techniques in this study to identify the behavioural traits of FDI attacks using historical measurement data. We then use the gained behavioural traits to recognise FDI attacks in real-time.

A. Proposed Scheme

The system suggests an electrical waveform-based adaptive hierarchical structure for active distribution systems with DERs for cyber-attack detection and localization.

To assess the effects of cyber attacks on distribution networks, high quality models of DER and cyber attacks are developed;

To assess the suggested approach's performance with quantitative analytics, numerous experiments are used. The cyber assault can be identified in the suggested system based on the monitoring measures' departure from steady-state, which is a challenge for anomaly identification according to our research.The strategy suggests first dividing the active distribution systems into various sub regions in order to properly locate the cyberattacks.

- *Service Provider*

The Service Provider must enter a valid user name and password to log in to this module. Figure 1 tells about the Service Provider flow chart, after successfully logging in, he can perform a number of actions, including log in, train and test cyber data sets, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, View Cyber Datasets Trained Accuracy in Bar Chart, View Cyber Datasets Trained Accuracy Results, Download Predicted Datasets, See the results of the cyberattack type ratio for all remote users.

ISSN No:-2456-2165

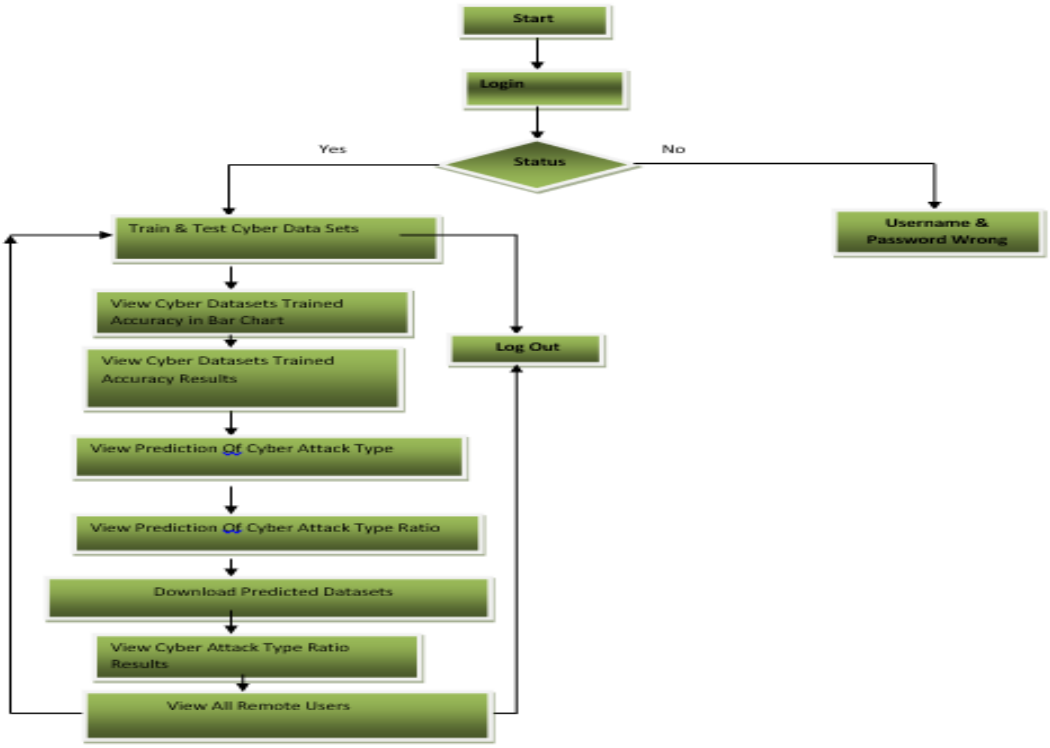

Fig. 1: Service Provider Flow Chart

➢ *View and authorized user*

The list of people who have registered can be seen by the administrator in this module. The admin can examine the user's information in this, including user name, email address, and address, and admin can also authorise users.

➢ *Remote User*

A total of n users are present in this module. Figure 2 tells about the Remote User flow chart. Before conducting any actions, users need register. Following registration, the database will store the user's information. He must log in using an authorised user name and password after successfully registering. Users can perform tasks like REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, and SEE YOUR PROFILE after successful login.

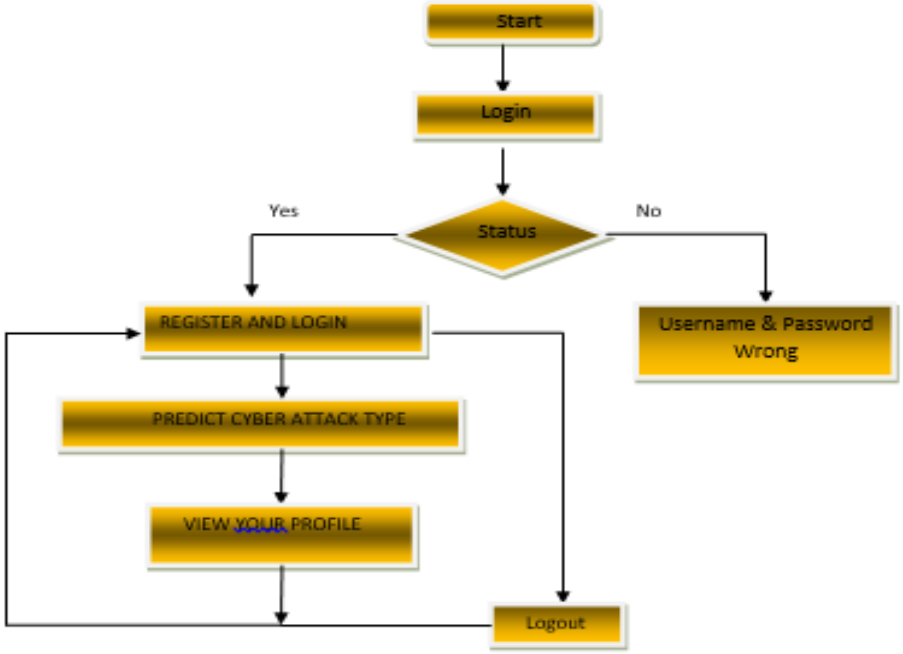

Fig. 2: Remote User Flow Chart

B. ARCHITECTURE

In order to learn from fresh data and adapt to changes in the active distribution system, the Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution System architecture was created to be adaptive. Figure 3 proposed architecture makes it suitable for real-world applications where the active distribution system is constantly evolving. This architecture consists of three modules they are service provider, view and authorized user and remote user. The service provider consists of login, train& test cyber data sets view cyber datasets trained accuracy in bar chart, view cyber datasets trained accuracy results, view prediction of cyber-attack type, view prediction of cyber-attack type ratio, download predicted datasets, view cyber Attack type ratio results and view remote users. The Web Server is connected to web database for accessing data and web server also connected to service provider for acceptingall informationand datasets results storage.The web database is used for Store and retrievals of data from service providers. The remote users should register and login, predict cyber-attack type, view your profile into the page.

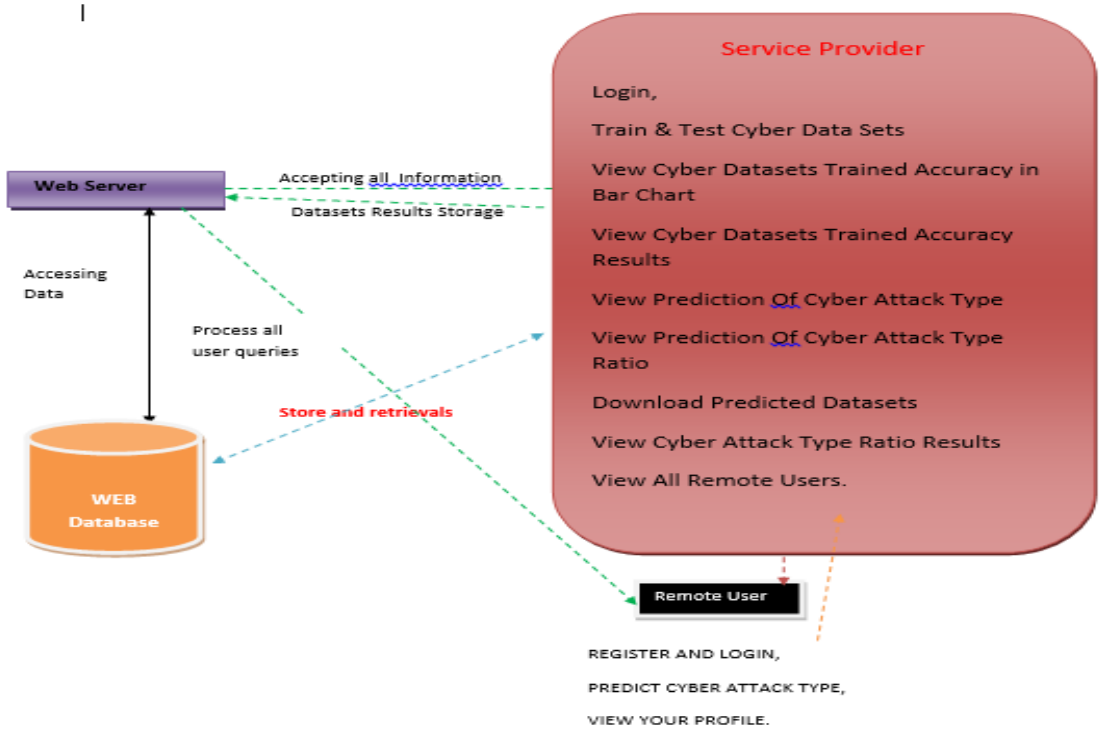

Fig. 3: Proposed Architecture

III. METHODOLOGIES

A. GRADIENT BOOSTING

For classification and regression analysis, machine learning algorithms called gradient boosting are used. By assembling a group of weak decision trees that have been trained on various subsets of the data, it operates. Combining all of the decision trees' projections yields the ultimate conclusion.

The adaptive hierarchical approach using gradient boosting involves the use of multiple layers of detection mechanisms that are organized hierarchically. At each layer, gradient boosting classifiers are used to classify system data and identify potential cyber-attacks. The top layer of the hierarchy consists of a broad-based detection mechanism that uses a gradient boosting classifier to identify known attack patterns and deviations from normal system behaviour. The classifier is trained on historical data and is capable of identifying common attack signatures and anomalies.

The middle layer of the hierarchy consists of more specific detection mechanisms that use gradient boosting classifiers to identify attacks that have bypassed the top-level detection mechanisms. These classifiers are trained on more specialized data and can identify attacks that are specific to certain components or behaviours within the system. The bottom layer of the hierarchy consists of response mechanisms that are activated once an attack has been detected. These mechanisms can include automated responses such as blocking traffic, quarantining infected systems, and alerting security personnel.Gradient boosting machine learning approach flowchart(Fig 4). A number of weak classifiers make up the ensemble classifiers. In the following classifier, the weights of the erroneously predicted points are increased. The weighted average of the individual predictions serves as the basis for the final judgement.

In addition to detection and response mechanisms, adaptive hierarchical cyber-attack detection and localization in active distribution systems using gradient boosting also includes localization mechanisms that can pinpoint the location of the attack. These mechanisms use techniques such as network topology analysis and geo-location to identify the source of the attack and the affected components in the system.

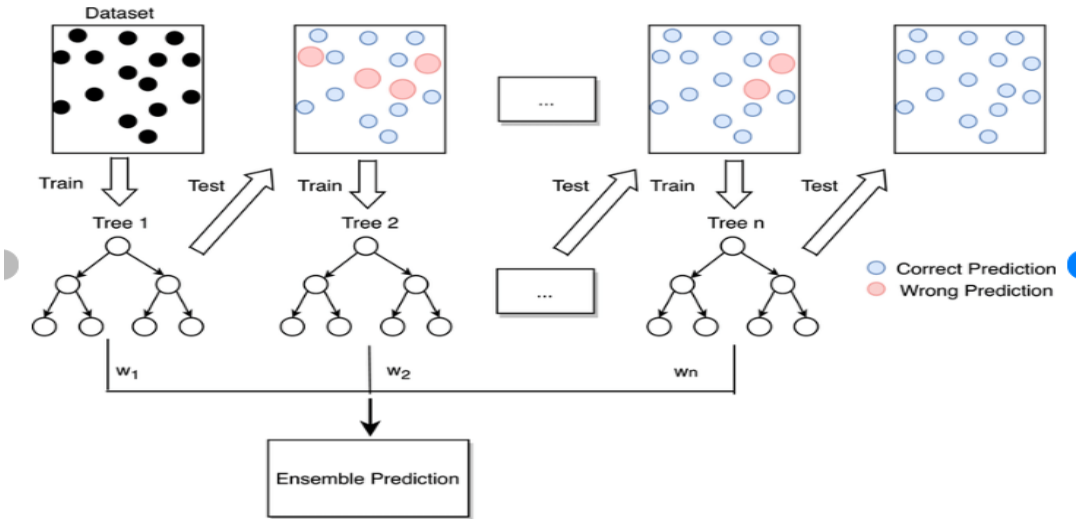

Fig. 4: Gradient Boosting

B. K-NEAREST NEIGHBORS (KNN)

Based on a similarity metric, this straightforward but extremely effective classification algorithm classifies objects. Lazy learning method that is non-parametric and waits to "learn" until the test example is shown. We determine a new data's K-nearest neighbors from the training data whenever we have new data to categorize. The fig 5 K-Nearest Neighbors (KNN) tells about the data points before applying KNN and after applying KNN.

➢ *Example:*

Because instances near to the input vector for the test or prediction may take some time to appear in the training dataset, learning based on instances also operates lazily. The means and space with categorization factors (non-metric variables) constitute feature space, and the training dataset is made up of the k-closest samples in feature space.

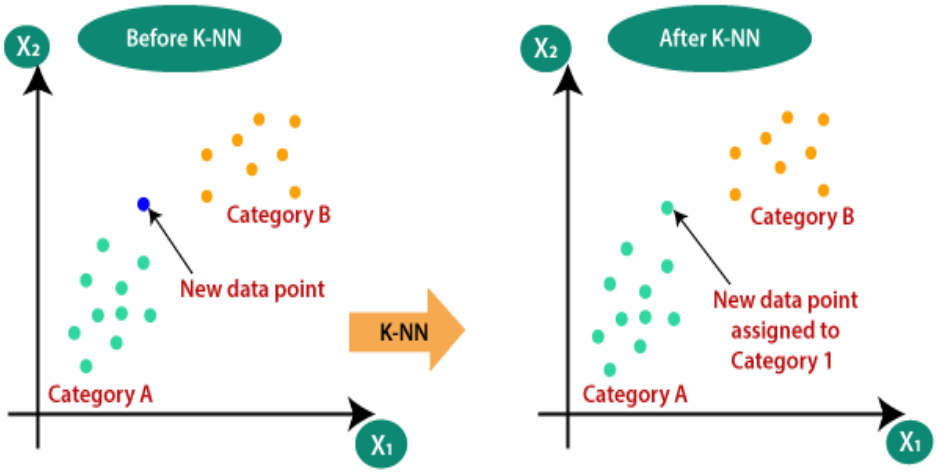

Fig. 5: K-Nearest Neighbors (KNN)

C. LOGISTIC REGRESSION CLASSIFIERS

The link between a collection of independent (explanatory) variables and a categorical dependent variable is examined using logistic regression analysis. The phrase "logistic regression" is used when the dependent variable only has two values, such as 0 and 1 or Yes and No. When the dependent variable, such as Married, Single, Divorced, or Widowed, has three or more distinct values, the term multinomial logistic regression is typically employed.Despite using a different set of data for the dependent variable than multiple regression, the method has a similar practical use.

This software computes binary logistic regression and multinomial logistic regression for independent variables that are both numerical and categorical. It contains details on odds ratios, confidence intervals, probability, and deviance as well as the regression equation. There is a detailed residual analysis performed, complete with diagnostic residual charts and reports. By carrying out an independent variable subset selection, it can search for the best regression model with the fewest independent variables. To help choose the ideal cut-off point for classification, it offers ROC curves and confidence intervals on predicted values. By automatically identifying rows that are not used in the study, it enables you to verify your results.

ISSN No:-2456-2165

The below shown fig 6 depicts about the logistic regression classifiers.The naive bays approach is a supervised learning technique that relies on the overly-simplistic premise that each feature of a class, whether present or absent, is unrelated to any other feature. But even so, it seems powerful and efficient. Its effectiveness is on par with that of other supervised learning method. There are numerous justifications offered in the literature. We emphasise a representation bias-based explanation in this tutorial. The naive Bayes classifier, linear discriminant analysis, logistic regression, and linear support vector machines are examples of linear classifiers (support vector machine). The approach used to estimate the classifier's parameters accounts for the disparity (the learning bias).

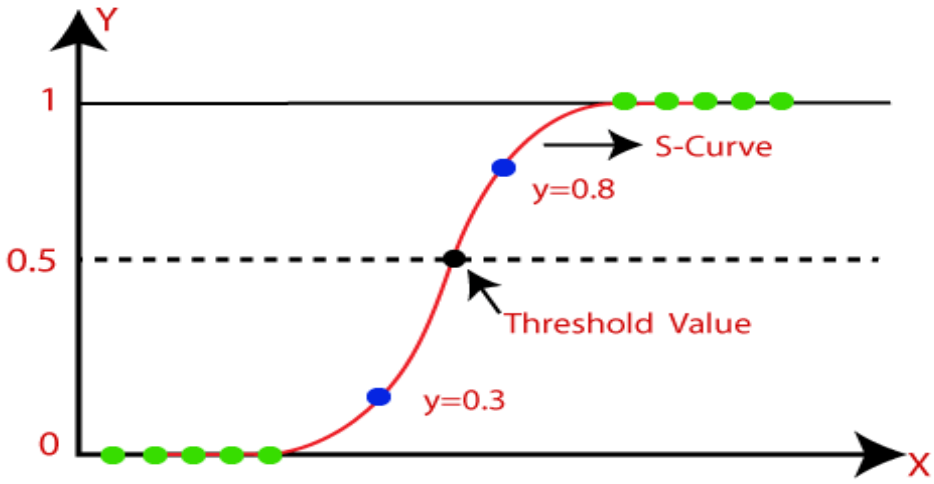

Fig. 6: Logistic Regression Classifiers

D. RANDOM FOREST

Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution System using Random Forest is a technique that aims to detect and localize cyber-attacks in active distribution systems.To categorise and pinpoint the kind of cyber-attack that has taken place in the system, the technique uses machine learning techniques, notably the Random Forest algorithm.

The method uses a hierarchical structure to raise the detection and localization process' accuracy. The hierarchical structure is based on a set of rules that are used to classify the type of cyber-attack that has occurred. The rules are organized in a hierarchical manner based on the severity of the cyber-attack, with the most severe attacks being classified first.

The model is trained using the Random Forest technique using a set of training data that contains different cyber-attacks. The algorithm creates a decision tree that is used to classify the type of attack based on the features of the attack. The features may include the source of the attack, the time of the attack, the type of attack, and other relevant information.

The sort of cyber-attack that has happened in the active distribution system is classified and located using the trained model, which is then used. The hierarchical structure is used to improve the accuracy of the detection and localization process by prioritizing the classification of severe attacks. The below figure 7 tells about the random forest in which it uses the training set and test set which will are applied training data for the prediction.

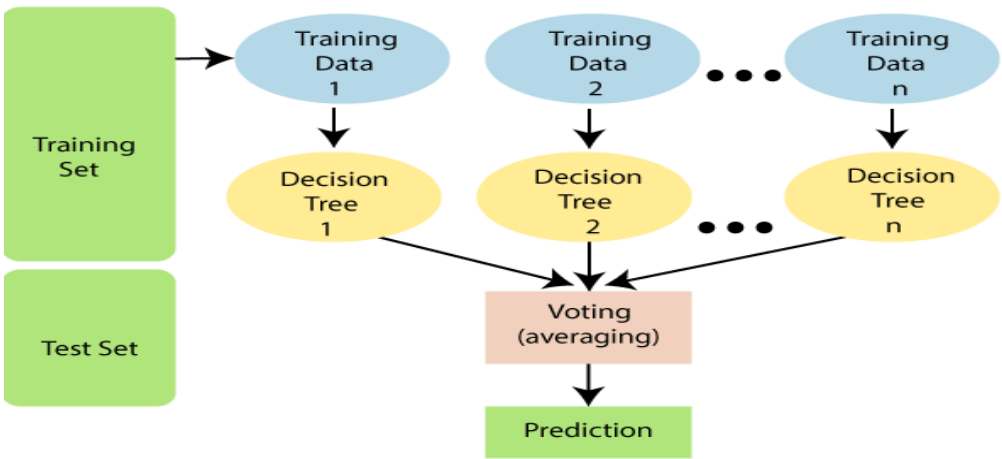

Fig. 7: Random Forest

ISSN No:-2456-2165

E. SVM

Using an independent and identically distributed (iid) training dataset, a discriminant machine learning technique for classification tasks seeks to identify a discriminant function that can precisely predict labels for recently acquired instances. In contrast to generative machine learning methods, which require the construction of conditional probability distributions, a discriminant classification function takes a data point x and assigns it to one of the different classes that are a component of the classification task. When outlier detection is a part of the prediction process, generative approaches are often used because discriminant processes are less effective. This is especially true for feature spaces with multiple dimensions and when just posterior probabilities are needed. Learning a classifier in terms of geometry is equivalent to finding the equation for a multidimensional surface that best divides the various classes in the feature space.

Below shown figure 8 shows SVM which is a discriminant approach, and unlike genetic algorithms (GAs) or perceptrons, both of which are frequently used for classification in machine learning, it always offers the same optimal hyperplane value since it solves the convex optimisation issue analytically. The initiation and termination requirements have a significant impact on perceptron solutions. While training provides uniquely defined SVM model parameters for a given training set for a specific kernel that converts the data from the input space to the feature space, perceptron and GA classifier models are distinct every time training is initialised.The purpose of GAs and perceptrons is to minimise error only during training, hence many hyperplanes will satisfy this criteria.

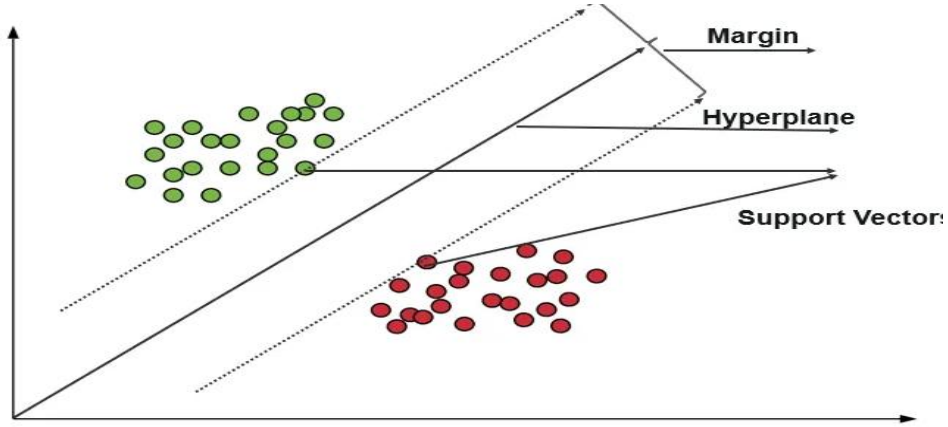

FIG 8: SVM

IV. RESULT ANALYSIS

Proposed methodology works is the following way. It consists of:

- Login
- Train & Test Cyber Data Sets
- View Cyber Datasets Trained Accuracy in Bar Chart
- View Cyber Datasets Trained Accuracy Results
- View Prediction Of Cyber Attack Type
- Download Predicted Datasets
- View Cyber Attack Type Ratio Results
- View All Remote Users.

A. Login Page

This below fig 9 consists of user register and user login. Here, user can register and login in to this page.

Fig. 9: Login Page

B. View Cyber Datasets Trained Accuracy Results

Below fig10 shows the accuracy of datasets in a bar chart.In this bar chart the accuracy of algorithms, they are SVM, random forest, KNN – neighbours classifiers and gradient boosting algorithms. The accuracy results are shown in bar chart, line chart and pie chart.

➢ *View Cyber Datasets Trained Accuracy in Bar Chart*

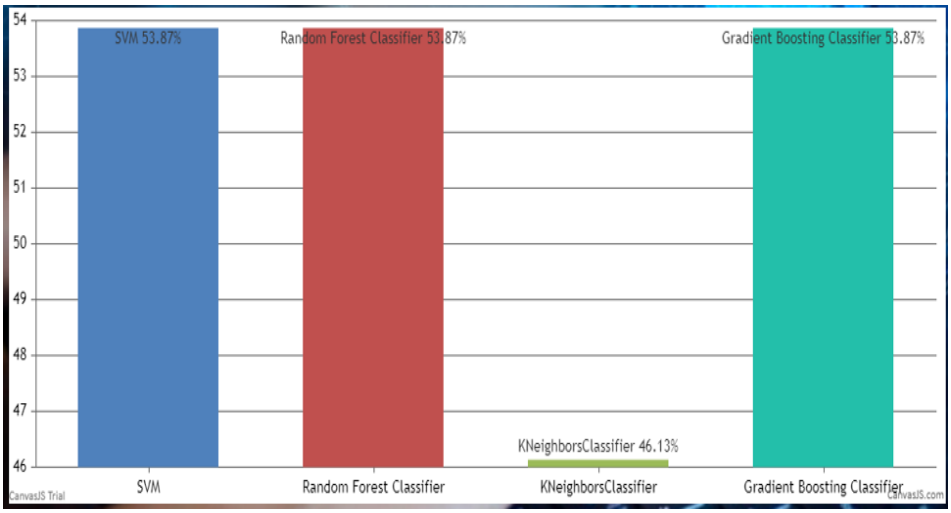

Fig. 10: Bar Chart

C. View Prediction of Cyber Attack Type

Fig 11(a) and fig11(b) tells about the prediction of cyber-attack type.

Datetime	host	RID	proto	spt	dtp	ipaddress	cc	country	locale	latitude	longitude	
03-03-13 22:29	groucho-oregon	840591020	TCP	2712	23	50.26.102.172	US	United States	Texas	35.1613	-101.879	https://malpedia.caad
03-03-13 22:38	groucho-tokyo	621360428	TCP	45855	5900	37.9.53.44	RU	Russia	St.-Petersburg	59.8944	30.2642	NA
03-03-13 22:48	groucho-singapore	1033070424	TCP	6000	135	61.147.103.88	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.npr.org/2 suspected-saudi-arab
03-03-13 22:58	groucho-singapore	1033071474	TCP	6000	135	61.147.107.114	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.cybersco china-apt32-fireeye/
03-03-13 23:08	groucho-singapore	782615554	ICMP	NA	NA	46.165.196.2	DE	Germany	NA	51	9	https://www.cyber.go content/advisories/a compromises-tactics-

View Prediction Of Cyber Attack Type

dtp	ipaddress	cc	country	locale	latitude	longitude	Sources	Prediction
23	50.26.102.172	US	United States	Texas	35.1613	-101.879	https://malpedia.caad.fkie.fraunhofer.de/actor/blacktech	Cyber Attack Found
5900	37.9.53.44	RU	Russia	St.-Petersburg	59.8944	30.2642	NA	No Cyber Attack Found
135	61.147.103.88	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.npr.org/2020/01/24/799358557/behind-the-suspected-saudi-arabian-hacking-of-jeff-bezos-phone	No Cyber Attack Found
135	61.147.107.114	CN	China	Jiangsu Sheng	32.0617	118.7778	https://www.cyberscoop.com/vietnam-coronavirus-china-apt32-fireeye/	No Cyber Attack Found
NA	46.165.196.2	DE	Germany	NA	51	9	https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-	No Cyber Attack Found

Fig 11(a), 11(b): Prediction of Cyber Attack Type

D. View Cyber Attack Type Ratio Results

Below fig12 and 13 shows the cyber-attack results ratio are shown in the form of Pie chat.

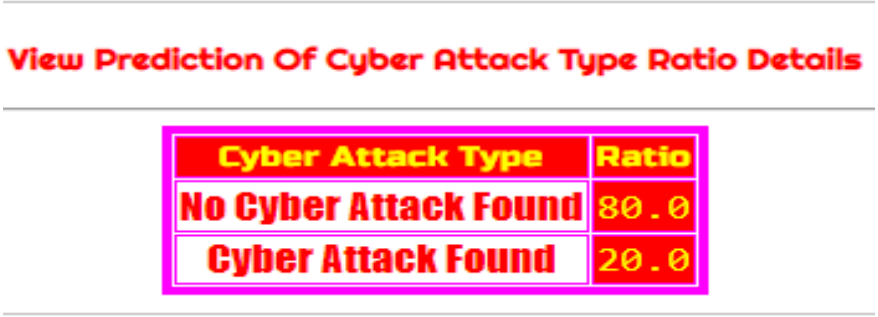

Fig. 12: Cyber Attack Type

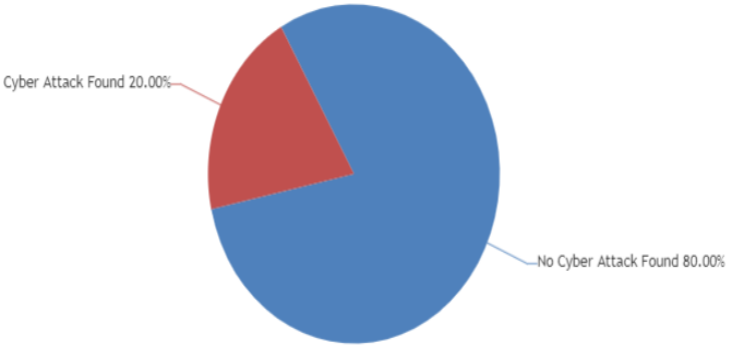

Fig. 13: Pie Chart

E. View All Remote Users

In this page it shows the list of remote users.

Fig 14: Users Table

V. CONCLUSION

In this research, we suggested an active distribution system-specific adaptive hierarchical cyber assault localisation method. The aberrant features are captured using electric waveform data from WMU sensors, which would otherwise go unnoticed. We suggest a modified spectral clustering method to firstly partition the entire large network into more efficient, "coarse" sub-regions. Each sensor's effect score in the potential sub-region can then be calculated and analysed to pinpoint the precise site of the 'fine' cyber-attack. Also, we contrast our approach with alternative approaches at each stage of the localization, sub-graph clustering, and detection of cyber-attacks, respectively. The outcomes from two example distribution grids demonstrate the potential of our strategy.

REFERENCES

[1.] Mehmood, A., Abbas, H., & Khan, S. (2018). A hierarchical intrusion detection system for power distribution networks using decision trees. IEEE Access, 6, 29268-29280. Doi: 10.1109/ACCESS.2018.2846620

[2.] Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, “Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach,” IEEE Journal of Emerging and Selected Topics in Power Electronics, Early Access

[3.] Li, G., Lu, Z., Wu, J., Liu, Y., & He, X. (2019). Anomaly detection in smart grids: A hierarchical approach. IEEE Transactions on Smart Grid, 10(6), 6728-6739. doi: 10.1109/TSG.2018.2847337

[4.] Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639–4657, 2021.

[5.] Raza, S., Hameed, A., Tariq, M., & Ahmed, M. (2019). A hierarchical intrusion detection system for industrial control networks using support vector machines. IEEE Access, 7, 30189-30201. doi: 10.1109/ACCESS.2019.2905985

[6.] B. Wang, H. Wang, L. Zhang, D. Zhu, D. Lin, and S. Wan, "A data driven method to detect and localize the single-phase grounding fault in distribution network based on synchronized phasor measurement," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, p. 195, 2019.

[7.] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505–2516, 2017.

[8.] Džafic, R. A. Jabr, S. Henselmeyer, and T. Đonlagi ´ c, "Fault location ´ in distribution networks through graph marking," IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1345–1353, 2016.

[9.] R. Bhargav, B. R. Bhalja, and C. P. Gupta, "Novel fault detection and localization algorithm for low voltage dc micro grid," IEEE Transactions on Industrial Informatics, 2019.

[10.] Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," IEEE Transactions on Automatic Control, vol. 65, no. 9, pp. 3919–3926, 2020.

[11.] Li, Y. Shi, A. Shinde, J. Ye, and W.-Z. Song, "Enhanced cyber physical security in internet of things through energy auditing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5224–5231, 2019.

[12.] Wilson, D. R. Reising, R. W. Hay, R. C. Johnson, A. A. Karrar, and T. D. Loveless, "Automated identification of electrical disturbance waveforms within an operational smart power grid," IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 4380–4389, 2020.

[13.] P. Dutta, A. Esmaeilian, and M. Kezunovic, "Transmission-line fault analysis using synchronized sampling," IEEE transactions on power delivery, vol. 29, no. 2, pp. 942–950, 2014.

[14.] Sadeghkhani, M. E. H. Golshan, A. Mehrizi-Sani, J. M. Guerrero, and A. Ketabi, "Transient monitoring function–based fault detection for inverter-interfaced micro grids," IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 2097–2107, 2016.

[15.] Bastos, S. Santoso, W. Freitas, and W. Xu, "Synchrowaveform measurement units and applications," in 2019 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2019, pp. 1–5.

[16.] Schweitzer Engineering Laboratories, Pullman, WA, USA, "SEL-T400L Time Domain Line Protection," https://selinc.com/ products/T400L/, Last Access: July 31, 2020.

[17.] Candura instruments, Oakville, ON, Canada. "IPSR intelligent Power System Recorder," https://www.candura.com/ products/ipsr.html, Last Access: July 31, 2020.

[18.] D. Borkowski, A. Wetula, and A. Bien, "Contactless measurement of ´ substation bus bars voltages and waveforms reconstruction using electric field sensors and artificial neural network," IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1560–1569, 2014.

[19.] B. Gao, R. Torquato, W. Xu, and W. Freitas, "Waveform-based method for fast and accurate identification of sub synchronous resonance events," IEEE Transactions on Power Systems, vol. 34, no. 5, pp. 3626–3636, 2019.

[20.] Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Song, "Online distributed iot security monitoring with multidimensional streaming big data," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4387–4394, 2020.

[21.] Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W.-Z. Song, "System statistics learning-based iot security: Feasibility and suitability," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6396–6403, 2019.

[22.] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Man tooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2495–2498, 2021.

[23.] Wang and J. Shi, "Holistic modeling and analysis of multistage manufacturing processes with sparse effective inputs and mixed profile outputs," IISE Transactions, vol. 53, no. 5, pp. 582–596, 2021.

[24.] Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639–4657, 2021.