Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN 1989-9572

DOI:10.47750/jett.2023.14.06.027

A SCALABLE APPROACH TO CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE POWER DISTRIBUTION SYSTEMS

1SHAILAJA.P,2THOTA VINAY KUMAR,3POOJA DONIKELA,4RAJ KUMAR AKKINAPALLI,5AVUNOORI SAI NITHISH,6PUPPALA ROHITH

Journal for Educators, Teachers and Trainers, Vol.14(6)

https://jett.labosfor.com/

Date of Reception: 12 Aug 2023

Date of Revision: 05 Sep 2023

Date of Publication : 16 Oct 2023

1SHAILAJA.P,2THOTA VINAY KUMAR,3POOJA DONIKELA,4RAJ KUMAR AKKINAPALLI, 5AVUNOORI SAI NITHISH,6PUPPALA ROHITH (2023). A SCALABLE APPROACH TO CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE POWER DISTRIBUTION SYSTEMS. *Journal for Educators, Teachers and Trainers*,Vol.14(6).270-282

Journal for Educators, Teachers and Trainers
The LabOSfor electronic, peer-reviewed, open-access Magazine

Journal for Educators, Teachers and Trainers, Vol. 14(6)

ISSN1989 –9572

https://jett.labosfor.com/

A SCALABLE APPROACH TO CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE POWER DISTRIBUTION SYSTEMS

[1]SHAILAJA.P,[2]THOTA VINAY KUMAR,[3]POOJA DONIKELA,[4]RAJ KUMAR AKKINAPALLI,
[5]AVUNOORI SAI NITHISH,[6]PUPPALA ROHITH
[1]Associate Professor,[234] Assistant Professor,[56]Student
Department Of CSE
Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT:-

The increasing reliance on active power distribution systems for efficient and sustainable energy delivery has heightened their vulnerability to cyber attacks. These threats can compromise system integrity, disrupt operations, and lead to significant economic and societal consequences. This paper presents a scalable approach to cyber attack detection and localization tailored for active power distribution systems. The proposed framework integrates advanced machine learning algorithms with state estimation techniques to enable real-time monitoring, anomaly detection, and precise localization of cyber threats.

Key features of the approach include a distributed architecture for data collection and processing, ensuring scalability and resilience in large and complex power networks. A hybrid detection mechanism combines supervised learning for known attack patterns with unsupervised anomaly detection for zero-day threats. Additionally, the localization methodology leverages graph-based models of the power grid to pinpoint compromised nodes and isolate affected subsystems effectively.

Simulation results on realistic power distribution test systems demonstrate the robustness, accuracy, and efficiency of the proposed solution in detecting and localizing various types of cyber attacks, including

false data injection, denial of service, and coordinated attacks. The framework's scalability is validated through performance evaluations across networks of varying sizes and topologies.

This research contributes to the advancement of secure and resilient power distribution systems by providing an adaptable and practical solution to mitigate the risks posed by cyber threats in the evolving energy landscape.

I. INTRODUCTION

The modernization of power distribution systems has led to the integration of advanced communication technologies, distributed energy resources (DERs), and automation frameworks, collectively referred to as active power distribution systems. While these advancements improve efficiency, reliability, and flexibility, they also increase the system's vulnerability to cyber attacks. Cyber threats targeting these systems, such as false data injection (FDI), denial of service (DoS), and malware attacks, can disrupt operations, compromise data integrity, and lead to widespread outages with significant economic and social consequences.

Active power distribution systems are characterized by their decentralized and dynamic nature, incorporating various interconnected nodes, sensors, and control devices. This complexity, coupled with the increasing deployment of Internet of Things (IoT) devices and renewable energy sources, expands the attack surface for adversaries. Detecting and localizing cyber attacks in such systems is a challenging task due to their scale, heterogeneity, and the rapid evolution of cyber threats. Traditional detection methods, which often rely on static rules or centralized processing, struggle to meet the demands of modern power grids in terms of scalability, responsiveness, and adaptability.

This paper addresses these challenges by presenting a scalable approach to cyber attack detection and localization tailored for active power distribution systems. The proposed framework combines advanced machine learning techniques with graph-based modeling of the grid to provide real-time monitoring, robust anomaly detection, and accurate localization of cyber threats. The key contributions of this work include:

Scalable Design: A distributed architecture that ensures efficient processing and communication across large-scale power distribution networks.

Hybrid Detection Mechanism: A combination of supervised learning for recognizing known attack patterns and unsupervised anomaly detection to identify zero-day threats.

Precise Localization: A graph-based analytical model to trace the source of anomalies and isolate affected subsystems, minimizing system disruption.

The methodology is validated through simulations on realistic test systems, demonstrating its effectiveness in detecting and localizing diverse types of cyber attacks while maintaining scalability and computational efficiency. The results highlight the framework's potential to enhance the security and resilience of active power distribution systems in an

increasingly digital and interconnected energy landscape.

This research aims to bridge the gap between traditional cyber attack mitigation strategies and the needs of modern, dynamic power distribution systems, offering a practical and robust solution to the growing cybersecurity challenges in the energy sector.

II. RELATED WORK

An inventive intrusion detection system (IDS) built on the ideas of the Forest PA classifier, the JRip algorithm, and the decision tree and rules-based REP Tree. The third classifier uses the first and second classifiers' outputs as inputs, together with the original data set's attributes. Mehmood et al.'s experimental results on the CICIDS2017 dataset [1] show that the suggested IDS performs better than state-of-the-art techniques in terms of accuracy, speed, false positives, and overhead.The distribution power infrastructure's dependability is at risk from both digital and physical threats. Photovoltaics (PVs), one of the quickly growing renewable energy sources, has a unique set of security issues. In this study, we propose an existing system that creates a novel high-dimensional data-driven cyber physical attack detection and identification (HCADI) technique employing electric waveform data collected by waveform sensors in the distribution power networks.

Power providers cannot increase reliability and efficiency until smart grids (SGs) are monitored and managed in real time. We create a system that detects irregularities in real time using data from smart meters (SM) in customers' homes. The method's objective is to identify unusual occurrences at the consumer and lateral levels. In addition to data gathered from SMs, Li, G., Lu, Z., et al. [3] proposed a generative model for anomaly detection that considers the hierarchical structure of the network.

Power electronics systems have become more susceptible to cyber-physical threats due to their extensive use in Internet of Things-enabled applications, such as connected electric vehicles (EVs). In response to this increasing demand, the IEEE Power Electronics Society recently launched a cyber-physical security project (PELS). According to a theory by J. Ye, L. Guo, and others [4], the cyber-physical security risk posed by connected electric automobiles will rise in tandem with the proliferation of Vehicle-to-everything (V2X) and electronic control units.

As information technology advances, standard Ethernet is being used more and more in industrial control systems. Although it removes the ICS's built-in isolation, it offers no extra security. An intrusion detection system (IDS) customised for a particular industrial setting is required by today's ICS. This study describes a number of attack methods, such as our special penetration and forging attacks. Nevertheless, we offer a hierarchical intrusion detection system that consists of a traffic prediction model in addition to an anomaly detection model. The autoregressive integrated moving average (ARIMA)-based traffic prediction model can be used to forecast the short-term traffic of the ICS network. In response to abnormal changes in traffic patterns, this model can detect infiltration attacks with high

accuracy. Raza [5] suggested using an anomaly detection model.There are more variables that can cause single-phase grounding issues in larger and more complex power systems.

We suggest a modified approach based on synchronised phasor monitoring to maximise the uses of huge data in power systems. Single-phase grounding faults are found and identified using the data-driven technique, which validates the connection between eigenvalues and power system state provided by B. Wang et al. [6]. Computational and communications intelligence significantly enhances smart grid monitoring and control. Because of our reliance on information technology, we are far more susceptible to destructive attacks. The data integrity attack known as fake data injection (FDI) is currently posing a serious threat to the supervisory control and data acquisition system. As suggested by Y. He et al., we employ deep learning techniques in this study to identify the traits of FDI attacks from historical measurements. [7]. We next use the learned characteristics to the detection of ongoing FDI assaults.

A. Suggested Plan

The approach suggests an electrical waveform-based adaptive hierarchical structure for active distribution systems with DERs to detect and pinpoint cyberattacks. To assess the effects of cyberattacks on distribution networks, high-quality models of DER and cyberattacks are built. Quantitative analytics and numerous experiments are used to assess the efficacy of the suggested method. According to our research, if the monitoring measurements diverge from the steady state—a problem for anomaly detection—the cyberattack could be identified in the suggested system.According to the concept, the operational distribution networks should be divided into smaller areas where cyberattacks are more likely to happen.

The provider of services

The Service Provider must provide their username and password in order to access this section. Figure 1 depicts the process of the service provider, who can access training and testing cyber data sets among other things after logging in. View the Cyberattack Prediction, View the Cyberattack Type Ratio Forecast, View a Bar Graph of Cyber Dataset Accuracy Following Training Examine Cyber Datasets' Accuracy Following training, Prepared-to-Use Datasets: Examine the breakdown of all remote users by type of attack.

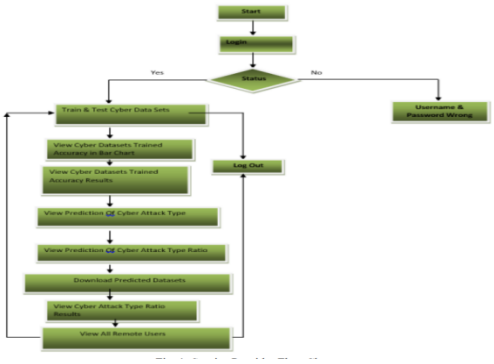


Fig. 1: Diagram of Flow for Service Providers

Examine the authorised user.

The administrator can view a list of users who have signed up for the service within this module. In addition to having the power to approve users, the administrator can view user data, including name, email address, and address.

Remote User

There are currently n users logged into this module. Figure 2 displays the Remote User flow chart. Before participating in any activities, users must first register. Following registration, the user's information will be stored in the database. He must enter a working user name and password after successfully enrolling in order to access the system. Users can perform a number of tasks after successfully logging in, such as SEE YOUR PROFILE, PREDICT CYBER ATTACK TYPE, and REGISTER AND LOGIN.

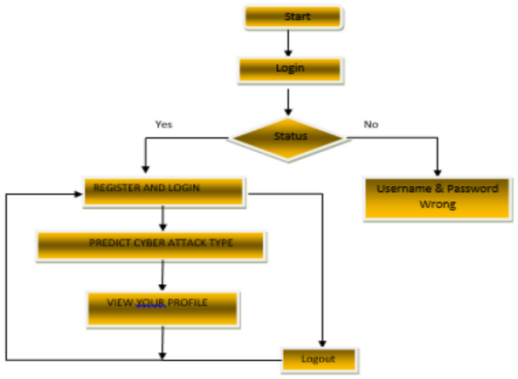


Fig. 2: Distribution Map of Distant Users

B. ARCHITECTURE

The Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution System architecture was designed to learn from new data and adjust to the dynamic nature of the active distribution system. The active distribution system is continually changing, but the suggested design in Figure 3 can adapt to these changes. The service provider, the view, and the authorised user and the remote user are the three components that make up this architecture. Login, train and test cyber data sets, view trained accuracy in bar chart, view 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, view remote users; these are all part of the service provider. The web server is linked to a web database for data retrieval, and it is also linked to a service provider for data collection and storage.Data from several service providers is stored in a web-based database and retrieved as needed. Users from afar need to sign up, log in, and make cyberattack predictions before they can access your profile.

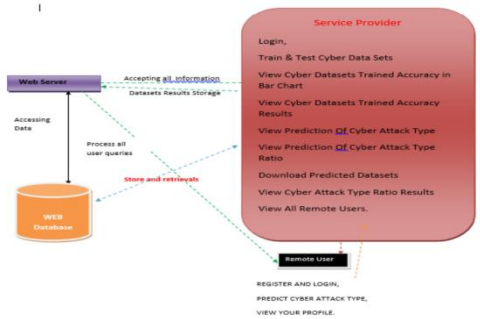


Fig. 3: Conceptual Design

I. III. METHODOLOGIES

A. GRADIENT BOOSTING

Gradient boosting machine learning methods are utilised for regression and classification analyses. It works by building a series of weak decision trees that have been trained on different subsets of the data. The final result is obtained by adding the predictions from all the decision trees. Multiple layers of hierarchically organised detection techniques are used in the adaptive hierarchical approach with gradient boosting. Gradient boosting classifiers are employed at each layer to categorise system data and spot possible cyber-attacks. The broad-based detection technique at the top tier of the hierarchy utilises a gradient boosting classifier to recognise well-known assault patterns and deviations from typical system activity. The classifier can recognise

typical attack characteristics and abnormalities since it has been trained on past data. Gradient boosting classifiers are used in the intermediate tier of the hierarchy's detection techniques to find assaults that have gotten past the top-level ones. These classifiers may identify assaults that are exclusive to certain system components or activities since they were trained on more specialised data. After an assault has been discovered, reaction mechanisms are initiated in the hierarchy's bottom layer. Automated reactions including traffic snarling, quarantining infected systems, and warning security personnel are examples of these techniques.Flowchart for the gradient boosting machine learning technique (Fig. 4). The ensemble classifiers are made up of a number of weak classifiers. The weights of the incorrectly predicted points are raised in the next classifier. The ultimate determination is made using the weighted average of each forecast. Adaptive hierarchical cyber-attack detection and localization in active distribution systems employing gradient boosting contains localization techniques that may identify the attack's location in addition to detection and response methods. These mechanisms use methods like network topology analysis and geo-location to pinpoint the attack's origin and the system components that were harmed.

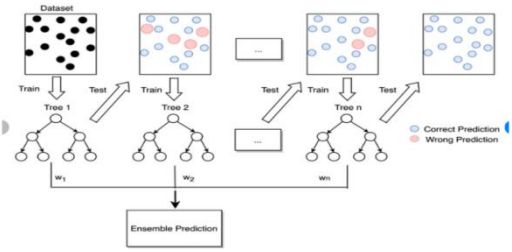


Fig. 4: Boosting Gradients

B. K-NEAREST NEIGHBORS (KNN)

This straightforward yet incredibly effective classification algorithm groups items according to a similarity metric. Lazy learning that is non-parametric and delays "learning" until the test example is shown. Every time we have new data to classify, we use the training data to determine the new data's K-nearest neighbours. The data points before and after utilising K-Nearest Neighbours (KNN) are shown in Figure 5. For instance:

Instance-based learning also operates in a sluggish fashion. This is because it could take some time for samples in the training dataset that are geographically close to the input vector for the test or prediction to appear.

.

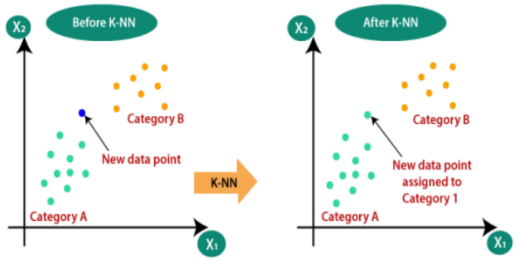


Fig. 5: K-Nearest Neighbors (KNN)

C. LOGISTIC REGRESSION CLASSIFIERS

Logistic regression technique probes the association between a set of independent values to help choose the best cut-off point for a categorical dependent variable (outcome) and (explanatory) variables. The phrase "logistic regression" is used when the dependent variable can only have the values 0 and 1, such as "Yes" and "No." When the dependent variable has three or more distinct values, such as married, single, divorced, or widowed, multinomial logistic regression is frequently employed.The method works similarly to multiple regression, however different data are used for the

dependent variable. This program can compute binary logistic regression and multinomial logistic regression for both categorical and numeric independent variables. Included are the regression equation, odds ratios, standard deviations, probabilities, and confidence intervals. Diagnostic residual charts and reports are produced after a comprehensive residual investigation. By doing an independent variable subset selection, it looks for the best regression model with the fewest number of independent variables. It offers confidence intervals and ROC curves for expected classification. The automated identification of rows that were skipped over throughout the analysis makes it easier to validate your results.
Figure 6 displays the regression classifiers.The fundamental premise of the supervised learning technique known as the "naïve bays approach" is that a feature's presence or absence in a class has no effect on any other feature. Nevertheless, it appears effective and powerful. Effectiveness-wise, comparable to other supervised learning techniques. There are numerous theories for this in the literature. We concentrate on a representation bias-based explanation in this lesson. The naive Bayes classifier, logistic regression, linear discriminant analysis, and linear support vector machines are examples of linear classifiers (also known as support vector machines).
The technique used to estimate the classifier's parameters takes this mismatch (the learning bias) into account..

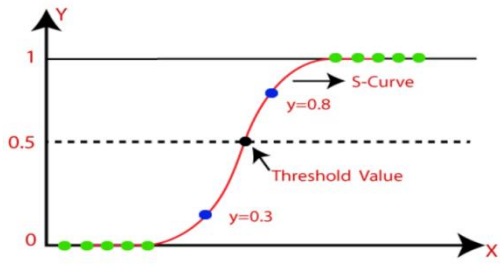


Fig. 6: Classes Determined Using Logistic Regression

D. RANDOM FOREST

One technique designed to accomplish this is titled "Adaptive Hierarchical Cyber Attack Detection and Localisation in Active Distribution System using Random Forest."To categorise and pinpoint the type of cyberattack that has taken place in the system, the technique uses machine learning techniques, most notably the Random Forest algorithm.
To increase the accuracy of the detection and localisation process, hierarchical structuring is employed. The ruleset that the hierarchy is based on is used to classify the type of cyberattack that has occurred. The rules are organised in a hierarchical manner, classifying the most severe cyberattacks first.
The program is trained using Random Forest on a dataset of cyberattack examples. To identify the type of assault, the program creates a decision tree based on attack characteristics. These criteria could include the assault's origin, time, and nature, as well as any other relevant information.
The trained model can be used to classify and localise cyberattacks on the active distribution system. The hierarchical structure aids in improving the accuracy of the detection and localisation process by placing greater emphasis on the classification of severe assaults. Figure 7 below displays the training and test sets that will be utilised to guide the random forest's prediction.

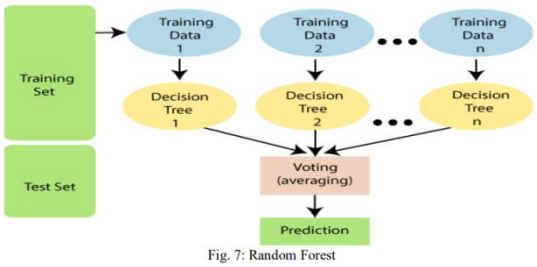


Fig. 7: Random Forest

E. SVM

Using a iid training dataset, a discriminant machine learning method for classification issues finds a discriminant function that correctly predicts labels for recently acquired cases. Unlike generative machine learning methods that generate conditional probability distributions, a discriminant classification function takes a data point x and assigns it to one of the multiple classes that comprise the classification task. Generative approaches are frequently employed because discriminant algorithms become less dependable when outlier identification is incorporated into the prediction process. This is especially true for multi-dimensional feature spaces, when only posterior probabilities are needed. The geometrical equivalent of learning a classifier is to find the equation for a multidimensional surface that optimally divides the various classes in the feature space.

Figure 8 illustrates SVM, a discriminant method that, by solving the convex optimisation problem analytically, always yields the same optimal hyperplane value, unlike GAs and perceptrons, which are also frequently used for classification in machine learning. The necessary start and stop periods have a significant impact on perceptron solutions. In contrast to the models of a perceptron and a generalised additive classifier (GA), the parameters of a support vector machine (SVM) model for a certain training set and a specific kernel that converts the data from the input space to the feature space vary each time training begins.Numerous hyperplanes will satisfy this requirement because Perceptrons and gas are simply concerned with reducing training errors.

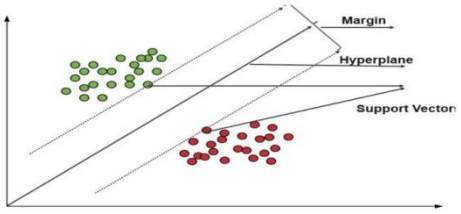


FIG 8: SVM

IV. RESULT ANALYSIS

- • The suggested method works as explained below. Accessing Cyber Data Sets for Training and Testing;
- Downloading Predicted Datasets; Viewing Cyber Attack Type Prediction Results;
- View findings for the cyber attack type ratio and bar charts showing trained accuracy on cyber datasets. See every remote user.

A. Login Page

Below Fig. 9 are the User Registration and User Login sections. Users may sign up for an account and enter their credentials here.


Fig. 9: Sign In Screen

B. View Cyber Datasets Trained Accuracy Results

Figure 10 displays a bar chart that illustrates the precision of multiple datasets.This bar chart displays the accuracy of SVM, random

forest, KNN-neighbors classifiers, and gradient boosting algorithms as bars. The reliability results are shown in a variety of charts (bar, line, and pie).

- **View Cyber Datasets Trained Accuracy in Bar Chart**

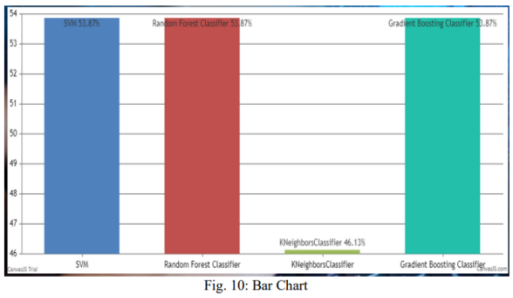
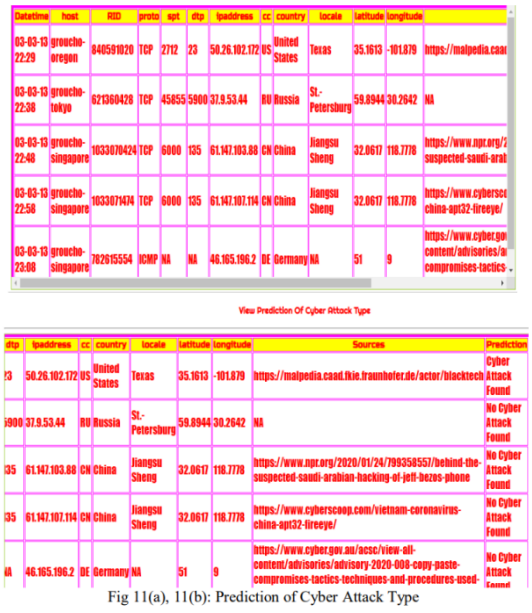


Fig. 10: Bar Chart

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	782915554	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

The percentages of successful cyberattacks are shown in a pie chart format in figures 12 and 13 below.

View Prediction Of Cyber Attack Type Ratio Details

Cyber Attack Type	Ratio
No Cyber Attack Found	80.0
Cyber Attack Found	20.0

Fig. 12: Forms of Cyber-Attacks

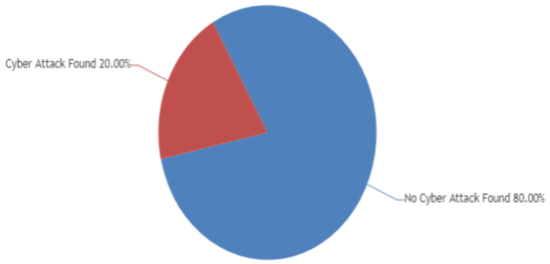


Fig. 13: Venn Diagram

E. View All Remote Users

The Remote Users List is shown on this page.

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Rajesh	Rajesh123@gmail.com	Male	#8928,4th Cross,Vijayanagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju13@gmail.com	Male	#892,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore

Fig 14: Table of Users

II. V. CONCLUSION

Active power distribution systems, as critical components of modern energy infrastructure, face an escalating threat from sophisticated cyber attacks. These threats have the potential to disrupt operations, compromise data integrity, and cause significant societal and economic impacts. This paper proposed a scalable and efficient framework for cyber attack detection and localization in active power distribution systems, addressing the unique challenges posed by their distributed and dynamic nature.

The framework combines advanced machine learning techniques with graph-based modeling to achieve robust anomaly detection and precise localization of cyber threats. A hybrid detection mechanism allows the system to identify both known and unknown attack patterns, while a distributed architecture ensures scalability

across large and complex networks. The ability to accurately localize attacks within the power grid minimizes the impact of cyber threats and facilitates timely mitigation measures.

Simulation results validate the effectiveness of the proposed approach, demonstrating high detection accuracy, computational efficiency, and adaptability to various attack scenarios. These findings highlight the framework's potential to enhance the resilience and security of power distribution systems in an increasingly digital and interconnected energy landscape.

This research represents a significant step toward strengthening cybersecurity in power systems, ensuring their reliability and robustness in the face of evolving threats. Future work will focus on integrating real-time adaptive learning capabilities and exploring the application of the framework in more diverse and heterogeneous grid environments.

By addressing the critical need for scalable, accurate, and efficient cyber attack detection and localization, this work contributes to the broader effort to secure the energy infrastructure of the future. Future research will focus on extending the framework to incorporate adaptive learning for real-time evolution with emerging threats and integrating with broader grid management systems to enhance overall grid resilience

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.