e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

☎ 6381 907 438 ☎ 6381 907 438 ✉ ijmrset@gmail.com @ www.ijmrset.com

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707232 |

Adaptive Hierarchical Cyber Attack Detection

Gautami Totad[1], Praveen K S[2]

Student, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: Due to the enclosure of distributed renewable energy generation, it is challenging to develop a cyber security strategy for active distribution systems. By analyzing electrical waveforms, this paper proposes an adaptive hierarchical cyber attack detection and localization framework for distributed active distribution systems. A sequential deep learning model that can identify even minor cyberattacks serves as the foundation of cyber attack detection. Prior to finding the particular digital assault inside the assessed sub-district, the two-step digital assault confinement calculation first gauges the sub-area of the assault. For the different evened out computerized attack 'coarse' restriction, we propose a new spooky gathering-based network distribution. From that point forward, a standardized effect score in view of waveform measurable measurements is proposed to deliver a "fine" digital assault area by additional characterizing different waveform properties. In a comprehensive quantitative assessment with two contextual investigations, the evaluation results of the proposed system finally look promising when compared to conventional and cutting-edge methods.

I. INTRODUCTION

CYBER attack localization is important to protect smart distribution grids, but also a challenging task because of the inherent distributed energy resources (DER) and topology complexities. Raw electrical waveforms, signals of electrical networks, together with those in cyber networks provide great potentials in cyber attack detection. For example, devices in power networks must leave clues of their operational status and health (including faults or attacks) information in the raw electrical waveform signals: a cyber-device in fault or under attack will cause unusual energy consumption pattern in power networks; a power electronics or electric machine in fault or under attack may cause unusual harmonics or energy profile in electrical networks.

By analyzing the electrical waveform signals and their root cause, waveform analytics can present utilities with a complete picture of the health and status of their system, both during outages and normal operating conditions. It could also provide a variety of operational benefits to system operators, asset management personnel, and repair crew. Electronic sensors placed on power grids and distribution systems can either measure the electricity properties, such as pharos measurement unit (PMU) sensors or directly record the raw electrical waveform using waveform measurement unit (WMU), depending on the needed fidelity of monitoring applications. Thanks to developed network connectivity, the streaming monitoring data flow can be obtained and analyzed online and in real-time.

The network of the waveform sensors form an Internet of Things (IoT) system, where the waveform sensors are viewed as networked IoT sensing devices. Therefore, we can potentially use the information embedded in electrical signals to enable security monitoring, diagnosis, and prognosis in the power networks. The possibility may be well beyond what we can imagine now. It broadly applies to many cyber-physical systems (CPS) and applications, such as power distribution networks, multi-stage manufacturing systems, electric vehicles,
and so on. Cyber attacks towards connected IOT devices trigger anomalies in system statistics, energy consumption, as well as electrical waveforms. Thus, recorded waveform which carries high fidelity current and voltage information should be adequate for cyber attack characterization. Furthermore, the transmission of the high-frequency waveform data is feasible in practice.

Data-driven methods have been widely adopted for event localization in power electronics networks and active distribution systems. Rule-based data-driven analytics, signal property-based approach, and neural networks (NN) based algorithms, such as auto encoders, convolution neural network (CNN), have been developed. However, N based algorithms typically require a large amount of training data to capture the sophisticated features, which cannot be fully simulated or acquired from real applications. Thus, combining the rule-based signal processing methods and machine learning methods could lead to a solution tackling the challenging problem using an affordable data size.

There have been numerous works targeting the event and cyber attack localization problem. Dynamic data analytics based localization is always a major branch for the distribution networks, DC micro grid, and islanded micro grid. This paper proposes a new adaptive hierarchical framework for efficient and accurate cyber attack detection and localization by taking advantage of the electrical waveforms. The proposed approach has a hierarchical architecture that divides the whole network into sub-groups and then locates the cyber attack within one local cluster. Based on a modified unsupervised clustering and a deep learning based anomaly detection method, cyber attacks in the active distribution systems can be adaptively detected and located. The performance of the proposed approach has been tested by multiple cyber attack scenarios in two representative case studies.

II. LITERATURE SURVEY

The CPS has three layers: the perceptual layer, the data transmission layer, and the application layer. The first layer, or perception layer, contains the recognition and sensor, as well as the global positioning system (GPS), RFID, sensor, actuator, camera, and IoT. Sound, light, mechanical, chemical, thermal, electrical, biological, and location data may be captured, and the sensor can create real-time data through node collaboration in wide-area and local network domain. As a result, the perception layer recognizes and gathers data, delivers it to the communication layer, and works with the network's IoT nodes.

The layer that handles communication is in charge of transferring and processing data between the sensor and the application. This layer interacts utilizing a variety of technologies, including cable (e.g., LAN, WAN), network devices (e.g., Switch, Router), and wireless (e.g., Bluetooth, ZigBee, WiFi, 4G, and 5G). This is one of the most important aspects of the CPS, which normally ranges from local to global. Because they can initially analyse and manage massive volumes of data across the Internet, most communications are extremely accessible and cost-effective. The communication layer is also in charge of dependability and allows for real-time transmission.

III. SYSTEM DESIGN

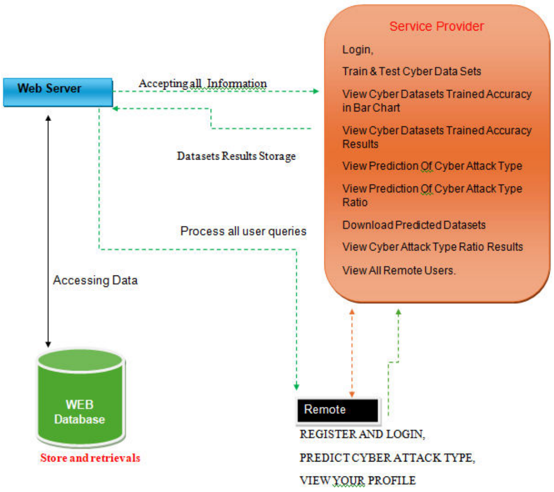

Service Provider
Login,
Train & Test Cyber Data Sets
View Cyber Datasets Trained Accuracy in Bar Chart
View Cyber Datasets Trained Accuracy Results
View Prediction Of Cyber Attack Type
View Prediction Of Cyber Attack Type Ratio
Download Predicted Datasets
View Cyber Attack Type Ratio Results
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Process all user queries
Accessing Data
WEB Database
Store and retrievals
Remote
REGISTER AND LOGIN,
PREDICT CYBER ATTACK TYPE,
VIEW YOUR PROFILE

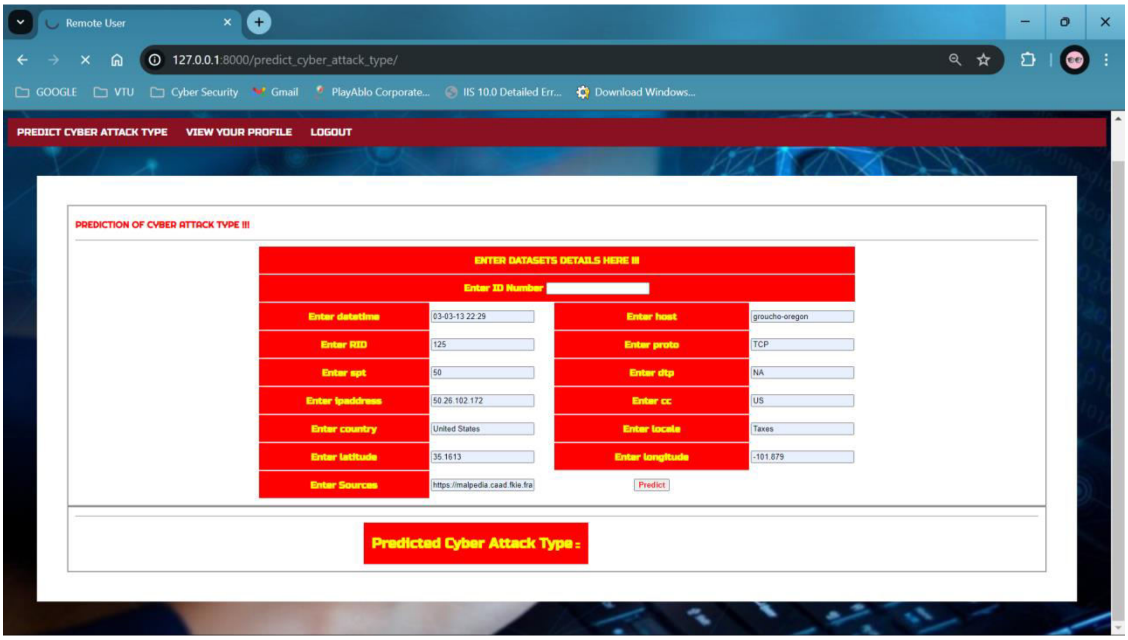
Figure 1: System Architecture

IV. RESULTS AND OUTCOMES

The "Adaptive Hierarchical Cyber Attack Detection" project is all about making our computer systems better at catching cyber attacks quickly and accurately. Here’s what this project aims to achieve:

1. **Better Detection:**
This system is smarter at finding cyber threats compared to older methods. It can adjust itself and look at different layers of data to catch attacks more accurately.
2. **Fast Responses:**
It can spot threats in real-time, which means it can react almost immediately, helping to stop attacks before they do too much damage.
3. **Handles Big Data:**
The system is built to handle large amounts of data, so it works well for both small and large networks, and can deal with a lot of activity without getting bogged down.
4. **Fewer False Alarms:**
By being adaptive, it reduces false alarms. This means cybersecurity teams won't waste time chasing down threats that aren't real.
5. **Learns Over Time:**
It uses machine learning, which means it gets better at detecting new types of attacks as it encounters them
6. **Layered Protection:**
The system looks at different parts of the network (like traffic, user behavior, and system logs) in layers, providing a stronger defense.
7. **Proven Performance:**
Tests show that this new system is better in terms of how quickly and accurately it detects attacks, and it uses resources efficiently.
8. **Real-world Use:**
The system has been tested in real-world situations and has proven effective at catching real cyber threats.
9. **Continuous Improvement:**
It keeps getting better by learning from each detection, making adjustments to improve future performance.
10. **Team Effort:**
The system can work together with other cybersecurity tools and share information, making the overall defense stronger.

Snapshots:



PREDICTION OF CYBER ATTACK TYPE !!!

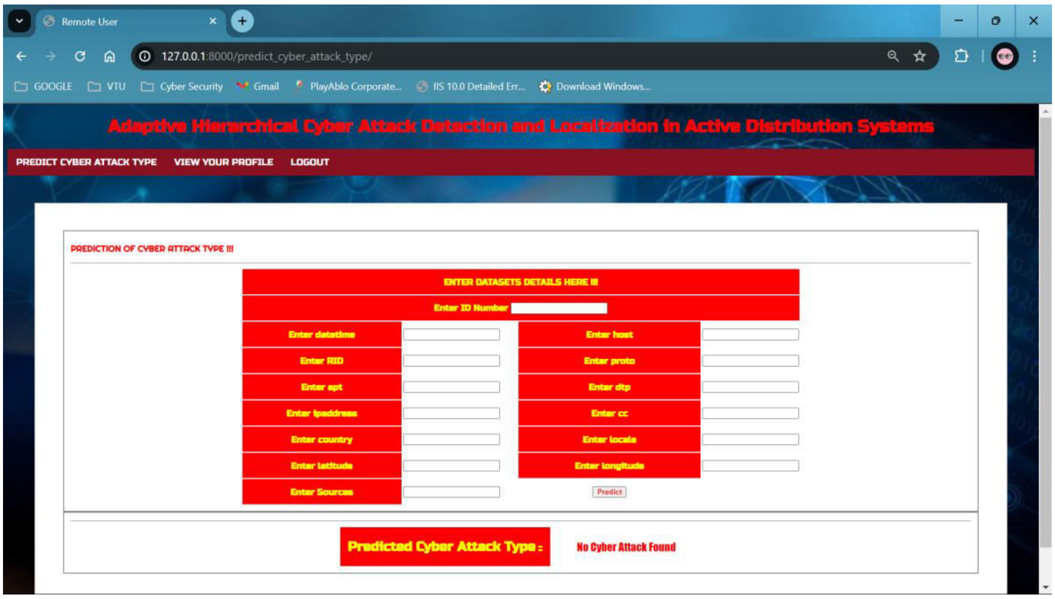
ENTER DATASETS DETAILS HERE !!!

Enter ID Number

Enter datetime	03-03-13 22:29	Enter host	groucho-oregon
Enter RID	125	Enter proto	TCP
Enter spt	50	Enter dtp	NA
Enter ipaddress	50.26.102.172	Enter cc	US
Enter country	United States	Enter locale	Taxes
Enter latitude	35.1613	Enter longitude	-101.879
Enter Sources	https://malpedia.caad.fkie.fra	Predict	

Predicted Cyber Attack Type :

Figure 1: DATA Prediction



Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

PREDICTION OF CYBER ATTACK TYPE !!!

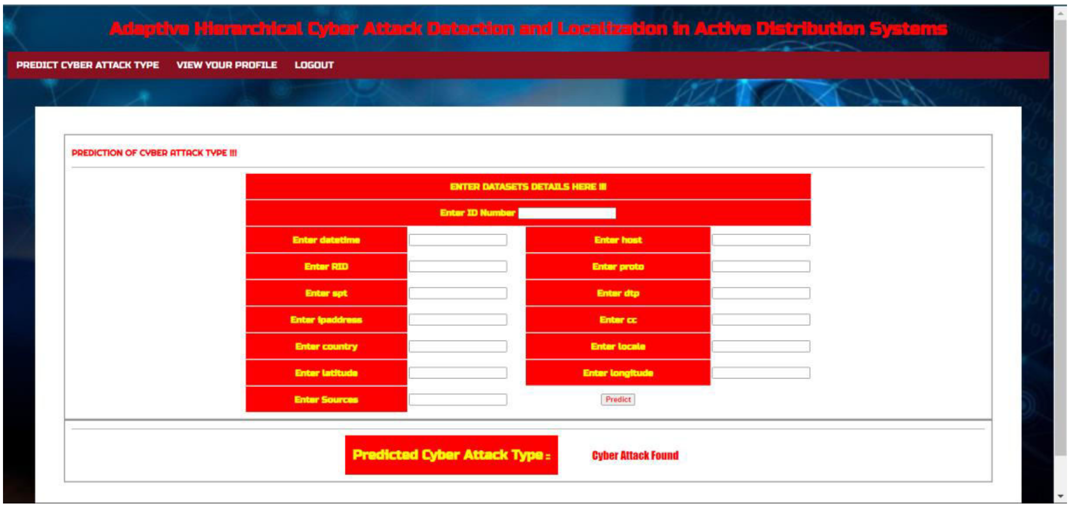
ENTER DATASETS DETAILS HERE !!!

Enter ID Number

Enter datetime		Enter host	
Enter RID		Enter proto	
Enter spt		Enter dtp	
Enter ipaddress		Enter cc	
Enter country		Enter locale	
Enter latitude		Enter longitude	
Enter Sources			

Predicted Cyber Attack Type : No Cyber Attack Found

Figure 2: Result is cyber attack not found



Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

PREDICTION OF CYBER ATTACK TYPE !!!

ENTER DATASETS DETAILS HERE !!!

Enter ID Number

Enter datetime		Enter host	
Enter RID		Enter proto	
Enter spt		Enter dtp	
Enter ipaddress		Enter cc	
Enter country		Enter locale	
Enter latitude		Enter longitude	
Enter Sources			

Predicted Cyber Attack Type : Cyber Attack Found

Figure 3: Result is cyber attack found

V. CONCLUSION

In conclusion Cyber attack detection represents a pivotal strategy in safeguarding organizations against increasingly sophisticated cyber threats. By implementing a layered approach that integrates advance technologies, proactive methodologies, and strategic enhancements, organizations can achieve robust defenses that adapt dynamically to evolving landscapes.

In this project, we proposed an adaptive hierarchical cyber attack localization approach for active distribution systems. Electric waveform signals obtained by WMU sensors are used to capture the abnormal features, which would be otherwise ignored. To improve the efficiency, we propose a modified spectral clustering method to first partition the whole large network into smaller 'coarse' sub-regions. Next, the accurate 'fine' cyber attack location can be determined by calculating and analyzing Impact Score of each sensor in the potential sub-region.

REFERENCES

[1] I. Džafi´c, 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.

[2] R. Bhargav, B. R. Bhalja, and C. P. Gupta, “Novel fault detection and localization algorithm for low voltage dc microgrid,” IEEE Transactions on Industrial Informatics, 2019.

[3] G. 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.

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

[5] A. J. 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.

[6] 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.

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

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com