International Journal of Basic and Applied Sciences, 14 (2) (2025) 49-57

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/0cz1w646
Research paper

An Analysis of cyber threats in distributed energy power networks

Vijaykumar Kamble [1]*, Vandana Navale [2], Varsha Dange [3], Archana Chaudhari [4]

[1] Department of Electrical Engineering, AISSMS Institute of Information Technology, Pune, Maharashtra, India
[2] Department of Artificial Intelligence and Data Science, Ajeenkya D. Y. Patil School of Engineering, Pune, Maharashtra, India
[3] Department of Information Technology, Vishwakarma Institute of Technology, Pune, Maharashtra, India
[4] Department of Instrumentation Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, India
**Corresponding author E-mail: vijaykumar.kamble@aissmsioit.org*

Received: May 11, 2025, Accepted: June 3, 2025, Published: June 9, 2025

Abstract

The power demand has increased dramatically in recent years. Conventional power generation provides about 80% of the world's energy. Distribution networks are essential to the electrical grid system because they link consumers to the transmission system. Distribution networks require careful planning since they are vast and complex. Congestion in the distribution network quickly affects the network's voltage profile as power demand increases, leading to power outages and delayed power delivery. Since Active Distribution Networks (ADNs) are more vulnerable to cyberattacks due to their integration with cutting-edge communication and control technologies, detecting these attacks is a critical problem in modern power systems. The possible cyberattacks on power systems are covered in this paper. To identify the possible, cyberattack, an IEEE-15 bus system with Cyber-Physical Layering (CPL) is suggested. Cyberattack detection systems defend ADNs against assaults including data alteration, illegal access, and service denial by utilizing machine learning, anomaly detection, and real-time monitoring. Using machine learning techniques, such as DT, NNN, and SVM, cyberattack detection is also carried out on modified IEEE-15 bus systems and CPL-based IEEE-15 buses. Additionally, a comparative analysis of the methods for cyberattack detection is conducted.
The paper discusses how advanced communication and control systems in active distribution networks (ADNs) face heightened cyber risks from both traditional threats like DoS and FDI attacks and emerging quantum computing-based attacks. It highlights vulnerabilities across CPL layers and recommends AI/ML anomaly detection, quantum-safe cryptography, and robust network designs for future resilience.

Keywords: *Cyberattacks, Vulnerabilities, Microgrid, Distributed System, Denial-of-Service, Communication, Algorithm.*

1. Introduction

21st century electric power structures have seen dramatic change because of progresses in digital technology, automation, and connectivity. Modern cyber power systems usher in a new era of extraordinary efficiency, reliability, and durability by fusing traditional energy infrastructure with cutting-edge communication and information technology. From production and transmission to distribution and consumption, every phase of the energy system makes use of ICT-enabled machinery, sensors, and software platforms. Their goals are to enhance grid resilience, facilitate better operations, and enable more informed decision-making. Furthermore, modern cyber power systems employ cutting-edge automation and control technologies to improve energy distribution efficiency and preserve a real-time supply-demand balance. Demand-side management programs, intelligent control algorithms, and distributed electrical resources enable real-time adjustments to grid properties, including voltage levels and electricity flow, to preserve stability and dependability in a variety of operating scenarios. An essential part of today's intelligent power system is a cyber-physical microgrid. Its goal is to provide safe and efficient electricity distribution while upholding a high standard of environmental responsibility worldwide. The CPL microgrid achieves optimal operation by implementing distributed control of electrical elements using modern processing and communication technologies. The microgrid's control unit manages regulated loads and a variety of Distributed Energy Resources (DERs) to deliver reliable, reasonably priced power with minimal environmental impact. A typical structured control system with three levels that operate on various time scales to achieve control objectives is shown in Figure 1.
All the micro-generating modules of a CPL Microgrid provide DC power. To provide AC power to the loads, inverter circuits are necessary. Communication agents with routers, links, local controllers, and advanced algorithms make up the cyber layer. Its goal is to address the various problems that microgrid operators and consumers face. The CPM may operate in single mode due to planned scheduling or an unforeseen attack.

Because of the low fault current in inverter-based CPM, it is discovered that traditional protective relays need to be enhanced to better protect the system. Faults that are closely associated with the line and ground are the most observed. For a fault mitigation model to work well, it needs an efficient fault detection technique that incorporates algorithms for accurately categorizing and recognizing defects. This method, which entails classifying the flaws and putting in place an appropriate mitigation strategy to decrease the time and cost needed for restoration, increases the credibility of the overall protection process.

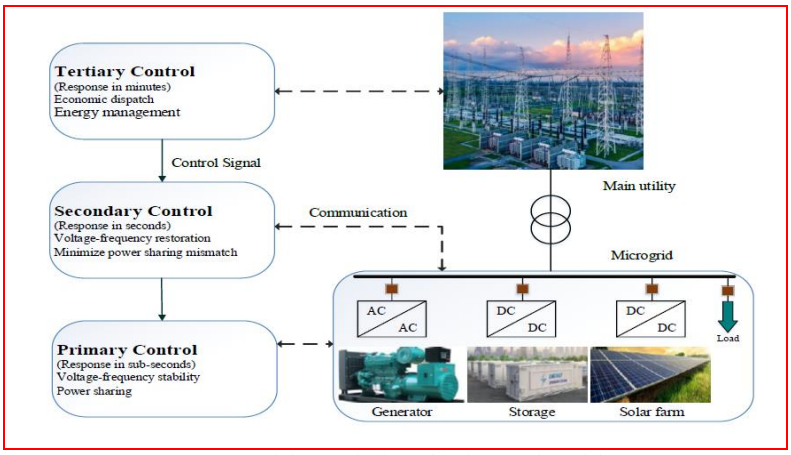

Fig. 1: Triple-Level Hierarchical Control Model

1.1 Cyber Threats in Distribution Systems

The distribution system is more vulnerable because of serious cybersecurity threats. Threats to exploit these vulnerabilities for assaults and disrupt the distribution system's functionality are growing significantly. The distribution system's automation and communication technologies have advanced, giving attackers the potential to alter or interfere with the ICS and cause disruptions. Additionally, more DERs are being integrated, which means that the grid is receiving more power than it needs. Because these DERs are configured to monitor and regulate the system, they increase the grid's susceptibility to cyberattacks and possible outages. To disrupt the system or induce a blackout, attackers employ a variety of attack techniques to compromise the distribution network.

The integrated nature of microgrids and the internet connections they are connected to make them extremely susceptible to cyberattacks. Information-sharing devices and intelligent gadgets may be vulnerable to malicious assaults that take advantage of system flaws due to their integration and the lack of thorough security standards. The volume of data flow is directly impacted by the scalability of smart grid technology since it raises the demands on computation and transmission. Figure 2 illustrates the various forms of cyberattacks on power systems.

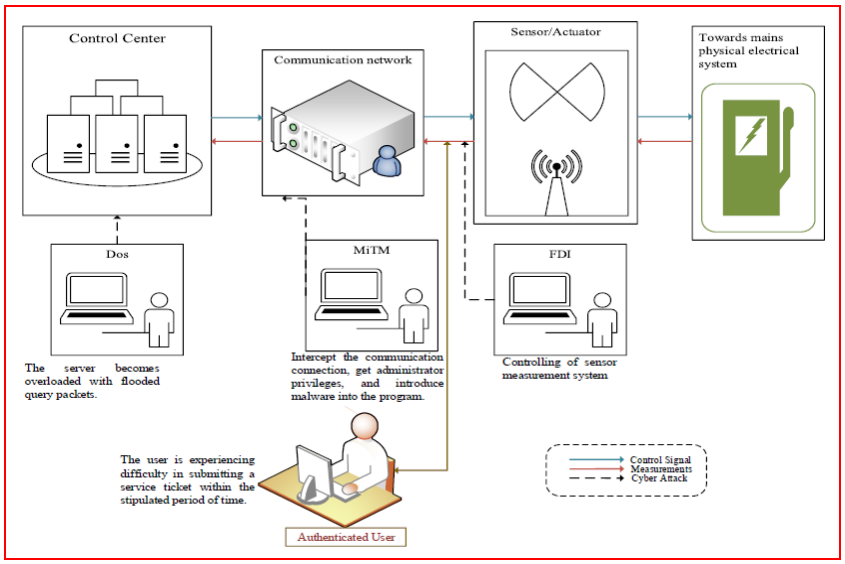

Fig. 2: Types of Cyberattacks

1.2 Denial of Services

A cyberattack that prevents an authorized user from interacting with a network is called a denial-of-service (DoS) attack. The attackers of this cyberattack can manipulate a small number of devices to cause harm to the electrical control system, even though they do not have full access to it. The goal of a DoS attack is to render a system unusable by flooding it with requests, denying access to authorized users. To prevent operators from responding to valid requests, the attackers use several customized distributed systems to send a substantial number of undesired queries to the target level. Demands and congestion overwhelm the system infrastructure, making it unable to respond to valid clients or processes. While these attacks are frequently associated with the disruption of websites or online services, they can also pose a major threat to critical infrastructure, including power grids. Network jamming is another form of denial-of-service attack. Since microgrid control is predicated on information sharing, DoS attacks pose a significant threat to their functionality. These types of assaults can be carried out without knowledge of the microgrid setups or the necessary skills to alter orders and measurements.

1.3 False Data Injection

The careful introduction of false or falsified information through the control networks or sensors in charge of keeping an eye on and managing the operation of the power grid is known as a False Data Injection (FDI) cyberattack in electrical systems. These attacks have the potential to have serious consequences, such as bodily harm, equipment malfunction, and power outages.
Malicious actors compromise electrical system sensors, such as voltage and current sensors, and then alter the data that is relayed. This is known as FDI. Adversaries can use fake data to manipulate such metrics and divert control systems from making appropriate judgments. In power systems, state estimate is crucial for ensuring system stability and dependability. FDI attacks have the potential to corrupt the data used for state estimation, leading to inaccurate assessments of the system's health. This could result in control systems making mistakes, such as failing to detect defects or making insufficient generation adjustments.
A sequence of failures could occur if incorrect data is injected into the electrical system and spreads throughout the network. Because FDI assaults often try to mimic typical system activity, they might be challenging to detect. To maintain credibility, attackers may carefully craft the data they introduce, making it challenging for system management to discern between accurate and fraudulent information. Attacks of this type alter data and may compromise system stability and reliability by exploiting flaws in the software, hardware, or communication regulations used in power electrical grids. Inaccurate state estimation and synchronization loss could emerge from the outcome, which would have a detrimental effect on economic dispatch and the supply of electricity to critical loads. This kind of erroneous data injection could harm the communication network, controller hardware, etc.

1.4 Reply Attack

In an electrical system, a reply-type cyberattack is when an adversary gains access to the system with the goal of altering data or interfering with its operation. Hackers may use hardware or software flaws to enter control systems without authorization during these attacks. This allows them to alter vital infrastructure or add false information to sensor readings. These kinds of attacks have the potential to seriously disrupt the economy, public safety, and the reliability of the electricity supply. Implementing stringent safety measures, such as regular system audits, establishing intrusion detection systems, and educating staff to recognize and promptly address any threats, is essential to preventing reply-type cyberattacks in power systems. Furthermore, the separation of networks and the use of encrypted communication protocols can both successfully limit the scope of assaults and lessen their effects.

1.5 Main-in-the-Middle Attack

An unauthorized third party can intercept and perhaps alter information between two authorized organizations within a power network between two legitimate devices, listen in on the discussion, or provide fake information or directives. This type of cyberattack is called a Man-in-the-Middle (MitM). Critical power system segments may also be the target of these attacks to gather information about communication with control center staff that may be utilized to launch more attacks. The attacker might disrupt the entire system by listening in on all requests and data sent between these actual devices.
Devices 1 and 2 are directly connected to a communication network in Figure 3, which illustrates a structural representation of MITM. A new connection is created by recording the two devices' conversation and sharing erroneous data across this intermediary channel.

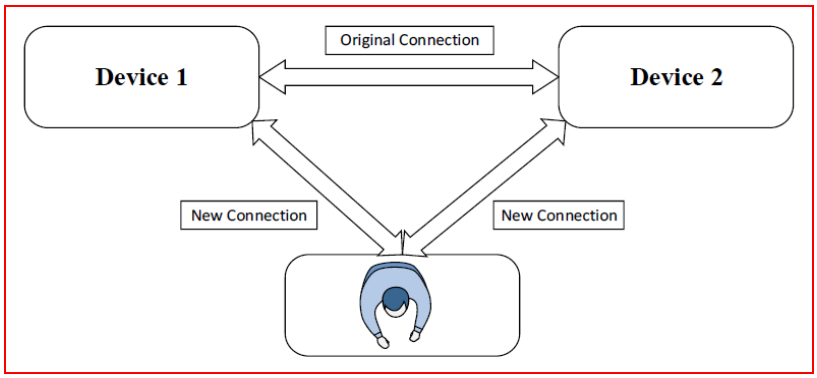

Fig. 3: Man in the Middle Cyberattack

1.6 Emerging Threats in the Cyber-Physical Layer of Active Distribution Networks:

The integration of advanced communication and control systems in active distribution networks (ADNs) has exposed them to increasingly sophisticated cyberattacks. While traditional threats like Denial-of-Service (DoS) and False Data Injection (FDI) attacks already compromise the reliability and stability of the power grid, emerging threats such as quantum computing-based attacks present an even greater risk. Quantum computing, with its ability to break traditional cryptographic algorithms rapidly, can potentially compromise data integrity and confidentiality in the communication layers of ADNs. This creates vulnerabilities in the CPL's layered structure, where secure data transmission and real-time monitoring are crucial.
The file highlights these vulnerabilities in the sensing, network, data processing, and application layers of CPL-based systems, making them susceptible to manipulations such as malicious data injections, man-in-the-middle attacks, and tampering of operational commands. As quantum computing evolves, it could break the encryption and authentication protocols that protect communication between sensors, controllers, and actuators, making quantum-based attacks a looming threat to the grid's stability and security.
Mitigating these emerging threats requires not only robust anomaly detection techniques using AI/ML, as explored in the document, but also the adoption of quantum-safe cryptography and resilient network designs that account for these advanced, future threats.

2. Techniques and Conceptualization of Problems

The distortion thereby induced by a malfunction or breach in one of the generators can be extended throughout the other generators by a synchronized control system that can put the entire system at risk. Finding anomalies in the control systems of the cyber-physical microgrid is still a challenge. A few disadvantages of traditional methods include a longer training period, hyper-parameter sensitivity, the possibility of data loss, and overfitting due to the discrete features of the transformation. These problems make it difficult to detect attacks in cyber-physical systems using traditional methods. Therefore, after the difficulties are identified, the goals are defined. Notable contributions consist of:

a. The goal is to develop an ideal machine learning algorithm that can reliably distinguish between a cyberattack and a fault in the cyber physics layer CPL-based IEEE-15 bus benchmark distribution system and the CPL-modified IEEE-15 bus system.
b. to identify the cyber-physical anomalies by introducing machine learning classifiers to the suggested SIFI model.
c. To create a method for employing DoS and FDI to identify cyberattacks.
d. Machine learning methods are compared to determine whether the anomaly is a cyberattack or a problem so that the performance of the constructed system can be evaluated.

3. Proposed System

The Modified IEEE-15 bus system, and the CPL-based IEEE-15 bus benchmark are employed in this research work. Both systems, as depicted in Figure 4, consist of two layers: the cyber layer and the physical layer.

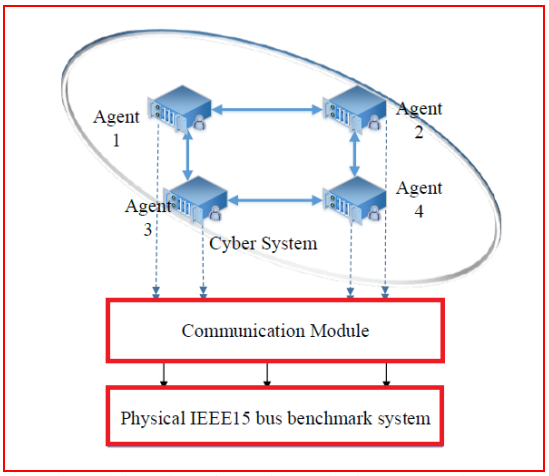

Fig. 4: Schematic representation of the cyber-physical layer in the IEEE 15-bus standard benchmark system.

The original IEEE-15 distribution system or its updated version, which is linked to the cyber layer, is the physical layer. Over a small network, the cyber layer makes it easier for physical components to communicate with one another. To provide the standard centralized secondary control, all the DGs must be connected to the central controller via an effective network. The cyber layer uses other algebraic variables and iterative computing to quantify cyber state variables. The state estimation unit's sensors provide precise real-time reading estimates, which are then sent to the processing unit. The computer unit uses a network connection to provide the estimated values to the controllers after processing the data.

The application, data processing, network, and sensing layers are the four distinct levels that comprise the structure of the cyber-physical layer. The first layer, referred to as the sensing layer, is composed of sensors and actuators connected to devices that collect and send physical or environmental data across the network. The second layer, referred to as the network layer, includes the data collecting system and the internet/network gateway. The data acquisition system gathers and combines data by converting analog data from sensors into digital format and transmitting it through an internet gateway. The data processing layer is the third layer. Prior to being transmitted to the data center, the data is pre-processed and examined in this layer. Applications for control and surveillance at the data center are used to access the data. In data centers or cloud environments, data management and storage are handled by the fourth application layer. End users then access and use this data for a variety of purposes.

This innovation improves skills in several applications. Using sensors, smart meters, communicative circuit breakers, and other intelligent electrical devices, the CPL microgrid uses a software interface to make the transition between physical and electrical distribution systems easier. With the help of the data provided, they can provide strong analytical capabilities. Critical operational technologies can now be operated and communicated with remotely, even at faraway locations, thanks to the use of CPL in distribution networks.

4. Attacks in the CPL Network

Two kinds of anomalies are taken into consideration in the modified IEEE-15 bus physical system and the cyber-physical IEEE-15 bus benchmark. The DoS at the bus node is thought to be the cause of the initial abnormality. The disconnection of network-connected resources is regarded as another FDI attack. The agent node-based IEEE-15 bus system, where the planned cyberattack is located, is depicted in Figure 5.

Intentionally adding false information to a network connection is known as malicious data injection. The attackers usually try to degrade the decision-making ability of the controller by injecting faulty data into the data stream of the cyber-physical layer. By carrying out phony data injections or transmitting misleading data to the microgrid carriers, hackers try to cause load shedding and needless tripping by increasing the reported electricity consumption to the electrical grid operator. The system controller may be alerted to a lagging power factor when a malicious risk exists. The cyber-physical layer operates at a leading power factor because of the controller's

inclusion of negative kVARs to stabilize the system's PF at unity. As a result, this dominant power factor may raise the voltage level within the secondary distribution system, which could harm household appliances.

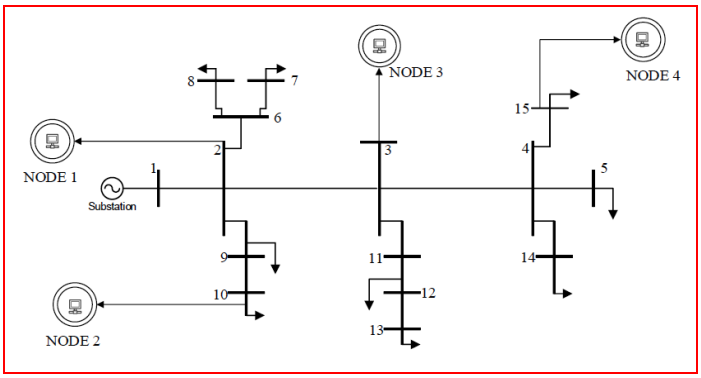

Fig. 5: IEEE-15 bus system with identified agent Nodes.

When people purposefully underreport their power usage to the operator to benefit financially by lowering their billing amount, this is known as electricity theft. Through obstruction or delay of the network connection, an intruder can make sure the operator doesn't notice changes in the load. By overloading the communication network with requests, the DoS attack takes advantage of flaws in the system and prevents the targeted components from operating as intended. Consequently, the server or communication network is unable to function effectively. A competent intrusion and fault detection system is therefore necessary.

5. Machine Learning-Based Analysis of Cyberattacks

The identification of cyberattacks or defects in CPL-based IEEE-15 and customized IEEE-15 bus systems is a good fit for machine learning methods. The cyber-physical layer module's defects and cyberattacks are found using an intelligent cyberattack and fault detection mechanism. To precisely ascertain the system's current state, the proposed method incorporates DT, NNN, and SVM classifiers. This involves determining whether the electrical distribution network is experiencing a real-time malfunction or a cyber-attack.

A cyberattack detection mechanism for the IEEE-15 bus benchmark and the updated IEEE-15 bus network system is depicted in Figure 6. For 60K samples, a database of voltage and current for symmetrical and asymmetrical faults is created. A unique categorization value is used to further classify the distribution network's defective and non-faulted statuses. The network is trained using machine learning classifiers, such as DT, NNN, and SVM, utilizing this database. Attacks of various stages, such as DoS and FDI at any node, are added in the very next step.

The distribution network's current state is made clear by interpreting this injected data as testing data. By altering sample values utilizing their multiplier changes in the original values, data manipulation is achieved. Disconnecting the different buses from their nodes also creates modified data utilizing the IEEE-15 bus. The machine learning classifier uses this data to train a network. The system is deemed to be in a real-time fault state if an attack is discovered to match the faulty data, or it is determined that the system is under cyber danger if no match is found. The modified IEEE-15 bus system and the CPL-based IEEE-15 bus benchmark both identify the cyber hazard of activity. The machine learning approach's results greatly aid in managing the distinction between an electrical distribution network outage and a cyberattack.

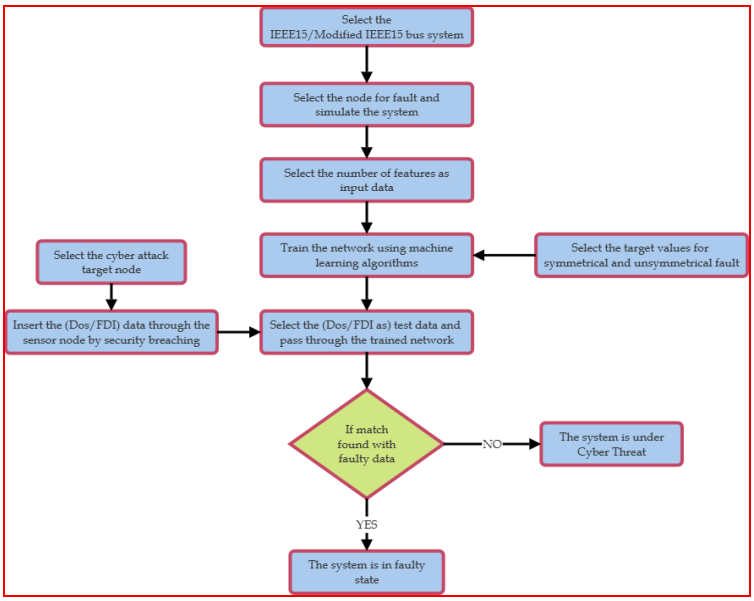

Fig. 6: Algorithm for cyberattack detection

6. Results

The CPL-based IEEE15 bus systems are subjected to performance analysis of cyberattacks and fault detection utilizing machine learning methods, such as DT, NNN, and SVM, to determine whether the system is experiencing a cyberattack or a malfunction. Two forms of cyberattacks—DoS and FDI—are suggested at various system nodes in the proposed study. The ML algorithms are thought to use the 3Ø Voltages and Currents as input. With the help of gathered data samples, the machine learning algorithms are trained and verified under no-fault, symmetrical, and unsymmetrical fault circumstances. To distinguish between a cyberattack and the existence of flaws, distinct target values are set.

The DoS and FDI attacks are proposed at the node of the IEEE15 bus network based on CPL to pick the cyberattack datasets. Both the DoS and FDI cyberattacks disrupted the sensor node and the real database. Until the problem is fixed, the network collapses because of these disturbances, which act as a network system breakdown. As illustrated in Figure 7, L-L-G faults are indicated by positions 4, 5, and 6 in the confusion matrix, while L-G fault validation is represented by places 1, 2, and 3. While the matrix 10 component suggests an L-L-L-G fault, positions 7, 8, and 9 imply an L-L fault. The DT network takes 13.14 seconds to train and has a validation error rate of 20.4%. The DT classifier maintains a validation error rate of 20.6% while achieving a validation accuracy of 79.56%. Overall, the SVM classifier has a 90.8% validation accuracy, whereas the NNN classifier has an 89.1% validation accuracy.

		Predicted Class										TPR	FNR
		1	2	3	4	5	6	7	8	9	10		
True Class	1	91.82	0.40		1.11	0.52	0.00	0.90	0.60	4.80		91.82	08.33
	2	0.81	93.28		0.40	3.12	0.10	1.46	0.10	0.90		93.28	06.89
	3	1.12	0.40	89.21	0.30	1.50	4.10	0.60	2.40	0.70		89.21	11.12
	4	0.00	0.10		94.00	1.10		5.30			0.00	94.00	06.50
	5	0.00				89.88	1.70		5.20		3.00	89.88	09.90
	6	0.00			0.50	0.60	93.52			3.50	1.90	93.52	06.50
	7	0.00	0.10	0.00	3.83	1.50		94.25	0.40	0.40	0.20	94.25	06.43
	8	0.00		1.43		12.81	0.80		82.15		1.90	82.15	16.94
	9	0.82	0.63	0.00	0.20	0.90	6.20		0.10	88.78	1.40	88.78	10.25
	10	0.00				5.80	0.20				94.68	94.68	06.00

Fig. 7: Validation matrix DT classifier

Figure 8 shows the validation matrix of SVM with an error rate of 9.2%

		Predicted Class										TPR	FNR
		1	2	3	4	5	6	7	8	9	10		
True Class	1	100.00										100.00	00.00
	2	0.00	100.00									100.00	00.00
	3	0.00		100.00								100.00	00.00
	4	0.00			100.00							100.00	00.00
	5	0.00				100.00						100.00	00.00
	6	0.00					100.00					100.00	00.00
	7	0.00						100.00				100.00	00.00
	8	0.00		0.12					100.00			100.00	00.12
	9	0.00								100.00		100.00	00.00
	10	0.00									100.00	100.00	00.00

Fig. 8: Validation matrix of SVM

The test data or the altered cyberattack data is run through the trained network following network validation. For both symmetrical and unsymmetrical defects, a test confusion matrix is seen. The confusion matrix in Figure 9 illustrates how the DT classifier predicts fault categorization during a cyberattack.

		Predicted Class											TPR	FNR
		0	1	2	3	4	5	6	7	8	9	10	11	
	0	74.10	1.62	24.3										74.10	24.30
True Class	1		100.00											100.00	
	2		0.41	99.49										99.49	00.41
	3		0.41	17.43						82.16					100.00
	4					100.00								100.00	
	5		0.41				82.05						17.59	82.05	18.00
	6					15.24		84.82						84.82	15.24
	7		0.41						99.61					99.61	00.41
	8		0.41				74.20			20.81			4.83	20.81	79.44
	9					15.24					84.91			84.91	15.24
	10		0.41										99.59		100.00
	11		0.41										99.60	99.60	00.41

Fig. 9: Test Confusion result matrix DT classifier

The classification rate of cyberattacks using the fault data is known as the true positive rate, or TPR. The fact that DT categorizes the cyberattack data as fault data is shown in the confusion matrix. Better accuracy in classifying cyberattacks is predicted by the false negative rate (FNR). The accuracy of cyberattack detection is thus represented by the overall misclassification rate.
The DT classifier demonstrates a 70.4% classification rate for cyber data as a fault. For the SVM and NNN, similar findings have been made. The test confusion matrix derived from SVM is shown in Figure 10. Figure 10 displays the classification characteristics from SVM, with the lowest classification range of 9.9% for cyberattacks from fault data. In the active distribution network, the improved misclassification findings demonstrate accurate prediction of cyberattacks. With a 90.1% success rate, SVM is shown to be the superior cyberattack classifier in this case.

		Predicted Class												TPR	FNR
		0	1	2	3	4	5	6	7	8	9	10	11		
True Class	0		100.00												100.00
	1		100.00											100.00	
	2		100.00												100.00
	3		84.77					15.23							100.00
	4		100.00												100.00
	5		87.86										12.00		99.86
	6		100.00												100.00
	7		100.00												100.00
	8		92.42										7.58		100.00
	9		100.00												100.00
	10		80.82									0.42	18.86	0.42	99.68
	11		80.82									0.42	18.86	18.86	81.24

Fig. 10: Test Confusion result matrix using SVM

Case study: Denial of Service
In the first scenario, the CPL-based IEEE-15 bus system's Node 2 is the target of the DoS cyberattack. When an unequal load is linked as a real-time request, the attack is suggested to inject data into the system, causing the system to enter a failure or breakdown condition. DG-based modified IEEE-15 bus systems are believed to have the same observation. The 3-phase voltage and current exhibit a more subtle variance in this observation. This data is fed into the trained network classifier and is regarded as testing data.
The symmetrical faults data, where the DoS threat has been categorized in the IEEE-15 bus radial distribution network, is displayed in Figures 11 and 12. The cyberattack had the lowest classification value of 58.5% for L-L-L fault situations and 19.5% for L-L-L-G fault conditions according to the DT classifier. NNN classifies the DoS assault with an accuracy of 62% and 54.4%, respectively, in the case of symmetrical defects. With a maximum rating of 99.6% and 100%, the SVM similarly categorized the incident as the same defect.

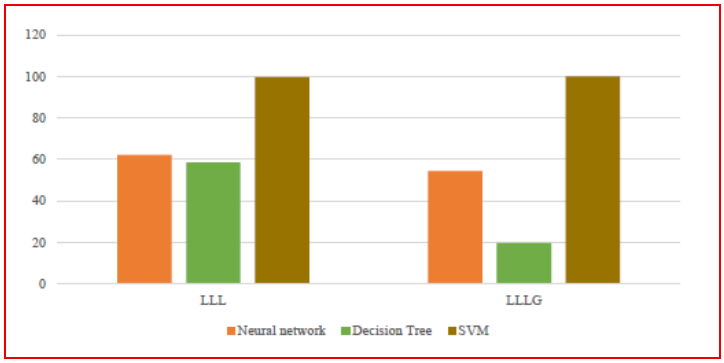

Fig. 11: DoS detection in a symmetrical fault in an IEEE-15 bus radial distribution system based on CPL

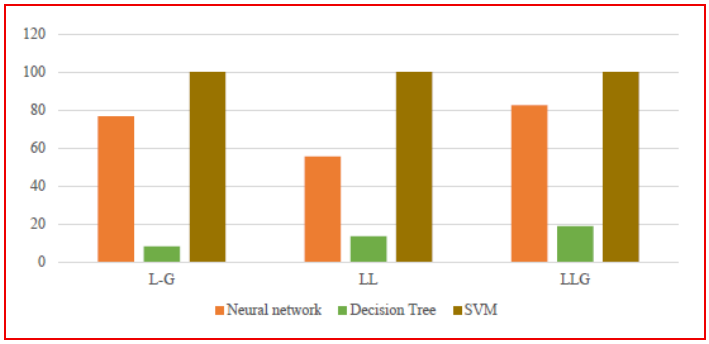

Fig. 12: DoS detection in an unsymmetrical malfunction in an IEEE-15 bus distribution network based on CPL

The accuracy of DT's cyberattack classification in the case of an unsymmetrical fault is 8.6% for L-G, 13.43% for L-L, and 18.8% for L-L-G faults, respectively. The accuracy of the NNN's assault prediction was 76.66%, 55.46%, and 82.4%. SVM identified the cyberattack under L-G, L-L, and L-L-G fault situations with 100% classification accuracy.

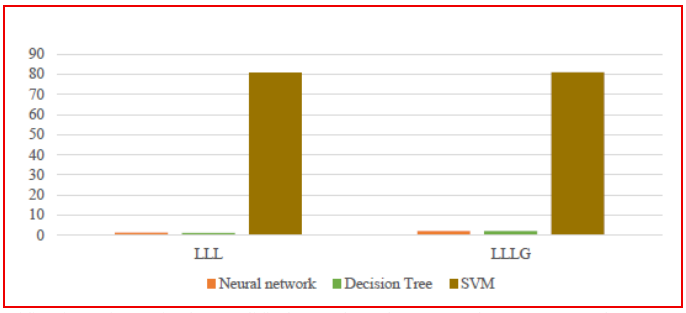

Fig. 13: Classification of DoS in the modified CPL-based IEEE-15 bus system under symmetrical faults

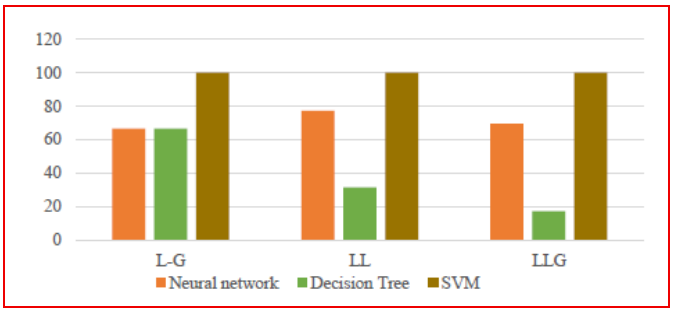

Fig. 14: Classification of DoS in the modified CPL-based IEEE-15 bus system under unsymmetrical faults

In a similar vein, DG-based modified IEEE-15 bus systems have been subject to a DoS attack. The accuracy of classification is displayed in Figures 13 and 14. With 66.32, 31.58, and 16.92% for unsymmetrical fault types, DT has the lowest classification. L-G, L-L, and L-L-G fault classification accuracy has increased at a rate of 66.36%, 77.29%, and 69.25%, respectively. When symmetrical faults occur, the cyberattack is classified as a system fault by DT and NNN. As seen in Figure 4, SVM can classify cyberattacks with a maximum accuracy of 80.28% and 81.08%. SVM achieves 100% accuracy in classifying the DoS in unsymmetrical fault data.

The categorization outcome of the DoS attack in the modified IEEE-15 bus system and the cyber-physical layered IEEE-15 bus system is shown in figure 15. The SVM classifier has the highest accuracy of 90.28% in classifying DoS attacks in the IEEE-15 bus system, while the DT classifier has the lowest accuracy of 29.05%. The SVM has a maximum validation of 90.12%.

With validation percentages of 73.89%, 86.19%, and 93.21%, respectively, the DT, NNN, and SVM are highly effective in the context of the modified IEEE-15 bus system. The SVM classifier identified the cyberattack with the best accuracy of 92.58%, while the DT had the lowest performance in attack classification with a rate of 23.54%

Sr. No.	Machine Learning Classifier	Features	Preset	CPL-based IEEE-15 bus system		CPL-based modified IEEE-15 bus system	
				Validation	Accuracy	Validation	Accuracy
01	Decision Tree	Voltage and Current	Fine Tree	78.86	29.05	73.89	23.54
02	Neural Network		NNN	88.95	66.88	86.19	43.05
03	SVM		Fine Gaussian SVM	90.12	90.28	93.21	92.58

Fig. 15: Analyzing DoS attacks in comparison with machine learning methods

7. Conclusion

In this study, a comprehensive analysis was conducted on the cyber vulnerabilities associated with Distributed Generation (DG)-based power networks, particularly focusing on Active Distribution Networks (ADNs). The integration of advanced communication technologies within these systems has opened new avenues for efficiency, but simultaneously introduced significant cyber threats. Key cyberattacks such as False Data Injection (FDI) and Denial of Service (DoS) were modelled and investigated using a Cyber-Physical Layered (CPL) approach on the IEEE-15 bus benchmark and modified systems.

To effectively distinguish between physical faults and cyberattacks, machine learning classifiers—Decision Tree (DT), Nearest Neighbor Network (NNN), and Support Vector Machine (SVM)—were employed. The results demonstrate that while all three classifiers were effective to varying degrees, SVM achieved the highest detection accuracy, making it the most reliable technique among the evaluated methods.

References

[1] 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, doi: http://dx.doi.org/10.1109/TSG.2011.2119336.

[2] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU Placement Protection Against Coordinated False Data Injection Attacks in Smart Grid," IEEE Trans. Ind. Appl., vol. 56, no. 4, pp. 4381–4393, Jul. 2020, doi: http://dx.doi.org/10.1109/TIA.2020.2979793.

[3] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," J. Netw. Comput. Appl., vol. 170, p. 102808, Nov. 2020, doi: http://dx.doi.org/10.1016/j.jnca.2020.102808.

[4] B. M. R. Amin, A. Anwar, and M. J. Hossain, "Distinguishing Between Cyber Injection and Faults Using Machine Learning Algorithms," in 2018 IEEE Region Ten Symposium (Tensymp), Jul. 2018, pp. 19–24. doi: http://dx.doi.org/10.1109/TENCONSpring.2018.8691899.

[5] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems," IEEE Trans. Ind. Inform., vol. 13, no. 2, pp. 436–447, Apr. 2017, doi: http://dx.doi.org/10.1109/TII.2016.2612645

[6] B. M. R. Amin, S. Taghizadeh, Md. S. Rahman, Md. J. Hossain, V. Varadharajan, and Z. Chen, "Cyber-attacks in smart grid – dynamic impacts, analyses and recommendations," IET Cyber-Phys. Syst. Theory Appl., vol. 5, no. 4, pp. 321–329, 2020, doi: http://dx.doi.org/10.1049/iet-cps.2019.0103.

[7] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes," IEEE Trans. Power Syst., vol. 35, no. 1, pp. 440–450, Jan. 2020, doi: http://dx.doi.org/10.1109/TPWRS.2019.2924441.

[8] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," IEEE Trans. Smart Grid, vol. 8, no. 2, pp. 572–580, Mar. 2017, doi: http://dx.doi.org/10.1109/TSG.2016.2545683.

[9] F. Ünal, A. Almalaq, S. Ekici, and P. Glauner, "Big Data-Driven Detection of False Data Injection Attacks in Smart Meters," IEEE Access, vol. 9, pp. 144313–144326, 2021, doi: http://dx.doi.org/10.1109/ACCESS.2021.3122009.

[10] L. Wang and A. A. Girgis, "On-line detection of power system small disturbance voltage instability," IEEE Trans. Power Syst., vol. 11, no. 3, pp. 1304–1313, Aug. 1996, doi: http://dx.doi.org/10.1109/59.535671.

[11] Vijaykumar Kamble, Ajit Bansode, Tushar Waghmare, Kalyan Bamane, "Development of Hybrid Compensators for Enhancing Power Quality in Electrical Distribution Systems Using Innovative Optimization Techniques" International Journal of Smart Grid, Vol.9, No.1, March 2025

[12] P. K. Reddy Shabad, A. Alrashide, and O. Mohammed, "Anomaly Detection in Smart Grids using Machine Learning," in IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society, Oct. 2021, pp. 1–8. doi: http://dx.doi.org/10.1109/IECON48115.2021.9589851.

[13] E. Naderi and A. Asrari, "Toward Detecting Cyberattacks Targeting Modern Power Grids: A Deep Learning Framework," in 2022 IEEE World AI IoT Congress (AIIoT), Jun. 2022, pp. 357–363. doi: http://dx.doi.org/10.1109/AIIoT54504.2022.9817309.

[14] D. Thukaram, H. P. Khincha, and H. P. Vijaynarasimha, "Artificial neural network and support vector Machine approach for locating faults in radial distribution systems," IEEE Trans. Power Deliv., vol. 20, no. 2, pp. 710–721, Apr. 2005, doi: http://dx.doi.org/10.1109/TPWRD.2005.844307.

[15] M. Mirzaei, M. Z. A. Ab. Kadir, H. Hizam, and E. Moazami, "Comparative Analysis of Probabilistic Neural Network, Radial Basis Function, and Feed-forward Neural Network for Fault Classification in Power Distribution Systems," Electr. Power Compon. Syst., vol. 39, no. 16, pp. 1858–1871, Oct. 2011, doi: http://dx.doi.org/10.1080/15325008.2011.615802.

[16] G. B. Gaggero, P. Girdinio, and M. Marchese, "Advancements and Research Trends in Microgrids Cybersecurity," Appl. Sci., vol. 11, no. 16, Art. no. 16, Jan. 2021, doi: http://dx.doi.org/10.3390/app11167363.

[17] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids," IEEE Trans. Smart Grid, vol. 12, no. 3, pp. 1929–1938, May 2021, doi: http://dx.doi.org/10.1109/TSG.2020.3047949.

[18] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal Temporal Logic-Based Attack Detection in DC Microgrids," IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 3585–3595, Jul. 2019, doi: http://dx.doi.org/10.1109/TSG.2018.2832544.

[19] M. S. S. Hakim and H. K. Karegar, "Detection of False Data Injection Attacks Using Cross Wavelet Transform and Machine Learning," in 2021 11th Smart Grid Conference (SGC), Dec. 2021, pp. 1–5. doi: http://dx.doi.org/10.1109/SGC54087.2021.9664053.

[20] Y. Yang, L. Guo, X. Li, J. Li, W. Liu, and H. He, "A Data-Driven Detection strategy of False Data in Cooperative DC Microgrids," in IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society, Oct. 2021, pp. 1–6. doi: http://dx.doi.org/10.1109/IECON48115.2021.9589318.

[21] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 10, pp. 2765–2777, Oct. 2019, doi: http://dx.doi.org/10.1109/TIFS.2019.2902822.

[22] A. Kavousi-Fard, W. Su, and T. Jin, "A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids," IEEE Trans. Ind. Inform., vol. 17, no. 1, pp. 650–658, Jan. 2021, doi: http://dx.doi.org/10.1109/TII.2020.2964704.

[23] A. Basati, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, and S. Golestan, "A Data-Driven Framework for FDI Attack Detection and Mitigation in DC Microgrids," Energies, vol. 15, no. 22, Art. no. 22, Jan. 2022, doi: http://dx.doi.org/10.3390/en15228539.

[24] E. Tian, Z. Wu, and X. Xie, "Codesign of FDI Attacks Detection, Isolation, and Mitigation for Complex Microgrid Systems: An HBF-NN-Based Approach," IEEE Trans. Neural Netw. Learn. Syst., vol. 35, no. 5, pp. 6156–6165, May 2024, doi: http://dx.doi.org/10.1109/TNNLS.2022.3230056.

[25] Farhad Zishan, "Investigating the Reliability and Optimal Capacity of Microgrid Electricity Storage Systems with the Aim of Reducing Costs" International Journal of Smart Grid, Vol.8, No.3, September 2024

[26] Z. S. Warraich and W. G. Morsi, "Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids," Sustain. Energy Grids Netw., vol. 34, p. 101027, Jun. 2023, doi: http://dx.doi.org/10.1016/j.segan.2023.101027.

[27] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids," IEEE Syst. J., vol. 16, no. 1, pp. 1487–1498, Mar. 2022, doi: http://dx.doi.org/10.1109/JSYST.2021.3086145.

[28] Ehsan Nazemorroaya, Mohsen Shafieirad, Mahdi Majidi, Mahdieh Adeli, "Consensus-Based Algorithm for Distributed Continuous-Time Convex Optimization Over Undirected and Directed Networks" Journal of Applied Research in Electrical Engineering, Vol. 3, No. 1, pp. 74-82, 2024