TRUST PRIORITY BASED CLUSTERING MODEL FOR MALICIOUS ATTACKS DETECTION WITH SECURE DATA TRANSMISSION IN SMART GRIDS

CHADALAVADA NAGA PRIYANKA[1], NANDHAKUMAR RAMACHANDRAN[2]
[1,2]School of Computer Science and Engineering, VIT-AP-522237, Andhra Pradesh, India.
E-mail: [1]nagapriyankach79@gmail.com [2]nandhakumarr03@gmail.com

ABSTRACT

The use of Smart Grids (SG) and smart meters is becoming widespread in several nations. Hackers with even a rudimentary understanding of computers can compromise smart meters and conduct cyber attacks. Government security and network operators are at risk in this cyberspace. SG companies should create defensive and preventative measures to lessen the impact of electricity theft on their bottom lines. Cyber assaults can compromise cyber-physical systems. In order to identify a cyber attack on the smart grid, numerous methods have been developed. Among the best security measures, weighted trust-based models are recommended. SGs use clustering model to group smart meters for monitoring them. There can be no trust unless the sensors work as intended, if they can communicate with one another, and if the nodes' servers are reliable. How the nodes have communicated in the past also has a role. This research proposes a smart grid sensor network security technique that is based on trust weights in a clustering model. The total trust of nodes by adding up their direct and indirect trust is performed in the smart grid that in a cluster. The presence of numerous bidirectional communication devices connecting consumers to the grid makes smart grid networks particularly vulnerable to network attacks. Malicious assaults can compromise the Smart Grid Network's backbone infrastructure, which consists of information and communication technologies. For the uninterrupted and effective supply of energy and to generate an accurate bill, it is vital to detect the assault and work on it. A large number of compromised grid communication devices or nodes send a flood of false data or requests to the smart grid network, which can disrupt smart meters, data servers, and the state estimator. As a result, end-user services could be affected. When it comes to protecting the network from malicious attacks, a malicious node detection model is proposed. The innovative model detects and eliminates malicious nodes from the network after successfully differentiating between physical and cyber intrusions. Data transmission in a smart grid is accomplished by wireless technologies. There are a variety of network attacks that could compromise SGs. When it comes to protecting massive communication networks from hostile network attacks, trust models are a key component. To avoid malicious actions in the SGs, this research proposes a Trust Priority based Clustering model to detect and avoid Malicious Attacks (TPbCMA) for secure data transmission and increasing the quality of service levels in smart grids. The proposed model efficiently detects the attacks in the smart grids to maintain quality of service levels. The proposed model achieved 98.7% accuracy in Node Clustering and 99.1% accuracy in Malicious Action Detection. The proposed model when contrasted with the traditional models performs superior than traditional models.

Keywords: *Smart Grid, Smart Meter, Cyber Attacks, Cyber Security, Malicious Attacks, Direct Trust, Indirect Trust, Clustering.*

1. INTRODUCTION

By combining conventional power grids with modern information and communication technology, "smart grids" enhance power distribution and management [1]. Nonetheless, they bring about fresh security holes that cybercriminals might use to their advantage, which can have disastrous results like infrastructure destruction and widespread power outages [2]. Modern electricity usage and demand are going to skyrocket, and traditional power systems just can't keep up. There are a lot of factors contributing to this, such as problems with automated analysis and situational awareness, poor vision, and slow response times [3]. Smart grids enable more dependable power distribution and better demand-side management by utilizing modern information and communication technologies to create a two-way flow of data and electricity. A smart grid's three tiers of hierarchical organized communication link the four main components: generation, transmission, distribution, and consumption. Consumers' smart home appliances can be linked to the smart grid by Smart Meters (SM) [4], which are transmitted at the consumption stage by the Home Area Network (HAN), the first level of the communication network, to enhance energy management and demand response. In order to relay control orders for sophisticated metering applications and receive data from smart meters, the distribution stage establishes contact with the Neighborhood Area Network (NAN), the second tier of the communication network [5]. Connecting NANs to utility control centers at the top level, the Wide Area Network (WAN) satisfies the communication requirement of the smart grid's power generating and transmission stages [6].

While traditional power grids gain greatly from the incorporation of advanced ICTs for power distribution and control, these same grids simultaneously become more susceptible to new security threats [7]. Cyber assaults can affect physical power systems; two common instances are the Aurora attack and the Stuxnet virus. A cyber attack in Ukraine recently knocked power off for hours, affecting over 200,000 customers. All of these incidents highlight the need to strengthen smart grid security in order to prevent cyber assaults. Here, a way to detect cyber assaults using data collected by phasor measuring units (PMUs) is considered. For the purpose of wide area monitoring, protection, and control, a PMU is a sensor device that is installed at the WAN level of a smart grid network [8]. It offers real-time measurements of the power system conditions. A phasor data concentrator (PDC) links several PMUs in a WAMS. After that, the data is gathered from PDCs by the WAMS central authority [9].

Smart Grid technologies are poised to revolutionize existing sectors by enhancing the efficiency of conventional electric networks. The term Smart Grid describes an electrical distribution system that relies on electronic communication. Issues including power outages, overheating, and voltage drops have arisen as a result of the increased demand [10]. Another important factor in reducing the impact of the cyber attack is the rise in carbon emissions from the current electrical network. Unfortunately, the US absorbs as much as 40% of the nation's CO_2 emissions. The Smart Grid is expected to improve the system's availability, efficiency, and reliability by integrating state-of-the-art communication and calculating capabilities [11]. Smart Grids can also communicate with one another, which is a great feature. Renewable energy sources, including as solar panels and wind turbines, have long been a part of the Smart Grid's history, alongside fossil fuels and natural gas. Many different kinds of smart devices, transformers, and machines can reap the benefits of the Smart Grid's efficient power delivery and usage. It achieves these objectives by switching from the conventional grid system's one-way communication to a two-way one. The Smart Grid enables the rapid adoption of solutions to energy problems while also improving and speeding up customer services [12]. The smart grid general architecture is shown in figure 1.

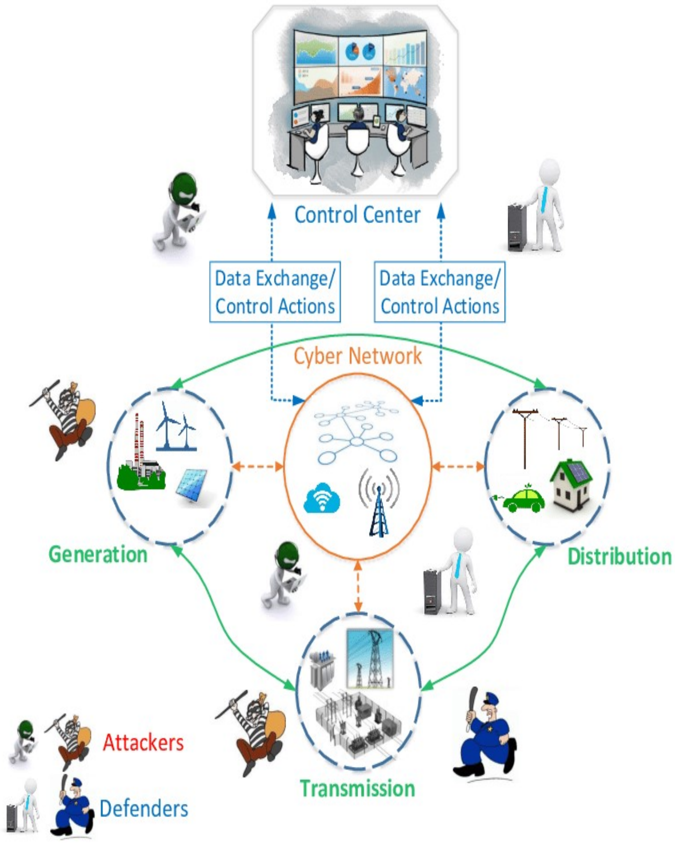

Fig 1: General Architecture of Smart Grid

Nevertheless, there are several drawbacks to Smart Grid technology. One major issue is that it cannot protect data, which is an extremely important asset [13]. Since the Smart Grid could retain sensitive information, data sharing will need to happen often. There will be a proliferation of interconnected devices, both at home and in the workplace, that will use various forms of cyber security to communicate with one another and keep the networks safe. Securing the Smart Grid from cyber threats is of the utmost importance [14]. In order to address these intricate issues, a number of security methods will be examined and evaluated. Electricity generation, distribution, and consumption are all handled by a smart grid that makes use of communication and information technologies [15]. Implementing two-way information flow allows for the integration of renewable technologies to decrease carbon footprint, real-time control, operational efficiency, and greater grid resilience. Theft or manipulation of sensitive data transmitted across smart grid networks poses a risk to user privacy. Following the discovery of these issues, the smart grid has attracted the attention of both public and private organizations [16]. Threat actors are increasingly targeting smart grids with False Data Injection (FDI) assaults [17]. Current data detection technologies are so inadequate that they cannot detect sneaky FDI attacks. One possible replacement for FDI detection is machine learning [18]. The concept of a false data injection attack (FDIA) initially emerged in a smart grid context. Even though it seems like tampering, there are actually quite a few methods an attacker can manipulate sensor readings in order to sneakily alter state variables and values [19]. Injection attacks allow for the injection of malicious input into online applications, which can then be used to execute specified commands [20].

Distributed systems are far more complex, include a variety of smart software-controlled components, and have wider network connectivity than large-scale, centralized structures that rely on offline or private network elements controlled by proprietary code. This transition is happening all over the world in electrical infrastructures [21]. By incorporating a multitude of smaller power sources, such commercial wind farms or individual customer solar panels, these systems are able to more effectively route power from supply to demand, which is just one of many benefits [22]. We can manage and monitor most, if not all, components remotely, and there are more interconnected software control systems in use than ever before—all in an attempt to keep costs down. On the other hand, this makes systems vulnerable to hostile influence from entities that aren't necessarily physically close to them. Given the enormous damage that can be caused by disconnecting electrical infrastructure, this is also an obvious target for state-funded and well-organized gangs [23].

Malicious assaults on electricity systems are considered where an attacker takes over a group of meters and tampers with their readings. Two attack regimes are analyzed. The adversary assaults enough meters in the strong attack regime for the control center to no longer be able to observe the network state. A graph theoretic technique is used to characterize the smallest set of attacked meters that can cause network unobservability for assaults in this regime. The identification of the lowest set of vulnerable meters is demonstrated to have polynomial complexity by recasting the problem as one of minimizing a supermodular graph functional.

A thorough review of smart-grid applications and components is required first, along with the identification of susceptible components and possible cyberattack types. In addition, it is critical to comprehend the short-term and long-term techno-economic-safety-social consequences of cyberattacks on smart grids, particularly the domino effect on linked parts. Research on actual cyberattacks on live smart grids, as well as the creation of quantitative models and metrics to measure their effects, are essential. Further research is also required to determine the effects of cybersecurity measures on live smart grids and to provide quantitative models and metrics for evaluating these effects.

By integrating Cyber Physical Systems (CPS) with information and communication technology, smart grids improve the performance of traditional power networks. Electricity providers may now offer low-cost, dependable power with little losses with these technologies. These CPS have many benefits, but they are vulnerable to several types of assaults that might compromise sensitive information [24]. Much of the research that attempts to address these smart grid vulnerabilities has pointed to malicious actions detection models as a viable option. Nevertheless, such systems' primary issues are around their resilience, precision, and ability to adapt to novel threats. Big energy systems provide data at a rate and volume that traditional threat detection systems can't keep up with. Cyber security systems must continue to be robust and efficient in order to handle these emerging threats and successfully identify harmful network data [25].

Smart grids have emerged as a result of the increasing dependence on interconnected technologies in contemporary power systems. These grids offer improved efficiency and sustainability and aim to mitigate the effects of climate change. On the other hand, these vital infrastructures are vulnerable to a plethora of cyber threats due to their rising complexity. A thorough comprehension of smart grids' components, vulnerabilities, and possible repercussions is crucial due to the increasing frequency and complexity of assaults on these systems.

There will probably be tighter integration between the cyber infrastructure for sensing, control, scheduling, dispatch, and billing in future smart grids. In order to control generation and enable two-way communications between customers and providers, utility companies already depend on computer networks. A smart grid cannot exist without such interconnection, but this critical physical infrastructure is also more susceptible to cyberattacks from enemies all around the world. A generator reportedly self-destructed after researchers conducted an experimental cyber assault, and it has been widely claimed that cyber spies had hacked the US electrical grid. A uniformly most powerful test does not exist in general, and the challenge of detecting malicious data cannot be expressed as a simple hypothesis test since the adversary can pick where to attack the network and design the injected data.

Data infiltration assaults are the most common kind of cyber attack that targets the smart grid. The three most common types of data intrusion assaults are Denial-Of-Service (DoS), Load Redistribution (LR), and FDI. Attacks like these give CAs the ability to change the data used by the power grid for management and control purposes, which can compromise the system's safety, lead to financial gain, or even cause physical damage. Identifying and distinguishing aberrant data from normal data is a crucial capability for modern malicious nodes detection [26]. Malicious actions detection systems protect networks from malicious actors and keep data accessible at all times. In its most basic form, the malicious attacks detection system is built on this paradigm. Since engineering problems are often nonlinear, ill-defined, and noisy, intrusion detection models are essential for dealing with them. Resolving such issues requires the implementation of an attack detection model that is resilient, dependable, and cost-efficient [27]. This concludes the part that offered an overview of current research into making smart grid malicious actions diagnosing models better. The attacks in smart grid network is shown in Figure 2.

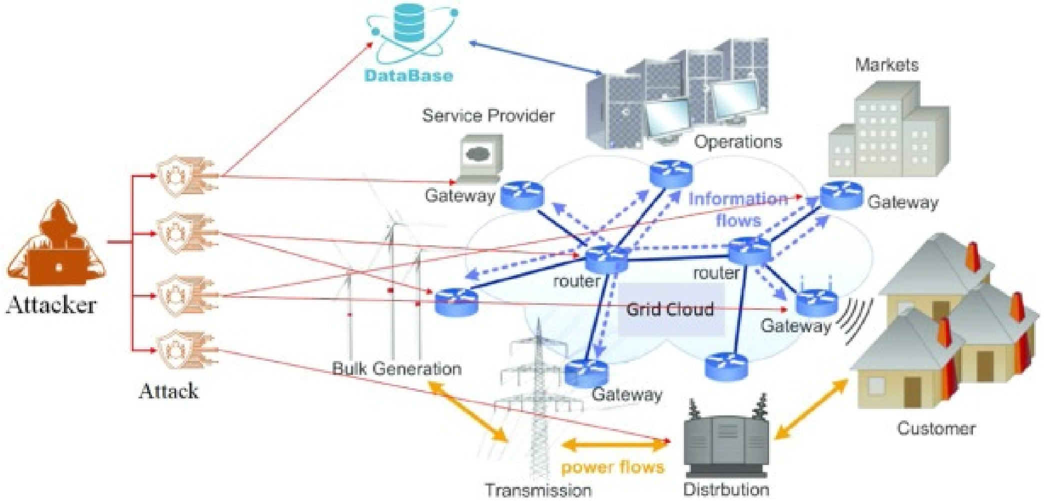

Fig 2: Attacks in Smart Grid

In order to safeguard against malicious interference, solutions that go beyond patching are now essential due to the increased technical complexity and interconnectedness. One component of that defense-in-depth strategy has been the incorporation of learning algorithms to track command and sensor data traffic in networks. This helps identify injected commands and data that could be used to manipulate physical systems that are meant to safeguard electrical components from harm. The problem with detecting attacks is that sensor data can be almost indistinguishable from anomalous readings that have been maliciously injected, such as when electrical transmission lines are down for emergency maintenance or when lightning strikes near the substation. To avoid malicious actions in the SGs, this research proposes a Trust Priority based Clustering model to detect and avoid Malicious Attacks (TPbCMA) for secure data transmission and increasing the quality of service levels in smart grids.

2. LITERATURE SURVEY

A smart grid incorporates state-of-the-art sensors, efficient measuring methods, advanced control technology, and other tools to ensure the grid system operates safely, efficiently, and affordably. However, because the smart grid is both dynamic and open, its energy and data are vulnerable to malicious attacks. Data integrity attacks are typical cyber-physical attacks that significantly impact grid functioning since the attackers might vary their attack vector to avoid traditional detection methods. Following the description of an adversarial attack method for power grid dynamic state estimation by D. An et al. [1], this study recasts the data integrity assault detection problem as a partially observable Markov decision process exhibiting sequential decision behavior. The multi-step learning method is employed to enhance the precision of the Q value estimation. An approach called prioritized experience replay has been put up to address the scarce rewards problem and improve training efficiency.

Smart grid technology has quickly become the standard for future power systems due to its ability to make choices, allocate resources efficiently, and monitor systems in real-time. Due to the linked structure of the information system and the power physical system, a smart grid is susceptible to dangers such as hostile attacks. The fact that fake data injection attacks (FDIAs) are able to circumvent traditional bad data detection methods is a major and challenging problem with smart grid operations. Using matrix separation theory, Huang et al. [2] introduced a novel method for attack detection. It successfully detects FDIA by examining the structural sparsity of the attack matrix and the low-rank feature of the unattacked measurement matrix. Furthermore, a structural sparse matrix separation method is proposed to improve the precision of attack detection. To make sure the plan was effective, the author ran testing under three distinct attack scenarios.

The newer, smarter smart grid is more efficient, flexible, and trustworthy than the older, less reliable electrical infrastructure. However, because to the increasing diversity of application needs, it struggles to find a balance between data privacy, efficiency, and robustness. In this paper, Pang et al. [3] presented a smart grid model that makes use of fog computing. In addition to facilitating communication for aggregated, malicious smart grid consumption data, the proposed model is the foundation for an efficient and privacy-preserving approach. To address problems like erroneous data detection, this smart grid solution is the first of its kind to integrate secure aggregate communication with data privacy and data resilience. Specifically, households can safely send data about their power use to the cloud and fogs via Boolean/Arithmetic secret-sharing protocols, according to the proposed method. To further protect against malevolent home users who try to insert fraudulent data, a method for detecting spurious data is proposed.

Yan et al. [4] investigated the cyber-physical system problem of attack detection of fake data injection attacks for a certain sort of large-scale smart grid system. Remaining signals for the assault detection task are sourced from a meticulously constructed bank of dynamic reduced-order observers. By decomposing the system under consideration into a network of interdependent subsystems, graph theory paves the way for this bank. We next propose a novel decentralized attack detection system that makes use of adaptive detection thresholds that meet the performance requirements. The proposed detection method is more robust against process disruption and measurement noise, and it uses less conservative thresholds, therefore it is more detectable than the present results. Lastly, two simulations and experimental data from an IEEE 30-bus system built in the OPAL-RT real-time simulator validate the accessibility and efficacy of the proposed scheme.

Because of the growing openness of network settings brought about by the proliferation of information and communication technologies, smart-grid control systems are extremely susceptible to hostile attacks. Under the radar, FDI attacks alter measurement data, leading the control center to make incorrect decisions that have a significant impact on the power system's regular operation. In this paper, Lei et al. [5] presented a method for detecting FDI attacks that makes use of edge computing for real-time data collecting and is based on CPRs. At the periphery of the sensing network, the CPR scheme generates a reliable prediction model to foretell the collected measurement data. It improves detection accuracy by classifying anticipated residuals apart from incorrect data using a new real-time classification algorithm supported by edge devices. These two measures substantially enhance the FDI assault detection rate. An actual microgrid testbed verifies the suggested method. The experimental findings demonstrate that the CPR method is effective in identifying FDI attacks and maintains sensitivity to the likelihood and severity of injection attacks. Even with a low injection attack probability of 5% and magnitude of 0.018 per thousand, the detection technique is effective.

Cyberattacks on Industrial Control Systems (ICS) have been devastating in several sectors, including critical infrastructure, due to malware that masqueraded as an ICS process and transmitted legitimate ICS messages. Such actions are often missed by more traditional approaches. When it comes to ICS communications, intrusion detection systems (IDSs) typically employ pre-defined patterns to weed out harmful messages, whereas anomaly detection systems (ADSs) depend on statistics to spot unusual data packets by searching for specific traits, rather than performing in-depth analysis. Havlena et al. [6] presented a new detection method that uses Deterministic Probabilistic Automata (DPAs) to capture the intended semantics of the ICS message exchange. Using a set of DPAs that represent expected traffic patterns, the method may simulate the sequence of messages sent by ICS. The detection system employs model reasoning to unearth harmful actions in the ICS flow whenever it detects suspicious ICS signals. This study shows that the automata-based detection method is more effective and has a lower false-positive rate. A technique that produces additional information about detected abnormalities was also provided by the author, which is crucial for practical implementation.

Cyberattacks are a real possibility with the Smart Grid due to the extensive usage of many forms of communication, control, and information technologies. Cyber assaults, if undetected by security systems, might compromise critical power system infrastructure and the services offered to many energy users. In particular, hackers might get control of the smart grid and install malicious instructions. A new tool for the Cyber-Physical Security Assessment (CPSA) of hostile control instructions that target actual smart grid components in real-time was developed by Saxena et al. [7] to address these concerns. The tool can identify and prevent known Trojans like BlackEnergy. It does more than just identify malicious commands; it also examines the power system's health in real-time and does it fast and effectively. The security analysis of this approach takes a look at three system-generated metrics: threat capability, access points, and system susceptibility. An examination of performance takes into account factors such as overhead, precision, scalability, resilience, reaction and execution durations, and robustness.

Based on their analysis of the structural vulnerability of smart grids, Luo et al. [8] investigated resilient protection strategies for FDIAs. It achieves this by utilizing cybernetic and graph-based methods. By avoiding traditional bad data detection methods, a well-planned hack called FDIA can wreak havoc on smart grids. Enhance smart grids' inherent security flaws by implementing a solid defense control strategy based on concealed virtual networks. Preventing FDIAs will be easier with this. A local consensus dynamic model with reduced dimensions is derived using the Kron reduction approach as the first stage. Second, by constructing and connecting a virtual hidden network based on graph theory, we can indirectly increase the smart grid's structural vulnerability. Using a competitive connectivity strategy based on the network zero-sum game further enhances the smart grid's structural vulnerability. Improving the smart grid's resilience can be achieved by modifying the topology of the connection bipartite graph and the virtual hidden network. Third, the author demonstrated that while FDIAs are present or not, the virtual hidden network defense controller remains stable. The results show that the smart grid can effectively mitigate the effects of FDIAs, but that the steady-state operating point of the original grid stays the same after adding the virtual hidden network.

In order to improve billing, load monitoring, and energy management efficiency, the smart grid's advanced metering infrastructure (AMI) gathers more accurate data on power use through SMs. Unfortunately, some dishonest customers are able to hack their meters, which results in attempts at more complex evasion or the more prevalent type of power theft. The goal of employing EAs is to trick theft detection systems into believing that there is an attempt to illegally decrease power consumption. Because they use users' massive consumption data to train detection algorithms, existing approaches for detecting these attacks present privacy concerns. Bondok et al. [9] suggest federated learning (FL), a method for cross-client collaborative training, to solve privacy issues. A solid starting point would be to safeguard ML models from evasion attacks by utilizing adversarial training (AT). The vulnerability of conventional power theft classifiers conditioned on FL to EAs for Non-IID and Independent and identically distributed (IID) consumption data is first examined in this research. Next, it assumes that all FL participants will behave responsibly and checks how well AT prevents EAs from compromising the global electricity theft detector. Distilation, No-Adversarial-Sample-Training, and False-Labeling were three additional attacks that the author introduced to make the global model susceptible to evasion during inference. It is most effective to conduct such an attack during the AT procedure.

Electricity theft detectors that are data-driven use the energy usage readings that consumers report to identify suspicious activity. The proper tagging of the training data is a typical implicit assumption in such detectors. Detectors like these are susceptible to data poisoning assaults, which use bogus labels to train the system. Takiddin et al. [10] proposed a model that shows the detectors based on shallow and deep learning that are vulnerable to data poisoning assaults, which can significantly reduce their detection rate by as much as 17%. In addition, compared to shallow detectors, deep detectors provide a performance boost of 12%. Despite data poisoning assaults, generalized detectors outperform customer-specific detectors by 4%. The author suggested a sequential ensemble detector that combines feed-forward neural networks, gated recurrent units (GRUs), and a deep auto-encoder with attention (AEA) to make the detectors more resistant to data poisoning attacks.

3. PROPOSED MODEL

Significant societal shifts are being prompted by Cyber Physical Systems (CPSs). The current critical infrastructures rely on CPS, which consists of computing, communication, and physical systems and processes, to integrate and coordinate many components. These components are becoming more intelligent, interactive, and dispersed [28]. As one of the most intricate CPSs ever constructed, the smart grid is undergoing these changes as it continues to integrate power and energy systems with ICTs. Not alone will the energy industry feel the effects of these basic infrastructure changes, but so will a slew of other vital, interrelated industries. Power, energy, control, sensing, computation, and communication are all interconnected parts of the smart grid [29]. There are possible threats to the security and resilience of this architecture due to its complexity and heterogeneity. To begin with, safeguarding bulk power systems from their inherent physical vulnerabilities is becoming more difficult due to their interconnectedness. However, cyber-integration necessitates heavy expenditure on security architecture modifications to ward against cyberspace's unpredictable patterns and threats. Together, physical and cyber security researchers have made great strides, creating a new field of smart grid cyber physical (CP) security.

Investigating intricate attack plans is a key and main concern of CP security. Malicious actors can use cyberspace's data and computing power to devise elaborate plans to exploit smart grid vulnerabilities, both those that are already known and those that are entirely unknown. When compared to more established forms of network security, such as those for power systems and communications, CP security is quite new. But previous research has shown certain disastrous outcomes for which the public, businesses, and government are woefully unprepared. The foundations for thorough defensive strategies and emergency actions for the vital electrical power grid are being laid by the vulnerability and resilience assessments against CP attacks [30].

In order to analyze the impact of cyber attacks and take precautions against them, further study is needed in the field of power system analysis that links FDI attacks with system stability. This research examines the power system's physical properties and establishes a connection between FDI attacks and system stability metrics. Operators can better manage power distribution on a bigger scale with the use of smart grids that have networks of sensors and generators that enable two-way communication inside the system with ICTs. Having said that, this functionality increase the power system's susceptibility to cyber attacks and FDI attacks. The primary goal of cyber assaults is to bring about complete system meltdown by causing extreme frequency passivity. One of the most critical components of power grids, Automatic Generation Control (AGC) is also one of the most susceptible to cyber assaults. In order to keep the system's frequency within a safe range, AGC modifies the output of the generators. Damage to the system can occur if the frequency excursion induced by cyber attacks exceeds this safe range. Developing effective algorithms to identify various cyber attacks in real time is tough due to the high cost and time required to manually gather and label sensing data for each attack type.

Power distribution systems and communication networks are the two main components of the smart grid. Devices are able to communicate with one another over the communication network. The proliferation of computer connections in the communication network has introduced a host of new security risks. In particular, the AMI network and physical security are of the utmost importance because of the AMI's central role in smart grid security. Deploying malicious attack detection system in the smart grid is more difficult than in other contexts due to the serious consequences for system security and the associated economic fallout in the event of an attack or failure. Ensuring seamless and dependable power transfer and usage data is a key component of the smart grid, which also involves addressing security restrictions in the power system network, sensor networks, and the complex process of communication between utilities and consumers. However, issues with data availability, integrity, and connectivity pose security risks to the system, of which the sensor network is a component. In addition, being a CPS, the power system can be physically affected by such smart grid incursions as a big blackout, loss of control, or system collapse if they are not detected. To improve predictions based on information-extensive data exemplars with no human interventions relying on learned behavior, and to enhance the process of computers self-learning and self-configuring from data patterns. The proposed model framework is shown in Figure 3.

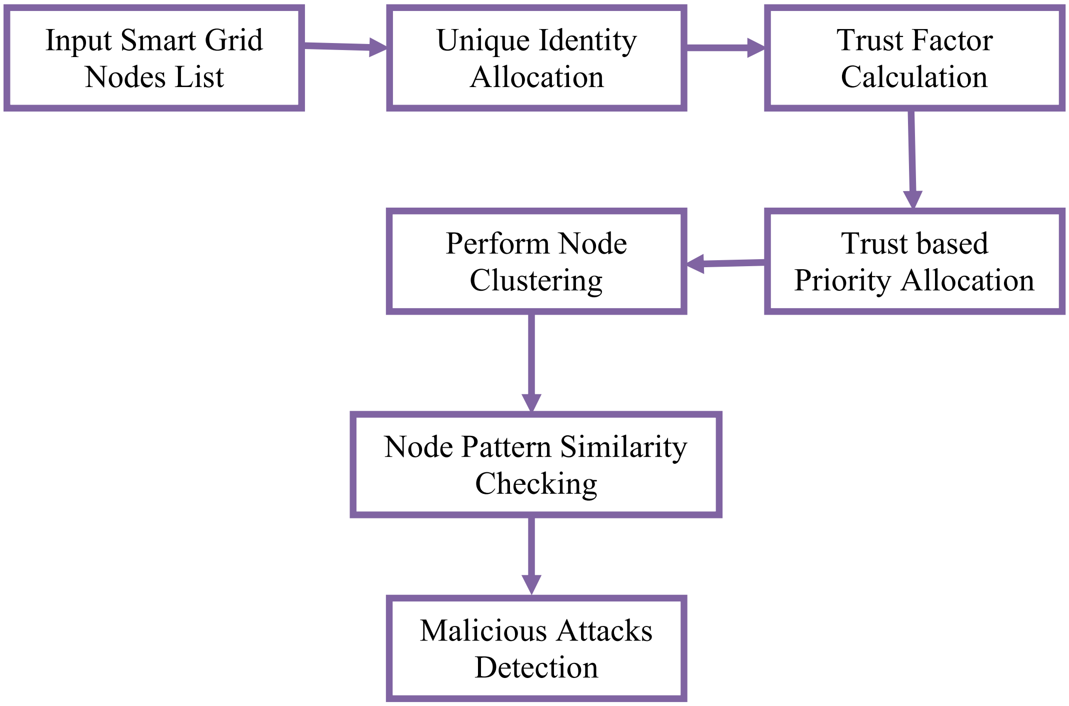
Input Smart Grid Nodes List
Unique Identity Allocation
Trust Factor Calculation
Trust based Priority Allocation
Perform Node Clustering
Node Pattern Similarity Checking
Malicious Attacks Detection

Fig 3: Proposed Model Framework

By making use of some novel structure, the smart grid outperforms the current matrix in terms of productivity. In order to improve the two-way flow of energy, sensors, smart meters, control relays, phases, or measurement units were typically introduced. In a typical scenario, customers can use their own optimum algorithms to purchase the most cost-effective power. They can even generate their own power and sell it to the smart grid. Similarly, smart grids allow energy providers to always know about power requests, allowing them to continuously assist their clients. This concept has several effects on the power distribution mechanism, even if it has greatly increased the smart grid's execution rate. The introduction of several new complicated devices at various locations has led to concerns that these devices might serve as vulnerabilities that could be exploited to inject malware and disrupt the normal functioning of smart grid, posing a serious threat to intelligent networks. To avoid malicious actions in the SGs, this research proposes a Trust Priority based Clustering model to detect and avoid Malicious Attacks for secure data transmission and increasing the quality of service levels in smart grids.

Table 1: Notations

Notation	Description
sgn	Smart grid node
$getnodeaddr$	Model to retrieve node address
$getattr$	Model to retrieve values
$getVal$	Retrieves node attaributes
$SGNset$	Smart Grid Node set
$Ninf$	Node Information
$UnqID$	Unique ID
$dist$	Distance among nodes
$Tfac$	Trust Factor
$SGNclus$	Smart Grid Node Cluster
Tpr	Trust Priority Allocation
$PtrnAnaly$	Node Pattern Pattern Analysis
$MNset$	Malicious Node Set
M	Total nodes in smart grid
$Simm$	Model to identify similarity levels
δ	Model to calculate distance among the nodes
τ	Transmission Range
μ	Node Energy

Algorithm TPbCMA

{

Input: Smart Grid Nodes List {SGNset}

Output: Malicious Nodes List {MNset}

Step-1: *The nodes in the smart grid list is considered as input and each node information is processed and a unique identity is allocated to each node for node recognition and for further communication. This unique ID is allocated to each node that is generated as*

$$Ninf[M] = \sum_{sgn=1}^{M} getnodeaddr(sgn) + \mu(sgn) + \tau(sgn)\ where\ \ sgn \in SGNset$$

$$UnqID[M = \sum_{sgn=1}^{M} getattr(Ninf(sgn) + max(\tau(sgn)) + max(\mu(sgn)) + getVal(sgn)$$

Here μ is the energy level of a node in SG and τ is the range of transmission of a SG node. Getnodeaddr() model considers each node address to generate unique ID, sgn represents the smart grid node and getVal() model considers smart grid node attributes.

Step-2: *The proposed model considers the trust factor of each node in the smart grid. The nodes that are authenticated with the unique ID are allotted with a trust factor. The trust factor is calculated based on the nodes performance. The trust factor calculation is performed as*

$$dist(SGNset[M]) = \sum_{sgn=1}^{M} \frac{\delta(UnqID(sgn), UnqID(sgn+1))}{M-(sgn+(sgn+1))}$$

$$Tf[M] = \prod_{sgn=1}^{M} \frac{getUnqID(sgn)}{M} + maxrange(\mu(sgn)) + max(\tau(sgn)) + min\,(dist(sgn, sgn+1))$$

$$Tfac[M] = \prod_{sgn=1}^{M} max\,(Tf(sgn)) \begin{cases} Tfac \leftarrow setVal(Tf(sgn)) \\ Tfac \leftarrow 0 & Otherwise \end{cases}$$

Here δ model is used to consider the distance among the adjacent nodes in SG. UnqID() model considers the unique identity value generated for each sgn, maxrange() model considers the maximum value of nodes in the allocated range, and dist() model considers the distance among the nodes.

Step-3: *To all the nodes that has a trust factor, priority allocation is performed. Priority is allotted to the nodes that has highest trust factor. The priority allocation helps to consider the nodes for transmission in smart grid. The priority allocation based on trust factor is performed as*

$$Tpr[M] = \sum_{sgn=1}^{M} max(Tfac(sgn)) + \lim_{sgn \to SGNset} \left(maxrange(Tf(sgn)) + \frac{min\,(dist(sgn, sgn+1))}{M} \right)^{2}$$

The maximum trust factor is considered for priority allocation and minimum distance nodes are allocated with highest priority.

Step-4: *Nodes in the smart grid are allocated with priorities and based on the trust factor priorities, the node clustering is performed. Nodes having priority and trust similarities are grouped as a cluster for monitoring the malicious actions. The node clustering is performed as*

$$SGNclus[M] = \prod_{sgn=1}^{M} \sqrt{\frac{max(Tpr(sgn)) + min\,(dist(sgn))}{M} + simm(Tpr(sgn, sgn+1))}$$

The simm() model performs the similarity checking among the two adjacent smart grid nodes that have trust factors. The nodes that have maximum trust factor, minimum distance and similar in trust factor are grouped as a cluster.

Step-5: *Each node pattern analysis is performed to identify the malicious actions in the smart grid. The pattern dissimilarities are used to identify the malicious actions at nodes. The pattern analysis is performed and the nodes causing malicious actions and attacking the smart grid is listed as*

$$PtrnAnaly[M] = \prod_{sgn=1}^{M} getUID\left(SGNclus(sgn)\right) + diff\left(Tpr(sgn, sgn+1)\right) + simm\left(SGNclus(sgn, sgn+1)\right) + simm\left(Tfac(sgn, sgn+1)\right)$$

$$MNset[M] = \sum_{sgn=1}^{M} diff\left(PtrnAnaly(sgn)\right) + diff\left(Tpr(sgn, sgn+1)\right) + diff\left(Tfac(sgn, sg+1)\right) + \min\left(\mu(sgn)\right)$$

The pattern analysis is performed by considering the user ID, and the difference levels in the adjacent node properties and similarity levels in the cluster group. The trust factor similarity is also considered in pattern analysis. The malicious nodes are identified as the nodes that has differences in the data patterns, differences in trust factors and having high energy consumption.

}

4. RESULTS

The smart grid's novel two-way, real-time (RT) communications are made possible by the AMI systems, which include millions of smart meters in distribution systems. These technologies encourage various advantages from energy management, consumer interaction, and demand response. Electricity generation, transmission, and distribution are also undergoing continuous change due to new technologies such as energy storage and electric vehicles. Along with the PSs, the cyber infrastructure that the smart grid's information, computation, and communication technologies have produced is pervasive and interwoven. Measurements and instructions are continuously generated and transmitted between internet and PSs. The majority of the measurements made by PSs are digital data, which measures system dynamics, and status data, which includes the topological connectedness of power grid components. The measurements that determine the relevant control policies are used by operators to issue control instructions that coordinate the actuators in the PSs. To help with the localization, evaluation, mitigation, and restoration of faults or disturbances, extra recording devices capture diagnostic logs during emergencies.

Recent developments in intelligent electronic devices and programmable logic circuits have made the smart grid more reliant on distributed and localized computations. These advancements strive to make the grid more efficient, resilient, and flexible. Despite the numerous benefits, there is a significant rise in the surface area for cyber-attacks when power grids are transformed into smart cyber-physical systems. Consequently, a solution is necessary. Problematically, data-driven defenses against cyber-attacks, validation, and testing procedures lack essential information derived from real cyber-occurrences. Machine learning-based detection methods are part of this category. As opposed to attack data derived from real cyber occurrences, infrastructure standards and expertise can be accessible through expert and topic knowledge. The proposed approach uses domain knowledge to describe a smart grid's behavior when assaults are not present, in order to detect attack patterns and anomalies. An analysis of malicious attacks on electrical systems is conducted in which an attacker gains control of a cluster of meters and manipulates their results. Under the strong attack regime, the enemy hits enough meters that the control center loses all visibility into the network's status. Here, the graph-theoretic approach is employed to define the bare minimum of attacked meters that could lead to unobservability in the network. The issue of finding the minimum set of susceptible meters is shown to have polynomial complexity when reformulated as a reduction of a supermodular graph functional. To avoid malicious actions in the SGs, this research proposes a Trust Priority based Clustering model to detect and avoid Malicious Attacks (TPbCMA) for secure data transmission and increasing the quality of service levels in smart grids. The proposed model is compared with the traditional False Data Injection Attacks Detection in Smart Grid: A Structural Sparse Matrix Separation Method (FDIA-SSMS) and FDI Attack Detection at the Edge of Smart Grids Based on Classification of Predicted Residuals (CPRs) model.

The proposed model identifies malicious actions in the network by identifying pattern dissimilarities at each node level. Each node is allocated with a unique identity value that is used for future communication. The Node Identity Allocation Accuracy Levels are shown in Table 1 and Figure 4.

Table 1: Node Identity Allocation Accuracy Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	97.9	94.6	92.8
100	98	94.8	93.1
150	98.2	95	93.5
200	98.5	95.2	93.8
250	98.6	95.5	94
300	98.8	95.6	94.3

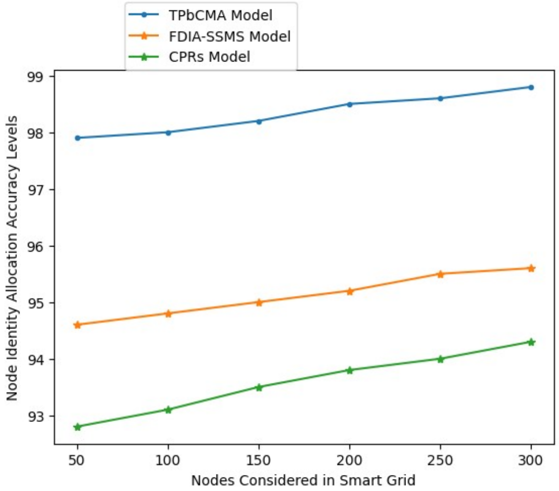

Fig 4: Node Identity Allocation Accuracy Levels

The proposed model considers the trust factor of the smart grid nodes in the network. The trust factor is calculated based on the node performance levels and energy consumption. The trust factor represents the genuine levels of each node to consider them in communication. The Trust Factor Calculation Accuracy Levels are indicated in Table 2 and Figure 5.

Table 2: Trust Factor Calculation Accuracy Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	13.2	17.3	20.3
100	13.5	17.6	20.5
150	13.7	17.9	20.8
200	14	18	21.1
250	14.2	18.2	21.3
300	14.5	18.4	21.6

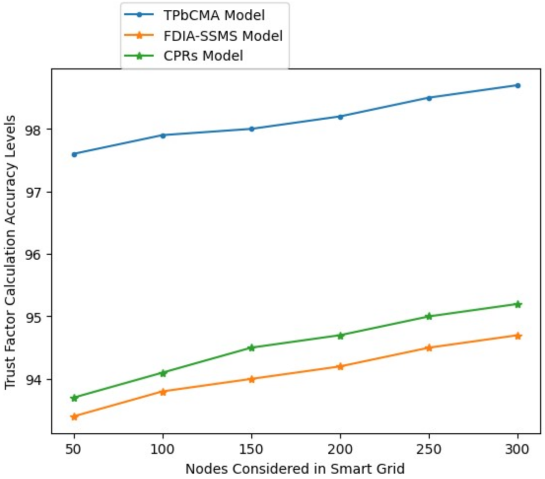

Fig 5: Trust Factor Calculation Accuracy Levels

The nodes that has best performance levels will be allocated with the trust values. The priorities are allocated to the nodes based on the trust levels. The nodes with highest trust levels are considered to be high priority nodes. The Trust based Priority Allocation Time Levels are indicated in Table 3 and Figure 6.

Table 3: Trust based Priority Allocation Time Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	97.6	93.4	93.7
100	97.9	93.8	94.1
150	98	94	94.5
200	98.2	94.2	94.7
250	98.5	94.5	95
300	98.7	94.7	95.2

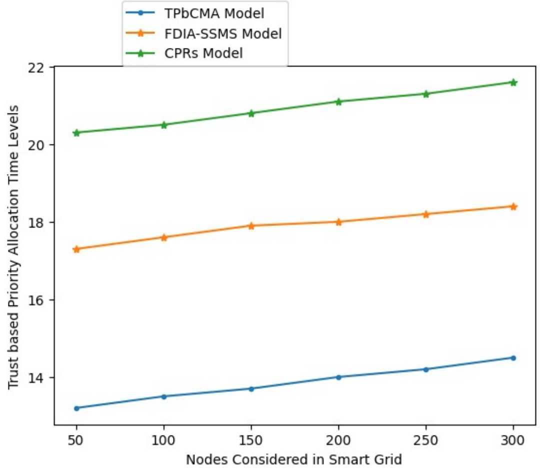

Fig 6: Trust based Priority Allocation Time Levels

The node clustering is performed that groups nodes with high trust factor as a single unit to involve in communication. The node clustering helps to identify the trusted and non trusted nodes. The Table 4 and Figure 7 represents the Node Clustering Accuracy Levels.

Table 4: Node Clustering Accuracy Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	97.7	93.2	92.6
100	98	93.5	92.8
150	98.2	93.8	93
200	98.3	94	93.2
250	98.5	94.2	93.4
300	98.7	94.3	93.7

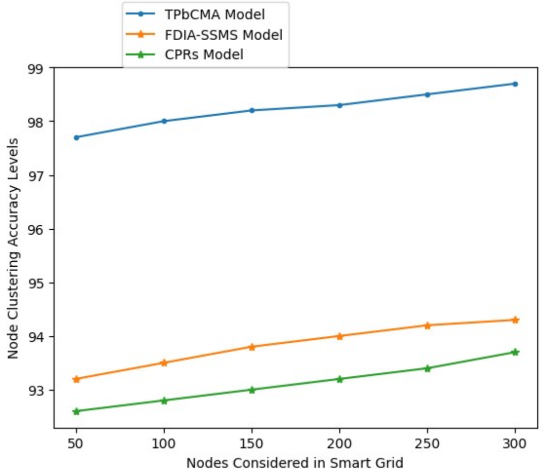

Fig 7: Node Clustering Accuracy Levels

The trusted nodes are considered and involved in data transmission. The node patterns are frequently analyzed and the similarity levels and dissimilarity levels are considered for detection of malicious actions in the smart grid. The Node Pattern Analysis Accuracy Levels are indicated in Table 5 and Figure 8.

Table 5: Node Pattern Analysis Accuracy Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	98.1	94.3	92.7
100	98.3	94.8	92.9
150	98.5	95	93
200	98.7	95.2	93.2
250	99	95.3	93.4
300	99.2	95.4	93.6

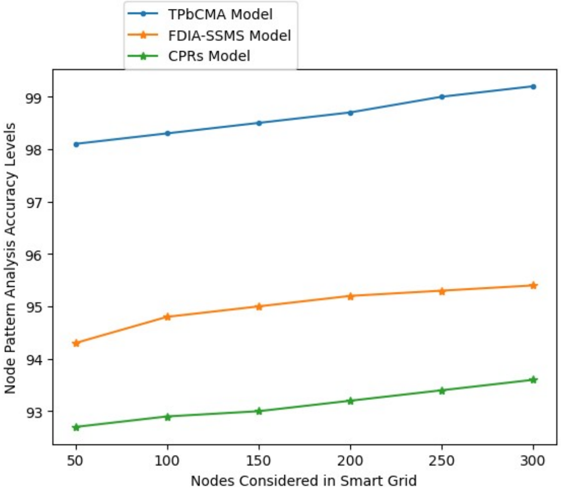

Fig 8: Node Pattern Analysis Accuracy Levels

The proposed model effectively detects the malicious attacks in the smart grid. The node patterns are monitored frequently and the malicious attacks are detected and nodes causing malicious attacks are listed to label them so such nodes will nor be used in smart grid communications. The Malicious Action Detection Accuracy Levels are shown in the Figure 9 and Table 6.

Table 6: Malicious Action Detection Accuracy Levels

Nodes Considered in Smart Grid	Models Considered		
	TPbCMA Model	FDIA-SSMS Model	CPRs Model
50	98.3	93.4	91.7
100	98.4	93.6	92
150	98.6	93.9	92.2
200	98.7	94	92.4
250	99	94.2	92.5
300	99.1	94.5	92.7

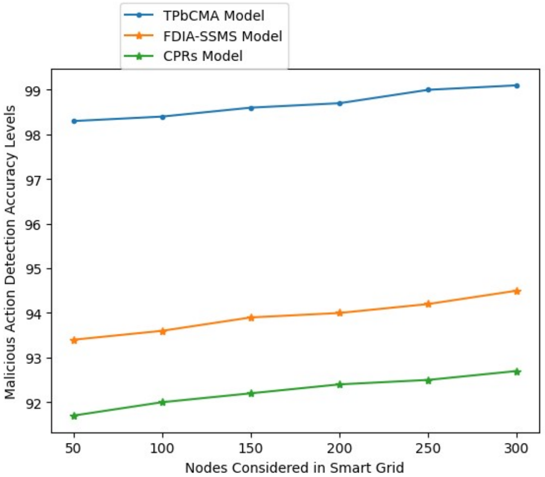

Fig 9: Malicious Action Detection Accuracy Levels

5. CONCLUSION

An adversary controls a set of meters and can modify the measurements from those meters; malicious attacks against smart grids are researched in this context. When an attacker hits enough meters in a powerful attack regime, the control center is unable to see the network's status. When it comes to smart grid attack detection, the challenges lie in statistical learning for various assault scenarios with batch or online measurements. This method uses machine learning techniques to classify measurements as either secure or attacked. The sparse structure of the problem can be circumvented and all system knowledge can be utilized with the help of an attack detection framework. Due to the increased reliance on communication technologies and procedures, grid operation is becoming increasingly vulnerable to cyber-attacks and breakdowns as a result of the widespread use of ICTs. Cyberattacks pose a new threat to smart grid and ICS process networks. The major characteristics of this environment are assets with a lengthy lifespan and the use of outdated components with inadequate security protocols. To protect critical security objectives like availability, secrecy, and integrity, as well as to stave off new dangers like cyber assaults, proactive or reactive cyber security remedies are required. The information and communication technology that make up the backbone of the Smart Grid Network is vulnerable to malicious attacks. Identifying and fixing the attack is critical for a reliable and effective energy supply and for producing an accurate bill. In light of power grids transitioning to SGs, countermeasures against sophisticated cyberattacks that depend on reliable detection methods are important. For safe data transfer and improved service quality in smart grids, this study suggests a Trust Priority based Clustering model to identify and prevent malicious attacks in SGs. The proposed model efficiently detects the attacks in the smart grids to maintain quality of service levels. The proposed model achieved 98.7% accuracy in Node Clustering and 99.1% accuracy in Malicious Action Detection. In future, meta-heuristic optimization techniques can be applied for the better dynamic attack detection models. Feature dimensionality reduction models can be applied in future for selecting the most relevant features to detect the dynamic attacks for improving the security in smart grids.

Compliance with Ethical Standards

Authors' contributions

The author CH.Naga Priyanka developed the abstract, introduction, literature survey and proposed model and author Nandhakumar evaluated the results and concluded the manuscript.

Acknowledgements

The author is thank to the supervisor Nandhakumar for his continuous support in completing the manuscript.

Conflict of Interest: The authors declare that they have no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability: The data can be made available on request.

Funding

There is no funding source for this research manuscript.

REFERENCES

[1] D. An, F. Zhang, Q. Yang and C. Zhang, "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures," in IEEE Transactions on Automation Science and Engineering, vol. 19, no. 3, pp. 1631-1644, July 2022, doi: 10.1109/TASE.2022.3149764.

[2] K. Huang, Z. Xiang, W. Deng, C. Yang and Z. Wang, "False Data Injection Attacks Detection in Smart Grid: A Structural Sparse Matrix Separation Method," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2545-2558, 1 July-Sept. 2021, doi: 10.1109/TNSE.2021.3098738.

[3] H. Pang, K. He, Y. Fu, J. -N. Liu, X. Liu and W. Tan, "Enabling Efficient and Malicious Secure Data Aggregation in Smart Grid With False Data Detection," in IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 2203-2213, March 2024, doi: 10.1109/TSG.2023.3316730.

[4] J. -J. Yan, G. -H. Yang and Y. Wang, "Dynamic Reduced-Order Observer-Based Detection of False Data Injection Attacks With Application to Smart Grid Systems," in IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 6712-6722, Oct. 2022, doi: 10.1109/TII.2022.3144445.

[5] W. Lei, Z. Pang, H. Wen, W. Hou and W. Han, "FDI Attack Detection at the Edge of Smart Grids Based on Classification of Predicted Residuals," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9302-9311, Dec. 2022, doi: 10.1109/TII.2022.3174159.

[6] V. Havlena, P. Matoušek, O. Ryšavý and L. Holík, "Accurate Automata-Based Detection of Cyber Threats in Smart Grid Communication," in IEEE Transactions on Smart Grid, vol. 14, no. 3, pp. 2352-2366, May 2023, doi: 10.1109/TSG.2022.3216726.

[7] N. Saxena, L. Xiong, V. Chukwuka and S. Grijalva, "Impact Evaluation of Malicious Control Commands in Cyber-Physical Smart Grids," in IEEE Transactions on Sustainable Computing, vol. 6, no. 2, pp. 208-220, 1 April-June 2021, doi: 10.1109/TSUSC.2018.2879670.

[8] X. Luo, J. He, X. Wang, Y. Zhang and X. Guan, "Resilient Defense of False Data Injection Attacks in Smart Grids via Virtual Hidden Networks," in IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6474-6490, 1 April1, 2023, doi: 10.1109/JIOT.2022.3227059.

[9] A.H. Bondok, M. Mahmoud, M. M. Badr, M. M. Fouda, M. Abdallah and M. Alsabaan, "Novel Evasion Attacks Against Adversarial Training Defense for Smart Grid Federated Learning," in IEEE Access, vol. 11, pp. 112953-112972, 2023, doi: 10.1109/ACCESS.2023.3323617.

[10] Takiddin, M. Ismail, U. Zafar and E. Serpedin, "Robust Electricity Theft Detection Against Data Poisoning Attacks in Smart Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2675-2684, May 2021, doi: 10.1109/TSG.2020.3047864.

[11] D. J. Miller, Z. Xiang and G. Kesidis, "Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks", *Proc. IEEE*, vol. 108, no. 3, pp. 402-433, Mar. 2020.

[12] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang and Y. Lu, "Automated labeling and learning for physical layer authentication against clone node and Sybil attacks in industrial wireless edge networks", *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 2041-2051, Mar. 2021.

[13] W. Xue and T. Wu, "Active learning-based XGBoost for cyber physical system against generic ac false data injection attacks", *IEEE Access*, vol. 8, pp. 144575-144584, 2020.

[14] A. Mustafa and H. Modares, "Attack analysis and resilient control design for discrete-time distributed multi-agent systems", *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 369-376, Apr. 2020.

[15] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber and O. A. Mohammed, "CPS attacks mitigation approaches on power electronic systems with security challenges

for smart grid applications: A review", *IEEE Access*, vol. 9, pp. 38571-38601, 2021.

[16] S. Tufail, I. Parvez, S. Batool and A. Sarwat, "A survey on cybersecurity challenges detection and mitigation techniques for the smart grid", *Energies*, vol. 14, no. 18, pp. 5894, 2021.

[17] Y. Zhang, J. Wang and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach", *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623-634, Jan. 2021.

[18] S. Roy, J. Li, B.-J. Choi and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks", *Future Gener. Comput. Syst.*, vol. 127, pp. 276-285, Feb. 2022.

[19] L. Yang, Y. Zhai and Z. Li, "Deep learning for online AC false data injection attack detection in smart grids: An approach using LSTM-autoencoder", *J. Netw. Comput. Appl.*, vol. 193, Nov. 2021.

[20] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao and M. Chen, " FDA 3 : Federated defense against adversarial attacks for cloud-based IIoT applications ", *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7830-7838, Nov. 2021.

[21] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao and M. Chen, " FDA 3 : Federated defense against adversarial attacks for cloud-based IIoT applications ", *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7830-7838, Nov. 2021.

[22] Y. Wang, I. L. Bennani, X. Liu, M. Sun and Y. Zhou, "Electricity consumer characteristics identification: A federated learning approach", *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3637-3647, Jul. 2021.

[23] M. M. Ashraf, M. Waqas, G. Abbas, T. Baker, Z. H. Abbas and H. Alasmary, "FedDP: A privacy-protecting theft detection scheme in smart grids using federated learning", *Energies*, vol. 15, no. 17, pp. 6241, Aug. 2022.

[24] J. Jithish, B. Alangot, N. Mahalingam and K. S. Yeo, "Distributed anomaly detection in smart grids: A federated learning-based approach", *IEEE Access*, vol. 11, pp. 7157-7179, 2023.

[25] J. Cao, Z. Bu, Y. Wang, H. Yang, J. Jiang and H.-J Li, "Detecting prosumer-community groups in smart grids from the multiagent perspective", *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 49, no. 8, pp. 1652-1664, Aug. 2019.

[26] F. H. Guo, L. Wang, C. Y. Wen, D. Zhang and Q. W. Xu, "Distributed voltage restoration and current sharing control in islanded DC microgrid systems without continuous communication", *IEEE Trans. Ind. Electron.*, vol. 67, no. 4, pp. 3043-3053, Apr. 2020.

[27] Q. Sun, K. W. Zhang and Y. Shi, "Resilient model predictive control of cyber-physical systems under DoS attacks", *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4920-4927, Jul. 2020.

[28] J. J. Yan and G. H. Yang, "Adaptive fault estimation for cyber-physical systems with intermittent DoS attacks", *Inf. Sci.*, vol. 547, pp. 746-762, 2021.

[29] A. S. Musleh, G. Chen and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids", *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218-2234, May 2020.

[30] S. Sahoo, J. Chih-Hsien, A. Peng, S. Devakumar Mishra and T. Dragičević, "On detection of false data in cooperative DC microgrids: A discordant element approach", *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562-6571, Aug. 2020.