Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Novel Approach For Enhancing Cyber Physical System Security And Attack Detection Techniques In Smart Grid System

S. Simonthomas[1*], Dr. R. Subramanian[2], Dr. S. Balakrishnan[3]

*[*1]Research Scholar, [#2]Professor, [#3]Professor*
Department of Computer Science
School of Engineering and Technology
Pondicherry University, Puducherry, India
[#3]Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation (DU), Chennai, Tamil Nadu, India
Email- simonthomas078@pondiuni.ac.in

Smart grid systems represent a crucial advancement in modernizing energy distribution infrastructure, offering improved reliability, efficiency, and sustainability in power dissemination. However, with escalated connectivity and integration of information technologies, they become more susceptible to cyber threats and attacks the smart grid becomes precarious to the cyber-attacks, causing substantial threats to its operation and protection. In this paper, it explores the innovative approaches to improving the protection of Cyber-Physical Systems (CPS) within smart grids by focusing on advanced attack detection techniques in Networked Control Systems (NCS). Smart grids, as an essential CPS, rely heavily on real-time data exchange between sensors, controllers, and actuators, making them vulnerable to various forms of cyber-attacks encompass False Data Injection (FDI), Denial of Service (DoS), and Man-in-the-Middle (MitM) attacks. This introduce novel security mechanisms, including state estimation, anomaly detection, and robust management approaches, designed to reduce the consequences of these attacks and maintain system stability. This approach leverages kalman filters for robust state estimation, along with machine learning-based behavior identification to identify abnormal behavior in real-time. The proposed envisioned techniques are evaluated through simulations, demonstrating their effectiveness in improving the resilience of smart grid systems under various cyber-attack scenarios. The implementation is examined with IEEE 39-bus system, demonstrating the impact of these methods in recognizing and alleviating cyber intrusions while ensuring system stability. This research supports to the development of more secure, reliable, and adaptive smart grid infrastructures by enhancing both detection capabilities and strategies for system recovery amid the rising sophistication of cyber threats.

Keywords: Smart grids security, Cyber-attack detection, Cyber-physical system Security, Machine learning techniques, Kalman predictor.

1. INTRODUCTION

The deployment of smart grid technologies has transformed conventional power grid infrastructure, promising enhanced efficiency, reliability, and sustainability [1]. Smart grids that utilize cutting-edge communication, control, and monitoring technologies to maximize electricity dissemination, integrate renewable energy sources, and facilitate real-time data analysis for more knowledge-based decision-making [2]. However, this enhancing network access and trust on digital infrastructures also expose smart grids to a myriad of cybersecurity threats, presenting considerable threats to the safety and dependability of energy distributed system [3]. Cyber-attacks targeting smart grids possess the capacity to disrupt workflows and expose confidential data and even cause widespread power outages with far-reaching consequences for both individuals and critical infrastructures [4]. The unique characteristics of smart grids, such as the incorporation of dispersed energy resources, the proliferation of IoT devices, and the reliance on complex communication networks, introduce new attack vectors and amplify the impact of cyber threats [5]. In light of these challenges, effective cyber-attack detection mechanisms are essential for safeguarding smart grid infrastructures against malicious activities [6]. Detection techniques play a crucial role in identifying anomalous behaviours, malicious intrusions, and potential security breaches in real-time, enabling timely response and mitigation strategies to reduce the impact of cyber threats [7].

This research paper presents, comprehensive summary of cyber-attack identification techniques in smart grids, aiming to analyse the current cutting-edge methodologies, identify key issues and challenges, and outline prospective research directions in this critical area of cybersecurity. By synthesizing existing literature, categorizing detection approaches, and evaluating their strengths and limitations [3], this paper seeks to offer insights into the development of robust and resilient cybersecurity frameworks adapted for the specific requirements of smart grid environments [8]. Throughout the paper, can explore diverse categories of cyber threats facing smart grids, ranging from common attacks including anomalies, malware infections and denial-of-service (DoS) [5] attacks to sophisticated intrusions like advanced persistent threats (APTs) [6] and insider attacks. This also discuss the inherent challenges associated with cyber-attack identification in smart grids, including the scale and complexity of networked systems, resource constraints, and the dynamic nature of evolving cyber threats [9]. Furthermore, this survey paper categorizes and analyses different detection techniques employed in smart grids, including anomaly-based detection [10], state estimation [11], signature-based detection [12], machine learning-based detection [13], and hybrid approaches [14]. By examining the strengths, limitations, and practical considerations of each technique, aim is to furnish researchers, experts, practitioners, and policymakers with thorough understanding perception of the available options for recognizing and controlling digital risks in smart grid environments [12]. The effective detection of cyber-attacks is crucial for preserving the security, reliability, and resilience of smart grid infrastructures. By advancing the cutting-edge in cyber-attack mitigation techniques and addressing the unique challenges posed by smart grid environments, that can facilitate the development of enhanced security and sustainable energy evolution [15]. The history of cyberattacks on smart grids and the resulting blackouts involves highlighting some of the notable incidents that have occurred over the years. Table. 1. provides a snapshot of these events, focusing on the nature of the attack, the impact it had, and the lessons learned [16].

Table. 1. History of Attacks in power sector.

Year	Location	Type of Attack	Impact	Lessons Learned
2003	North America	Software Bug (Not a cyber-attack but significant for grid security)	Widespread blackout affecting 50 million people	Highlighted the need for robust grid management and cybersecurity measures
2010	Iran	Stuxnet Worm	Targeted Iran's nuclear facilities but raised worldwide alarm on critical infrastructure security	Demonstrated the potential of malware to physically damage equipment
2015	Ukraine	Phishing & Malware	First successful cyberattack on a power grid, left 230,000 residents without power	Underlined the importance of cybersecurity training and the vulnerability of infrastructure to cyberattacks
2016	Ukraine	Malware Attack	Second blackout caused by a cyberattack, affecting one-fifth of Kyiv's power consumption	Showed that attackers learn and adapt, emphasizing the need for dynamic cybersecurity defenses
2017	Saudi Arabia	Triton Malware	Targeted safety systems at a petrochemical plant, could have caused massive harm	Revealed the risks to industrial control systems and the potential for catastrophic incidents
2019	USA and others	Ransomware	Disruptions and financial losses.	Stressed the need for comprehensive cybersecurity strategies and backup systems.
2020	Israel	Cyberattack on water systems	Attempted contamination of water supply.	Highlighted the interconnectedness of different types of infrastructure and the need for holistic security measures.
Various	Global	Espionage and malware targeting infrastructure	Continuous threat to infrastructure.	Emphasized the ongoing characteristics of cyber threats necessitate ongoing vigilance and the ability to adapt continuously.

These incidents emphasize the dynamic characteristics of cyber threats against the adoption of smart grids and the critical significance of enhancing security protocols designed to safeguard energy infrastructure. They also highlight the shift from theoretical vulnerabilities to actual incidents, demonstrating the real-world consequences of successful cyber-attacks [17][18]. It is learned from each incident have contributed to the development of more sophisticated security protocols, better incident response strategies, and a greater emphasis on resilience and recovery planning in the power industry.

1.1 Smart Grid Overview

The modernization of conventional electrical grid into smart grids represents a revolutionary transition in how electrical energy is produced, transmitted, distributed, and utilized. The smart grids incorporate innovative communication, control, and monitoring techniques to optimize the effectiveness, reliability, and environmental compatibility of energy transmission systems [13]. This transformation enables dynamic management of energy resources, facilitates the adoption of sustainable energy sources, and empowers users with enhanced insight and oversight of electricity consumption. The essence of smart grid is an intelligent framework of interconnected devices, incorporating sensors, smart meters, actuators, and control systems, deployed across various points in the power grid infrastructure [16]. These devices communicate with one another as well as with a central control center, transmitting real-time data and facilitating coordinated actions to assure optimal functioning of the grid.

Core elements of smart grids:

Advanced Metering Infrastructure (AMI) [15]: Smart meters serve as the cornerstone of AMI, providing Bidirectional communication between service providers and end-users. Smart meters gather detailed information on energy consumption patterns, enable remote meter reading, and support dynamic pricing mechanisms to encourage demand response.

Distribution Automation [16]: Distribution automation technologies enrich the dependability and effectiveness of power distribution systems through the automation of fault detection, isolation, and restoration procedures. The detection instruments and surveillance apparatus spread out across the distribution grid enable rapid detection of abnormalities and enable self-healing capabilities to minimize service disruptions.

Renewable Energy Integration [17]: Smart grids facilitate the smooth incorporation of sustainable energy sources like solar photovoltaic (PV) systems, wind turbines, and assimilation of battery storage into the electrical grid. The cutting-edge control algorithms and forecasting techniques optimize the utilization of intermittent renewable assets while managing grid control stability, consistency and reliability.

Distributed Energy Resources (DERs) [19]: The incorporation of renewable energy sources, improvement of grid resilience, and support for decentralised power generation and management, localized energy resources (DERs), including solar panels, wind turbines, and energy storage systems, are indispensable pieces of smart grid ecosystems.

Grid-Connected Devices [20]: The propagation of Internet of Things (IoT) devices, including sensors, actuators, and transmission modules, enables seamless connectivity and data exchange across the grid infrastructure. These devices facilitate grid monitoring, asset management, and control functions, but also introduce potential cybersecurity vulnerabilities.

Demand Response and Energy Management [21]: Smart grids empower users to engage proactively in energy management and participate in load management initiatives. The consumers can modify their patterns of electricity usage to better fit the needs of the grid, cut peak demand, and save overall energy expenditures by providing real-time feedback and incentives.

Cyber-Physical Systems (CPS) [12]: Cyber-physical systems form the backbone of smart grid infrastructure, integrating computational and physical components to oversee, regulate, and manage electricity generation, transmission, and distribution processes. Real-time monitoring of grid conditions is achievable via CPS., automated control of equipment, and coordination of decentralized power resources.

While smart grid provides diverse benefits, they also present new challenges and vulnerabilities, particularly in terms of cybersecurity. The interconnected aspect of smart grid components, reliance on digital communication networks, and integration of third-party devices increase the attack surface and expose critical infrastructure to cyber threats. Assuring the security, adaptability, and robustness of smart grids contrary to cyber-attacks is essential to maintain the stability, integrity and reliability of energy delivery systems [22]. Efficient cyber-attack detection mechanisms perform an essential function in identifying and mitigating threats, enabling proactive responses to security incidents and minimizing the impact on grid operations.

1.2 Importance of Cyber Attack Detection

The significance of cyber-attack identification in smart grids cannot be inflated, given the essential role that electricity plays in modern society. Smart grids, with their advanced communication and control technologies, offer significant improvements in the efficiency and reliability of electricity distribution [23]. However, these features also introduce vulnerabilities to cyber-attacks, which can have far-reaching consequences. Below are key reasons why cyber-attack detection being crucial in smart grids:

Ensuring Reliable Electricity Supply: Smart grids are crucial for managing and distributing electricity efficiently. Cyber-attacks targeting these systems may result in extensive power disruptions, disrupting essential services and daily life [24].

Protecting Critical Infrastructure: Electricity networks are considered critical national infrastructure. Their compromise can affect not just the energy sector but also other dependent regions such as healthcare, transportation, and water supply [25].

Maintaining System Integrity and Performance: Cyber-attacks can manipulate control signals and data, leading to inefficient grid operation, equipment damage, and increased operation costs. Detecting and mitigating these attacks help maintain optimal system performance [26].

Preventing Economic Losses: Significant economic losses can result from cyber-attacks on smart grids, including costs related to emergency response, system repairs, and loss of business for affected stakeholders [27].

Safeguarding Consumer Information: Smart grids collect detailed consumption data from consumers, which can be sensitive. Cyber-attacks could cause to unauthorized penetration and exploit misuse of this information, violating privacy and potentially leading to financial fraud [28].

Supporting the Incorporation of Renewable Energy: The smart grids perform a key influence in unifying renewable power resources into the power grid. Cyber-attacks could disrupt this integration, undermining efforts to transition to cleaner energy sources [21].

Enhancing National Security: The security of a nation's electricity supply can have direct implications for its security and geopolitical stance. Sustaining the adaptability, robustness of smart grids against cyber hazards is, therefore, a national security priority [29].

Adapting to Developing the Threat Landscapes: As technology improves, develop the sophistication and methods of cyber attackers. Continuous improvement in cyber-attack detection is essential for staying ahead of potential threats [22].

Compliance with Regulations and Standards: There are growing legal and regulatory requirements related to cybersecurity in the energy sector. Effective cyber-attack detection mechanisms are necessary to comply with these standards and avoid penalties [30].

Building Consumer Trust: Consumers expect their utilities to provide reliable and secure services. Demonstrating robust cyber-attack detection and response capabilities is critical for maintaining and building trust with consumers [31].

The cyber-attack identification is a cornerstone of smart grid security. It enables the proactive identification and mitigation of threats, ensuring the reliable, consistent, efficient, and secure functioning of modern electrical grids. As the smart grid evolves, so too will the strategies and technologies for defending against cyber threats, highlighting the ongoing need for innovation and vigilance in this area.

1.3 Objectives of the proposed system

The objectives of cyber-attack identification in smart grids revolve around safeguarding the infrastructure, ensuring the dependability and effectiveness of energy distribution, and protecting the data and privacy of consumers. Given the critical nature of electricity networks and their growing digitalization, these objectives become fundamental in preventing disruptions and securing the smooth operation of both the grid and the services that depend on it [32]. The primary objective is early detection of threats to identify potential cyber threats as soon as possible to minimize their impact. Early detection allows grid operators to implement countermeasures quickly, preventing attackers from achieving their goals and mitigating any potential damage [33]. Maintaining reliability and stability in cyber-attacks can disrupt the power supply, leading to outages or instabilities in the grid. Detecting attacks early

helps maintain the continuous and reliable delivery of electricity, ensuring that households, businesses, and critical services remain operational [34]. Protecting Infrastructure of a smart grid comprises various components, including hardware and software systems that control the generation, transmission, and distribution of power supply [35]. Protecting these assets from cyber threats is crucial to prevent physical damage, data breaches, and operational disruptions. Ensuring data integrity and privacy the smart grid generates and stores extensive quantities of information encompassing, sensitive information about consumer's energy consumption trends. Cyber-attack detection aims to preserve the data from unauthorized privilege, manipulation, or theft, ensuring its integrity and the privacy of the consumers [36].

The operators of smart grids are often subject to regulatory requirements that mandate specific cybersecurity measures, including robust attack detection capabilities. Meeting these requirements, it is essential not only for adhering to legal requirements but also for fostering public confidence in the energy system. A resilient smart grid can withstand, adapt to, and quickly recover from cyber-attacks. Detection is a key component of resilience, enabling the grid to engage to threats in real-time and maintain its essential functions even under attack [37]. Beyond the consumer protection of direct impact on grid operation, cyber-attacks can have serious consequences for consumers, including billing fraud, privacy breaches, and disruption of electricity-dependent services. Detecting and preventing these attacks protect consumers from financial loss and other harms. The cyber threat environment is persistently adapting with modern vulnerabilities and attack approaches that evolving periodically. An objective of cyber-attack detection is to adapt to these evolving threats, ensuring that the smart grid remains secure against both current and future challenges. Effective detection is the first step in responding to cyber incidents [38]. By identifying attacks promptly, operators can initiate their incident response protocols more effectively, mitigating the impact and facilitating a quicker recovery to normal operations. After an attack, understanding how the breach occurred and the extent of the damage is crucial for preventing future incidents. Detection systems can provide valuable data for forensic analysis, helping to improve security measures and support legal actions against perpetrators [39]. The objectives of cyber-attack identification in smart grids are to defend essential infrastructure from potential hazards, secure the consistent and proficient distribution of electricity, safeguard sensitive data, and comply with regulatory standards, all while adapting to the evolving cyber threat landscape [40].

2. CYBER THREATS TO SMART GRIDS

Cyber threats to smart grids are malicious attempts aimed at disrupting, damaging, or gaining unauthorized access to the digitalized infrastructure of electricity generation, transmission, and distribution networks. These threats exploit the vulnerabilities inherent in smart grids, which depend heavily on information and communication technologies (ICT) that operates more efficiently and reliably than traditional grids. The incorporation of these modern technologies, while beneficial for grid management and energy savings, also opens up new avenues for cyber-attacks [7][24]. Cyber threats to smart grids represent a significant concern due to the critical role these systems play in national infrastructure, impacting everything from individual households to national security. Smart grids, with their advanced control,

communication, and computing capabilities, offer substantial improvements over traditional grids in efficiency, reliability, and sustainability. However, these features also launch susceptibilities that can be subjected to exploitation by cyber attackers. The comprehension of these threats is crucial for developing effective countermeasures [15].

2.1. Smart grid architecture under cyber threat

Smart grid architecture integrates various components—such as smart meters, sensors, advanced metering infrastructure (AMI) [19], distribution management systems (DMS) [20], and supervisory control and data acquisition (SCADA) systems [22]—each of which is susceptible to cyber threats. These components, interconnected via digital communication networks, collectively enhance the effectiveness and dependability of the grid but also expand the attack surface for cyber adversaries. The smart meters and sensors acquire and communicate data instantaneously, making them prime targets for data breaches and tampering, potentially leading to inaccurate billing and energy theft. AMI is responsible for the interaction between smart meters and functionality companies that can be compromised to disrupt raw data flow or introduce malicious data, affecting grid management [27].

PMU and SCADA systems, crucial for monitoring and controlling grid operations, are vulnerable to malware, ransomware, and unauthorized access [28]. Attacks on these systems can lead to significant disruptions, including power outages and damage to infrastructure. For instance, a successful attack on SCADA can manipulate grid operations, causing cascading failures across the network. To mitigate these risks, deploying strong encryption, multi-factor authentication, and real-time intrusion detection systems is essential. Consistent security inspections and analyses of weaknesses, and ensuring software and firmware updates further enhance the resilience of smart grid components opposed to cyber threats, safeguarding the overall integrity and functionality of the grid. It constitutes a considerable improvement in modernizing the electricity distribution system, incorporating advanced digital communications, automation, and IT infrastructure to enhance efficiency, reliability, and sustainability [34]. This sophisticated network integrates various components, such as smart meters, sensors, and automated control systems, all interconnected through a digital communication network. However, this increased connectivity and reliance on digital technologies introduce substantial cyber threats, posing substantial threats to the functionality and safety of the grid [36].

The below figure 1, representing a smart grid beneath cyber-attack and depicts the power generation, distribution and broadcasted to the control center through various real time measurement components and the interaction with energy management system in the grid environment.

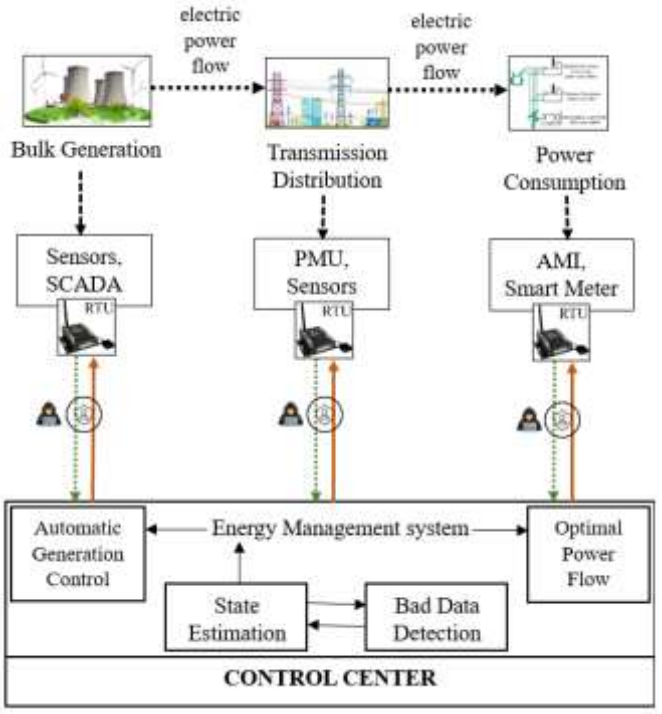

Fig. 1. Smart Grid architecture under cyber-attack.

Cyber threats to smart grids can manifest in multiple forms, includes occurrences like data leaks, denial-of-service (DoS) attacks, penetration by malware, and the alteration of control systems. Attackers can focus on diverse locations in the smart grid network, such as control centers, data acquisition systems, and even individual smart meters. These attacks can cause to severe consequences, including widespread power outages, disruption of services, stealing confidential information and harming vital systems [37]. A key challenge in securing smart grids is the vast attack surface created by the interconnected devices and systems. Each connected device represents a potential entry point for attackers. Moreover, the use of legacy systems, which may not have been created with cybersecurity considerations as a priority, exacerbates the vulnerability. Consequently, safeguarding the security of smart grids requires a comprehensive, multi-layered approach. To mitigate these threats, multiple actions can be implemented. Robust encryption protocols are essential to protect data integrity and confidentiality during transmission. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) sustenance a vital function in identifying and responding to suspicious activities in real-time. Conducting regular security assessments and penetration testing is essential for uncovering vulnerabilities and strengthen defences [38]. Additionally, implementing network partitioning can limit the distribute of attacks and protect critical components.

2.2 State estimation in SG

State estimation in smart grids is a sophisticated process that involves calculating the most probable state of the electrical grid using available measurement data from numerous components such as sensors, phasor measurement units, smart meters, and other monitoring devices [39]. The objective is to produce an accurate model of the grid's current operating conditions, despite the inherent uncertainties in measurement data. In table 2, summarizes the key steps involved in the process, the components used, and the purpose of each step,

Table 2. A process of systematic state estimation

Step	Components Involved	Purpose
Data Collection	Smart Meters, Sensors, Phasor measurement units, Remote terminal units	Collect accurate and instantaneous raw data records on voltage flows, current flows, frequency, and phase angles.
Data Transmission	Communication Networks	Transmit the collected data in a secure manner to a central control system for processing.
Data Processing	Data Aggregators, Software Algorithms	Filter and clean the data to remove noise and correct errors, validate and reconcile data discrepancies.
State Estimation	State Estimation Algorithms (e.g., WLS, EKF)	Apply mathematical models to estimate the grid's state based on the processed data.
Estimation Output	Control Center Displays, Monitoring Systems	Provide outputs that reflect the current state of the grid, including voltage levels, power flows, etc.
Utilization	Grid Operators, Automated Control Systems	Use the estimated state for monitoring, control, optimization, and decision-making within the grid.
Feedback and Updates	Feedback Systems, Continuous Improvement Processes	Update the estimation process and models based on feedback to improve accuracy and adapt to changes.

State estimation is fundamental function of smart grids, providing the necessary insights for maintaining stability, efficiency, and security [40]. As smart grid technologies evolve, so too will the methodologies and technologies for state estimation, adapting to more dynamic and complex grid environments.

2.3 Vulnerability of SG components

Smart grids, by their very nature as complicated and interrelated systems, incorporate various components that are susceptible to cyber-attacks. The interpretation of these risks is crucial for enhancing security measures and preserving the stability and trustworthiness of the power supply. In table 3, describes the main vulnerable components of smart grids and the anticipated impact of their exploitation.

Table 3. Vulnerability and its impact of smart grid components.

Components	Vulnerabilities	Impact of Cyber Attacks
Smart Meters	- Tampering with meter readings - Billing fraud - Disconnecting power - Entry points for broader attacks	- Incorrect billing - Loss of service - Breach of customer privacy
Communication Networks and Protocols	- Data interception and manipulation - Spoofing of control commands - Vulnerability to eavesdropping	- Disruption of operational data flow - False operational commands leading to malfunctions
Data Management Systems	- Data manipulation - Theft of consumer information - Introduction of malicious code	- Loss of data integrity - Privacy breaches - Malfunction of grid operations
SCADA Systems	- Control over physical grid operations - Potential for causing physical damage - Inducing system malfunctions	- Grid destabilization - Potential blackouts - Physical damage to infrastructure
Grid Management Software	- Operational disruptions - Incorrect electricity dispatching - Manipulation of energy markets	- Inefficient grid operation - Financial losses for utilities and consumers
Distributed Energy Resources (DERs)	- Mismanagement of energy distribution or storage - Instability in energy supply	- Unreliable power supply - Damage to energy storage systems
Substations and Transformers	- Remote control leading to outages or damage - Manipulation of electrical flows	- Localized or widespread outages - Permanent damage to critical infrastructure
Utility Websites and Customer Interfaces	- Personal and financial data breaches - Phishing attacks aimed at consumers	- Identity theft - Financial fraud

These vulnerabilities highlight the interdependent nature of modern smart grids where a breach in one component can have cascading effects across the system. The impacts range

from financial and operational disruptions to significant threats to public safety and security [41]. Effective cybersecurity measures, including robust encryption, secure communication protocols, persistent monitoring, and rapid incident mitigation capabilities, are essential to safeguard these critical infrastructures.

2.4 Smart Grid communication Protocols

Smart grids use a wide range of communication protocols to handle data transmission between different physical elements, comprising smart meters, data concentrators, and control centers [42]. These protocols are developed to ensure reliable, secure, and efficient communication across the complex infrastructure of a smart grid. The table 4, depicts some of the key communication protocols used in smart grid systems.

Table 4. Various communication protocols in SG

Protocol	Primary Purpose	Key Features
IEC 61850	Substation automation and inter-device communication	Supports real-time and non-real-time data, includes robust security features like data integrity.
DNP3	Communication between control centers and substations	Robust error checking, supports a wide range of data types, widely used in utilities.
Modbus	Connecting industrial electronic devices	Simple, easy to deploy, operates over serial lines and TCP/IP, widely used in various industries.
Zigbee	Home area network communications	Low-power wireless mesh network standard, suitable for short-range communications.
Wireless HART	Process automation in harsh environments	Wireless adaptation of HART, designed for secure and reliable sensor networking.
IEC 62351	Security for power system management communications	Focuses on enhancing the security of communications, including authentication and encryption.
IEEE 802.15.4g	Smart utility networks	Designed for large-scale utility networks, supports minimal energy consumption and robust networking.
LTE	High-speed wide-area communications	High bandwidth, low latency, supports mobile and fixed communication needs.
NB-IoT	IoT applications in smart grids	Low power, long-range capabilities, ideal for smart metering and other IoT devices in utility networks.

These protocols serve a crucial function in the functioning of smart grids, ensuring not only the efficient transmission of data but also the protection and consistency of the absolute grid system. As smart grid technologies develop, these protocols are continually being updated and new standards developed to meet changing demands and enhance grid resilience [43].

2.5 Categories of Cyber Attacks

1. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks [11][8]

This attacks target is to overwhelm the smart grid's network or resources, making them unavailable to users. For a smart grid, this could mean disrupting the communication between diverse elements of the grid, leading to operational failures and loss of control.

2. Man-in-the-Middle (MitM) Attacks [12]

MitM attacks entail the covert interception and potential modification of two parties' communications by the attacker. This could jeopardise the integrity of data interchange between field equipment and control centres in relation to smart grids, resulting in inaccurate grid control and misinformation.

3. Malware and Ransomware [15]

Malicious software utilised to interrupt, damage, or obtain unapproved reach to the smart grid infrastructure. Ransomware, a type of malware, encrypts files, demanding a ransom for decryption keys. Such attacks can cripple grid operations, leading to power outages or financial losses.

4. Phishing and Spear Phishing [16]

These techniques are employed to mislead individuals into revealing confidential information, such as login credentials. In a smart grid scenario, phishing could be used to obtain entry to safe areas of the network, allowing attackers to manipulate control systems or steal sensitive data.

5. SQL Injection [20]

By exploiting vulnerabilities in the software applications used by smart grids, attackers can use SQL injection to manipulate or steal data from databases. This could lead to the exposure of confidential operational data or consumer information.

6. Insider Threats [21]

The internal threats to the organisation, such as irate workers or contractors having access to the grid's control systems, pose a significant risk. Insiders could misuse their access to facilitate attacks or steal sensitive information.

7. Advanced Persistent Threats (APTs) [22]

APTs involve extended and focused cyberattacks in which an unapproved individual obtains entry to a network and stays hidden for a long time. In smart grids, APTs could be used for espionage or sabotage, aiming to disrupt critical infrastructure operations subtly.

8. Zero-Day Exploits [9]

These are attacks that exploit weaknesses in hardware or software that remain unidentified, giving the developer or vendor "zero days" to address the problem. Smart grids, reliant on complex software systems, are particularly vulnerable to zero-day exploits until patches or mitigations can be deployed.

9. Data Manipulation and Integrity Attacks [26]

Unlike attacks seeking to steal or encrypt data, these threats aim to subtly alter data, such as meter readings or control commands, without detection. This can lead to incorrect billing, misallocation of resources, or unsafe changes in grid operations.

10. Supply Chain Attacks [25]

Attackers target suppliers or vendors within the smart energy ecosystem to compromise the security of products or services before they are deployed within the grid. This could include tampering with software updates or hardware components to gain unauthorized access or introduce vulnerabilities.

Addressing these cyber threats needs an extensive and multiple layer security strategy that encompasses not only technology-based remedies but also regulatory compliance, employee training, and collaboration among industry stakeholders. comparison table 2, for various attacks in smart grids involves categorizing the types of attacks based on their targets, methods, impacts, and possible detection/mitigation techniques. Smart grids, with their sophisticated computational, communication, and control competencies, confront a diverse range of cyber threats that can affect everything from generation to consumption [24].

Table 5. Comparison for various attacks in smart grid

Ref	Attack Type	Target Component	Method	Impact	Detection/ Mitigation Techniques
[11]	Denial of Service (DoS)	Communication networks	Flooding networks with excessive traffic	Service unavailability, operational disruption	Traffic monitoring, rate limiting, redundant pathways
[12] [13]	Man-in-the-Middle (MitM)	Communication links	Intercepting and modifying transmission	Information theft, command falsification	Encryption, mutual authentication, secure channels

[14]	False Data Injection	Data acquisition systems	Injecting or altering sensor or meter readings	Incorrect operational decisions, energy theft	Anomaly detection, data validation, secure authentication
[15]	Malware Attacks	Software, control systems	Malicious software introduction	System control loss, data theft, service disruption	Anti-malware tools, secure coding practices, user training
[16]	Phishing Attacks	Human operators	Deceptive communication	Unauthorized access, data breaches	Employee training, email filtering, two-factor authentication
[18]	Physical Tampering	Infrastructure, hardware	Direct physical damage or alteration	Equipment damage, service disruption	Physical security measures, surveillance, access control
[20]	SQL Injection	Databases, web applications	Malicious SQL code injection	Unauthorized data access, database manipulation	Input validation, use of prepared statements
[21]	Insider Threats	Any component	Abuse of legitimate access	Sabotage, data theft, unauthorized changes	Access control, activity monitoring, policy enforcement
[22]	Eavesdropping	Communication networks	Passive interception of information	Privacy breaches, information theft	Data encryption, secure communication protocols
[23]	Energy Theft	Metering infrastructure	Manipulation of meter readings	Financial losses, inaccurate billing	Anomaly detection in usage patterns, secure metering
[25]	Supply Chain Attacks	Hardware, software supply chains	Compromising components before installation	Backdoors, vulnerabilities introduction	Secure supply chain practices, hardware/software verification

This table simplifies the vast landscape of cybersecurity threats to smart grids. Each attack type can have multiple variants and can be part of sophisticated cyber campaigns combining several attack vectors. The effectiveness of detection and mitigation techniques is contingent upon various factors, among which sophistication of the attack, the security protection posture of smart grid system, and timely response of the cybersecurity team.

2.6 Potential Impacts of Cyber Threats

Cyber threats focusing on smart grids represent a substantial damage to the dependability, stability, security, and efficiency of energy distribution and management. Smart grids, which include digital technology that monitors and controls the transmission of power generated from all sources generating to encounter the diverse electricity demands of end users, are inherently suscept vulnerable to cyber threats due to their increased connectivity and reliance on communication networks and information technology [44]. The effect of cyber-attacks on intelligent power distribution networks can be widespread, affecting not just the operational aspects of power distribution but also economic, social, and environmental factors [45]. The table. 6, Summarizing the possible effects of attacks targeting smart grid systems in cyberspace, highlighting the diverse consequences and the areas they affect.

Table 6. Impacts of Cyber Threats in Smart Grid.

Impact Category	Description	Potential Consequences
Service Disruption	Attackers disrupt electricity flow by shutting down critical grid components.	Power outages affecting homes, businesses, and critical services.
Economic Loss	Extended disruptions cause halted production and business revenue loss.	Economic instability, significant losses in revenue, and damaged equipment.
Data Security	Cyber attackers access confidential data from customer databases or business info.	Identity theft, financial fraud, and loss of consumer trust.
Safety Risks	Manipulation of control systems leads to unsafe operating conditions.	Public safety hazards, potential for accidents or catastrophic failures.
Grid Instability	Interference with load balancing or data corruption used for operational decisions.	Voltage fluctuations, uncontrolled power flows, systemic grid failures.
Physical Damage	Attacks cause physical damage to critical infrastructure like transformers.	Costly repairs, long-term outages, decreased operational lifespan of assets.
Regulatory Repercussions	Failure to secure the grid leads to regulatory compliance breaches.	Fines, legal actions, increased scrutiny, and overhaul of security measures.
Reputation Damage	Public perception of the utility's reliability and safety is compromised.	Loss of consumer trust, decreased market share, and profitability impacts.
Resource Diversion	Resources are diverted from regular operations to address cyber-attack aftermath.	Delayed progress on upgrades and expansion, affecting growth and innovation.

This table provides a comprehensive view of the different types of impacts that a cyber-attack can have on smart grids, emphasizing the significance of strong cybersecurity protocols to safeguard these vital infrastructure systems.

3. CYBER ATTACK DETECTION TECHNIQUES

Detecting cyber-attacks in smart grids is indispensable for maintaining the security and reliability of the electrical energy supply. Given the complex and interconnected nature of smart grids, a variety of detection techniques are employed, combining both traditional cybersecurity measures and innovative approaches adapted to the unique features of the smart grid environment [17][24]. These techniques focus on identifying potential threats, anomalies, and malicious activities before they can cause significant damage.

3.1 Anomaly Detection

By analysing deviations from normal operational patterns, anomaly detection systems can flag potential cyber threats before they cause significant damage. This process involves various techniques, each with its mathematical foundations, to effectively monitor and analyse to produced massive amounts of dataset by smart grid components. Anomaly detection algorithms identify unusual responses that fail to align with standard expectations. One common approach is statistical anomaly detection, which can be formulated as:

3.1.1 Statistical Anomaly Detection

The statistical anomaly identification method relies on defining a normative model of system behavior and then identifying deviations from this model. A simple statistical approach could be based on thresholding a parameter, say X, where X represents a measurable aspect of the grid's operation (e.g., traffic volume, login attempts, or command signals).

Threshold Model: $f(X) = \begin{cases} 1 & if\ X > \theta \\ 0 & otherwise \end{cases}$

Here, $f(X)$ denotes the detection function, returning 1 (anomaly detected) if X exceeds a threshold θ, and 0 otherwise.

Z-Score Analysis:

For a given dataset x, the Z-score for a data point x is calculated as:

$$z = \frac{(x - \mu)}{\sigma}$$

Where, x is a unique measured value, μ is the mean of the observed values of dataset, and σ is the standard deviation measure. Data points with a Z-score exceeding a threshold (e.g., $|Z| > 3$) are considered anomalies.

CUSUM (Cumulative Sum) Method:

The CUSUM technique is used to detect small changes from the expected sequence of observations. It computes the cumulative sum of deviations of each data point from the mean. Given a series of data points $x_1, x_2, \ldots, x_n$ the CUSUM at point i is:

$$S_i = max\ (0, S_{i-1} + x_i - \mu - K)$$

where μ is the target value, and K is a reference value to detect deviation. An alarm is raised if $S_i$exceeds a certain threshold.

3.1.2 Statistical based Machine Learning Approaches

Machine learning models, particularly supervised learning, can be trained to distinguish between normal and malicious activities. The machine learning models for cyber-attack identification can vary widely but often include supervised learning frameworks like Neural Networks (NN) and Support Vector Machines (SVM).

Support Vector Machine (SVM):

$$f(x) = w^T x + b$$

Where $f(x)$ is the decision algorithm, x is the input feature geometric vector, w is the weight vector quantity, and b is the bias. The sign of $f(x)$ determines the class of x.

The anomaly detection in smart grids can leverage SVMs to determine the hyperplane that efficiently separates data points into two classes: normal and anomaly. For linearly separable data, the hyperplane is defined by the equation: $w.x - b = 0$ where w is the orthogonal vector quantity to the affine subspace, x is a data point, and b is the bias. In practice, for non-linearly separable data with complex boundaries kernel functions are utilized to encode input data into an extended higher-dimensional space where the hyperplane can effectively achieve separation.

Classification Algorithm:

Given a feature vector $x \in \mathbb{R}^n$ that describes an event or observation in the smart grid, and a label $y \in \{0,1\}$ indicating normal (0) or attack (1) behavior, a classification model h: $\mathbb{R}^n \rightarrow \{0,1\}$ is trained on the dataset of such examples to forecast the label for new, unseen observations.

3.2. Intrusion Detection Systems (IDS)

Intrusion detection systems for smart grids can employ various algorithms, incorporating detection methods that rely on signatures and behavior-based identification, which might use state estimation or pattern recognition algorithms.

State Estimation for IDS:

State estimation in smart grids often uses models to evaluate the present state of the electrical network according to observable measurements. Discrepancies between observed measurements and model predictions can indicate potential cyber-attacks.

State Estimation Model: The electrical grid's state can be estimated using the model

$$z = Hx + e$$

where, z is the vector of measured observations, H is the determination matrix, x is the state variable to be estimated, e represents measurement noise or errors. Anomalies or attacks might be detected by analyzing the residuals $r = z - H\hat{x}$ where $\hat{x}$is the estimated state.

Kalman Filter:

A common approach for real-time status estimation in smart grids. The Kalman filter predicts the condition of a linear dynamic system from a sequence of inaccurate measurements.

Given the state equation: $x_k = Ax_{k-1} + Bu_k + w_k$

and the measurement equation: $z_k = Hx_k + v_k$

wherex_k is the state vector quantity, z_k is the measurement vector quantity, $A,\ B, and\ H$ are matrices defining the system dynamics, u_k is the control vector, and w_k, v_k are the process and measurement interference. The Kalman filter iteratively predicts and updates the state estimates, which can be used to detect anomalies or attacks by comparing the estimated states against measured states.

WLS State Estimation:

The Weighted Least Squares (WLS) estimator is commonly leveraged to detect inconsistencies indicative of cyber-attacks, for instance false data injection.:

$$\hat{x} = (H^T W H)^{-1} H^T W z$$

Where$\hat{x}$ is the predicted state space vector, H is the measurement matrix, W is the weight matrix for the measurements, and z is the vector of observed measurements.

3.3 Signature-Based Detection

Signature-based detection systems work by scanning network traffic or system activities for patterns that match known signatures of malware or cyber-attack techniques. It is a digital fingerprint of known malicious activity, which can include specific byte sequences in network traffic, known malicious code snippets, or Behavior patterns that signals of a cyber-attack. When a match is found, the system can alert administrators, block the activity, or take other pre-defined actions to mitigate the threat.

Rule-Based Methods

It involves the use of predefined rules that are based on the characteristics of known attacks. These rules can be thought of as a set of conditions that, when met, indicate a potential attack. In a smart grid, rule-based detection might involve rules for identifying abnormal behaviours or known attack signatures on the network. A rule R in a rule-based method can be characterized as a function that creates a mapping an input vector x (representing system or

network characteristics) to a boolean value indicating the presence (1) or absence (0) of an attack:

$$R(x) = \begin{cases} 1 & if\ conditions\ are\ met \\ 0 & otherwise \end{cases}$$

Pattern Matching Techniques

It involves comparing observed activities or data signatures against a dataset of known attack patterns or signatures to recognize matches. This approach might be used to scan network traffic for specific signatures associated with malware or hacking tools known to target smart grid infrastructures.

Let's define a signature database as $S = \{s_1, s_2, \ldots, s_n\}$, where each s_i is a vector representing the signature of a known attack. The observed data at any instance is represented as a vector d. A matching function M compares d against each s_i to find a match:

$$M(d, s_i) = \begin{cases} 1 & if\ d\ matches\ s_i \\ 0 & otherwise \end{cases}$$

3.4 Machine Learning-Based Detection

Machine Learning (ML) that leveraged cyber-attack identification and detection in smart grids utilizes various algorithms to recognize and alleviate possibility cyber threats in an automated and efficient manner. Machine learning-driven cyber-attack identification typically involves developing models capable of acquiring knowledge from data potential to detect anomalies or classify behaviours as normal or malicious. Here, outlines a common approach as follows,

3.4.1 Supervised Learning

This approach employs classified to train models that can classify or predict cyber-attacks. Common algorithms include Decision Trees, Neural Networks (NN), and Support Vector Machines (SVM).

Decision Trees

Decision trees classify patterns by splitting the tree from the root into multiple leaf nodes that provide pattern classification. Every node within the tree signifies a characteristic of the model intended for clustering, while each branch denotes a potential value that the node may assume.

Entropy (measure of disorder or impurity):

$$H(S) = -\sum_{x \in X} p(x)\, log_2\, p(x)$$

Where, S is the set of data samples, X represents different classes, and $p(x)$ is the ratio between the count of factors in class x and the count of factors in set S.

Information Gain (used to decide which feature to split on at each step in the tree):

$$IG(S,A) = H(S) - \sum_{t \in T} p(t)\, H(t)$$

Where,A is the feature by which the split is made, T are the subsets are created by dividing the set by function$A$, and $p(t)$ is the ratio of the elements in subset t to the count the frictions of elements in set S.

Support Vector Machine (SVM)

Support Vector Machines (SVM) are utilized to evaluate a hyperplane in an N-dimensional state space, where N depicts the set of features, that successfully distinguishes between different classes of data points. The objective is to optimize the margin separating the data points belonging to the two classes. The hyperplane equation is,

$$w^T x + b = 0$$

$$f(x) = sign(w^T x + b)$$

Optimization function, $min_{w,b} \frac{1}{2} ||w||^2$

Subject to, $y_i(w^T x_i + b) \geq 1$ for all i

Where, where w is normalized and x represents the shape vector. and b is the offset bias, $f(x)$ is a decision function and y_i are the labels.

3.4.2 Unsupervised Learning

Used to detect unusual patterns or anomalies without prior labelling of the data. Algorithms like k-Means, Tree-based Clustering, and Gaussian Mixture Models (GMM) are typical examples.

K-means Clustering

K-means clustering identifies unusual patterns in smart grid data, aiding in attack detection by isolating anomalies, indicating potential security breaches. The K-means algorithm divides the observations into k clusters. Here, every view is of the herd and its proximity.

Objective Function: $J = \sum_{j=1}^{k} \sum_{i=1}^{n} \; || \, x_i^{(j)} - c_j ||^2$

where $x_i^{(j)}$ is the ith measurement point in similar aggregation of j, and c_j is the centroid of similar data point cluster j. The goal is to minimize J.

Gaussian Mixture Models (GMM)

GMMs model with probabilistic data as a combination of several gaussian distributions. The probability of a data point is given as,

$$p(x) = \sum_{k=1}^{K} \pi_k \mathcal{N}(x|\mu_k, \sum\nolimits_k)$$

where π_k are the mixing load factors, and $\mathcal{N}(x|\mu_k, \sum_k)$ is the Gaussian distribution for component k. The Expectation-Maximization (EM) Algorithm is given as, E-step evaluate the subsequent probabilities $\gamma(z_{nk})$ that data point x_n belongs to cluster k

$$\gamma(z_{nk}) = \frac{\pi_k \mathcal{N}(x_n|\mu_k, \sum_k)}{\sum_{j=1}^{K} \pi_j \mathcal{N}(x_n|\mu_j, \sum_j)}$$

The M-step for Re-estimate the parameters using the posterior probabilities.

$$\mu_k = \frac{1}{N_k} \sum_{n=1}^{N} \gamma(z_{nk}) x_n$$

$$\sum_k = \frac{1}{N_k} \sum_{n=1}^{N} \gamma(z_{nk})(x_n - \mu_k)(x_n - \mu_k)^T$$

$\pi_k = \frac{N_k}{N}$, Where $N_k = \sum_{n=1}^{N} \gamma(z_{nk})$

Useful for detecting unusual patterns or anomalies without prior labelling, particularly effective in identifying new or evolving attacks.

3.4.3 Reinforcement Learning

Applied in scenarios where the system learns to make decisions through trial and error, optimizing a performance criterion. It's useful for developing adaptive systems that improve their policies over time.

Q-Learning

Q-Learning is a model-agnostic learning model that acquires the value of a task in a specific situation without a model in the environment. It can be deployed for making decisions in smart grid systems, such as response actions to potential cyber threats.

Define the Q-value mechanism $Q(l, a)$ which signifies the value of initiating in a phase s. The Q-function is updated using the bellman mathematical relationship as,

$$Q(l', a) \leftarrow Q(l', a) + \alpha[r + \gamma max_{a'} Q(l', a') - Q(l, a)]$$

Where, l and l' are the current and next states, respectively, a and a' are the actions taken in states s and s', r is the token obtained after taking the action a in state s, α is the learning ratio, γ is the discount factor. The agent learns the policy π that maximizes the expected reward. The optimal policy can be derived from the Q-values as,

$$\pi^*(l) = arg\, max_a \; Q(l, a)$$

It is suitable for developing adaptive security systems that optimize response strategies based on the dynamic environment of smart grids.

3.5 Deep-Learning based Attack Detection

Deep learning-based cyber-attack identification in smart grids is an advanced approach to safeguarding critical energy infrastructure from increasingly sophisticated cyber threats. This approach leverages the power of artificial neural networks to identify potential security breaches by analysing patterns and anomalies in the data that traditional methods might miss. We'll focus on a straightforward approach using a feedforward neural network (FFNN), one of the simpler and widely used architectures in anomaly detection tasks.

Step 1: Model Representation

A feedforward neural network comprises of multiple layers of neurons, each individual is fully connected to the neurons in the next layer. For simplicity, examine a network that contains a single hidden layer. The mathematical representation of this network is:

Input layer: Receives input vector $x \in \mathbb{R}^d$, where d is the number of features.

Hidden Layer: Applies weights W_1 and biases b_1, and the activation function that is non-linear in nature σ. The output of the hidden layer for input x is:

$$h = \sigma(W_1 x + b_1)$$

Output Layer: Transforms the hidden layer output using another set of weights W_2 and biases b_2. In a binary classification (normal vs. attack), the output layer often uses a sigmoid function to produce a probability distribution:

$$y = \sigma(W_2 h + b_2)$$

Step 2: Loss Function

In the context of binary classification, the loss function known as cross-entropy is employed, as it is well-suited for binary labels. The loss for a single data point with true label p (where t is 0 or 1) and predicted probability y is:

$$L(p, cy') = -p\, log\ (cy') - (c * 1 - p)\, log\ (1 - cy')$$

For a training dataset with N data points, the total loss is the average of individual losses:

$$L = \frac{1}{N}\sum_{k=1}^{N}(-p_k\, log(y'_k) - (1 - p_k)\ log\ (1 - y'_k))$$

Step 3: Training the Model

Training involves adjusting the weights W_1, W_2 and biases b_1, b_2 to diminish the loss function. This is usually accomplished using backpropagation and an optimization algorithm like gradient descent. The parameter update rule using gradient descent is:

$$\theta = \theta - \eta \nabla_\theta L$$

where θ represents any parameter in $\{W_1, b_1, W_2, b_2\}, \eta$ is the learning rate, and $\nabla_\theta L$ is the incline gradient vector of the error function with esteem to the parameter.

Step 4: Anomaly Detection

Once the model is trained, anomaly detection can be performed by feeding input data into the network and examining the output. If the output probability y exceeds a certain threshold T, typically close to 1, the input is classified as an attack; otherwise, it is considered normal. The threshold may be modified to achieve the preferred levels of sensitivity and specificity within the detection system. This is typically measured using a threshold T on the reconstruction error:

If $L(x,\ \hat{x}) > T$, then x is an anomaly.

Step 5: Model Evaluation and Adjustment

After training, evaluate the model using adequate metrics (accuracy, precision, recall, F1-score) and adjust criterion parameters, architecture, or even the model type as needed to improve detection capabilities.

3.6 Hybrid Detection Techniques

It involves integrating multiple detection methods and designing systems that adapt based on observed data and threat landscapes. This involves the use of both ensemble methods and adaptive learning strategies.

3.6.1 Integration of Multiple Detection Techniques

Ensemble Methods

Suppose you have N different models $\{M_1, M_2, \ldots, M_N\}$ each capable of predicting the likelihood of a cyber attack. Each model $M_i$outputs a score $s_i(x)$ for a given input x. The ensemble prediction $S(x)$ is given by:

$$S(x) = \sum_{i=1}^{N} w_i s_i(x)$$

where w_i are the weights assigned to each model's output, subject to $\sum_{i=1}^{N} w_i = 1$ and $w_i \geq 0$.

To find the optimal weights, can mitigate a loss function designed to assess the variation between the ensemble output and the actual outcomes over a dataset. A common choice is the logistic loss function, leading to the optimization problem:

$$\min_{w} \sum_{j=1}^{M} log\ (1 + exp\ (-y_j S(x_j)))$$

Where $y_j \in \{-1,1\}$ are the labels for the training samples x_j, and M is the total set of samples.

3.6.2 Adaptive Detection Systems

State Space S: Define the state space S to encapsulate the relevant information about the system, which could include metrics like system load, frequency of attacks, types of detected threats, and outputs from different detection models.

Action Space A: The action space A includes possible adjustments the system can make, such as changing thresholds for detection algorithms, toggling the use of particular detection models, or modifying parameters within existing models.

Reward Function R: The reward function R(s,a) needs to motivate the correct adjustments to maximize the effectiveness of the detection system. It often considers factors such as the increase in true positive rate or decrease in false positives:

$$R(s,a) = \alpha \times True\ Positives - \beta \times False\ Positives$$

where α and β are tuning parameters that prioritize certain aspects of the detection performance. The value function $V^{\pi}(s)$ as the anticipated return commencing from state and following protocolπ;

$$V^{\pi}(s) = \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^{t} R\big(s_t, \pi(s_t)\big) \mid s_0 = s\right]$$

where γ is the adjustment factor, reflecting the significance of prospective benefits.

3.7 Comparison of Detection Techniques

A systematic evaluation of various cyber-attack detection methodologies in smart grids, encompassing signature-based detection, anomaly-based detection, machine learning-based detection, and deep learning-based anomaly detection.

Table 7. Comparison of various Detection Techniques

Ref.	Feature/ Aspect	Signature-Based Detection	Anomaly-Based Detection	Machine Learning-Based Detection	Deep Learning-Based Anomaly Detection	Hybrid Detection Techniques
[28] [29]	Basis of Detection	Known attack signatures	Deviations from normal behavior	Patterns and correlations identified through machine learning algorithms	Complex patterns and relationships identified using deep neural networks	The integration of various detection techniques is frequently employed, incorporating both signature and anomaly-based elements

[30] [31]	Key Strengths	- High precision for known threats - Quick detection	- Detects novel threats - Adaptable to changing network behavior	- Adaptable to evolving threats - Learns from historical attack data	- Excellent at detecting subtle and complex anomalies - Can analyse substantial quantities of data	- Balances the strengths of included techniques - Can reduce false positives - Enhances detection of both known and unknown threats
[33] [35]	Key Weaknesses	- Ineffective against new, zero-day attacks - Needs regular signature updates	- High false positive rate - Difficulty in defining normal behavior	- Requires extensive historical data - Potential for overfitting	- Needs large data sets for effective training - High computational resources required	- Complexity in implementation - Depends on the effectiveness of constituent methods - May inherit weaknesses of combined techniques
[36]	Update Requirements	Frequent signature updates required	Needs ongoing adjustment to behavioural baselines	Model retraining with new data and attack patterns	Regular retraining with updated data sets and emerging threats	Varies, but often requires updates to machine learning models and signature databases
[38]	Effectiveness Against Zero-Day Attacks	Low	High	Moderate to high, depending on data and model	High, due to the ability to learn complex patterns	Very high, as it leverages multiple detection paradigms

[39]	Resource Intensity	Low to moderate	Moderate to high	Ranging from moderate to substantial, based on model complexity	High, due to the computational demands of training deep networks	Ranging from moderate to substantial, based on model complexity and number of integrated methods
[40]	Implementation Complexity	Moderate	High	High, requires machine learning expertise	Very high, requires expertise in deep learning and significant computational infrastructure	High, due to the need to integrate and manage multiple detection systems
[42]	Typical Use Cases	Best for environments with well-documented attack vectors	Suited for dynamic environments with evolving behaviours	Effective in scenarios where patterns in data can be learned over time	Ideal for complex environments with vast data and sophisticated attack patterns	Optimal for contexts requiring robust and comprehensive threat detection capabilities

This table illustrates how each cyber-attack detection technique, including hybrid methods, fits into the smart grid cybersecurity framework. Hybrid Detection Techniques, by integrating elements from multiple approaches, offer a comprehensive solution that seeks to capitalize on the advantages of each approach while addressing their respective shortcomings.

4. CONTROL SYSTEM COMMUNICATION SETUP

A Networked Control System (NCS) facing cyber-attacks within smart grids poses considerable difficulties, given that the efficient management of electrical power generation, transmission, distribution, and consumption is dependent on NCS. The incorporation of conventional power systems with digital transmission and control networks in smart grids increases their susceptibility to cyber threats. The following discussion offers an in-depth analysis of the effects of cyber-attacks on NCS in smart grids, along with the relevant defense strategies.

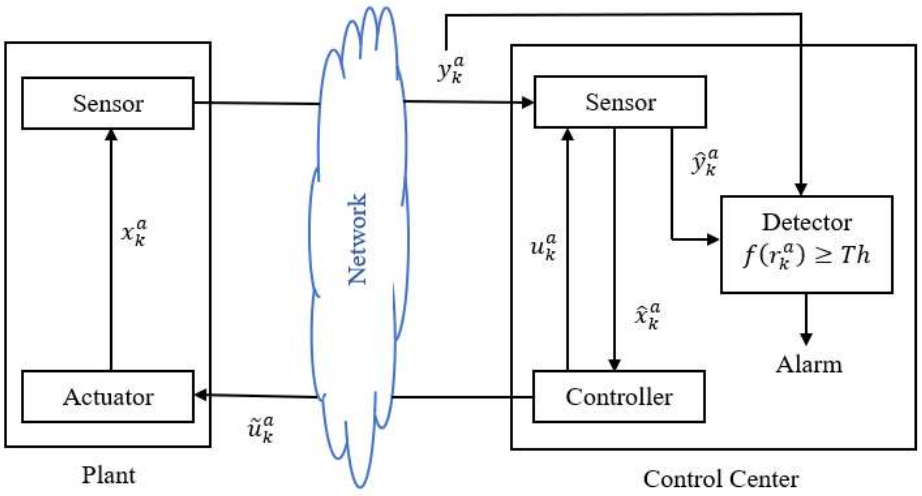

Fig. 2. Networked Control Center of CPS

Smart grids are susceptible to a range of cyber threats owing to their dependence on communication networks for the transmission of real-time data and control signals. Cyber-attacks, including False Data Injection (FDI), Denial of Service (DoS), and Man-in-the-Middle (MitM), have the potential to interfere with grid operations, resulting in instability, power outages, or even physical harm to the infrastructure. Ensuring secure communication, using encryption, intrusion detection systems (IDS), and employing resilient control strategies are essential for defending against these threats. Emerging techniques, such as blockchain and machine learning, offer promising approaches to strengthen the security and resilience of smart grid NCS under cyber-attacks. In this context, let's break down the plant model in the Networked Control System (NCS) under cyber-attacks, particularly focusing on False Data Injection (FDI) attacks.

4.1. Plant in NCS of Cyber physical systems

The physical plant is generally represented as a discrete-time linear time-invariant (LTI) system, which can be distinguished by the subsequent state-space equations.

$$x_{k+1} = Ax_k + Bu_k + \omega_k$$

$$y_k = Cx_k + \vartheta_k$$

Where, x_k is the state vector at time interval k, u_k is the control input applied to the plant at time interval k, y_k is the measurement or output observed at time interval k, A *and* B are matrices defining the system dynamics, C is the matrix that maps the state to the output, ω_k represents process noise, and ϑ_k represents measurement noise.

The State Vector $x_k \in \mathbb{R}^n$ represents the phase of the plant at time step k, where n is the dimensionality of the state, The $u_k \in \mathbb{R}^m$ denotes the control input applied to the plant at time step k, with m being the dimensionality of the input. The measurement output $y_k \in \mathbb{R}^p$ is the

observation or measurement obtained from the system at time step k, with p being the dimensionality of the output.

The system is affected by, Process Noise $\omega_k \sim N(0, Q)$ is a random noise that affects the system dynamics. It is a gaussian process noise that is independent and identically distributed (i.i.d.) characterized by a mean of zero and a specified covariance matrix Q. Measurement noise $\vartheta_k \sim N(0, R)$ is a random noise that affects the measurement output. It is also i.i.d. Gaussian noise with mean zero and covariance matrix R, independent of ω_k.

4.2. Controller in NCS of Cyber-Physical systems

The control center is furnished with a state-feedback controller, a detection system, and a state-estimator module.

State-Feedback Controller:

- The controller utilizes the present condition of the system to estimate the control input u_k that will be applied to the plant. This is typically based on a state-feedback law, such as $u_k = -Kx_k$, where K is the feedback gain.
- Although this controller plays a crucial role in system operation, the specific operations and control law are not relevant to the mathematical derivations in the article and are therefore not further specified.

Detector:

- The detector's primary function is to identify abnormalities or cyber-attacks, such as False Data Injection (FDI) attacks, in the system. It monitors the system's behavior by comparing actual measurements or control actions to expected patterns and triggers alarms if deviations are detected.
- The detection algorithm could involve statistical techniques, model-based anomaly detection, or machine learning methods to identify suspicious behavior in real-time.

State-Estimator:

- The state-estimator is responsible for assessing the actual condition of the system $\hat{x}_k$ based on the noisy measurements y_k and possibly compromised data. A typical estimator would be a Kalman Filter, which uses both the system model and the observed data to provide a best estimate of the system state, accounting for uncertainties like noise.
- The estimator is crucial when the measurement data is either noisy or under attack, as it helps mitigate the impact of incorrect or manipulated data, ensuring that the controller operates based on a more dependable assessment of the system's condition.

The state estimation is updated at each time step using the following equation:

$$\hat{x}_k = P\hat{x}_k + Qu_{k-1} + Li(y_{k-1} - R\hat{x}_{k-1})$$

Where, $\hat{x}_k \in \mathbb{R}^n$ is the estimated state vector at time interval k, $u_k \in \mathbb{R}^m$ is the control input applied to the system at time interval k, $y_k \in \mathbb{R}^p$ is the measurement vector received from the sensors, $A, B, and\ C$ are the system matrices as defined earlier.

In the Prediction Step, estimated state $\hat{x}_{k-1}$ from the antecedent time interval is employed to forecast the current state using the system dynamics $A\hat{x}_{k-1} + Bu_{k-1}$. The correction Step measurement vector y_{k-1} is compared to the predicted output $C\hat{x}_{k-1}$, and the difference (residual) $y_{k-1} - C\hat{x}_{k-1}$ is used to correct the state estimate. The correction is weighted by the Kalman gain Li, which determines how much the state estimate should be adjusted based on the measurement.

In Kalman Filter Prediction the control center uses the system model to predict the next state based on the antecedent state prediction $\hat{x}_{k-1}$ and the last control input u_{k-1}.

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1} + Bu_{k-1}$$

Update the covariance of the state estimate,

$$P_{k|k-1} = AP_{k-1}A^T + Q$$

In the Kalman Filter Update, after receiving the sensor measurement y_k, the control center corrects the predicted state:

$$\hat{x}_k = \hat{x}_{k|k-1} + L_k(y_k - C\hat{x}_{k|k-1})$$

Where, L_k is the Kalman gain,

$$L_k = P_{k|k-1}\, C^T (CP_{k|k-1}C^T + R)^{-1}$$

Then, update the covariance matrix,

$$P_k = (I - L_k C)P_{k|k-1}$$

A detection module in the control center monitors the transmission between the plant and the control center, checking for irregularities in measurement or control signals. Use machine learning models or anomaly detection algorithms to flag unusual data patterns, delays, or inconsistencies that may indicate attacks like FDI, DoS, or MitM. This algorithm ensures that the plant and control center maintain stable operation while providing mechanisms to recognize and address the potential cyber-attacks in a networked control system.

Procedure for NCS under Cyber-attack

```
# Control input using state-feedback control
u = -K * x_est
# System dynamics with process noise
x = A * x + B * u + process_noise[:, [k]]
# Measurement with noise
y = C * x + measurement_noise[k]
```

```
# Apply False Data Injection (FDI) attack after attack_start
if k >= attack_start:
    y += attack_magnitude
# Kalman filter prediction step
x_est = A * x_est + B * u
P = A * P * A.T + Q
# Kalman filter measurement update step
L = P * C.T * np.linalg.inv(C * P * C.T + R)
residual = y - C * x_est
x_est = x_est + L * residual
P = (np.eye(2) - L * C) * P
# Attack detection: Check the residual error against a threshold
if np.abs(residual) > attack_threshold:
    attack_detected.append(k)
# Log states, estimates, and measurements
states.append(x.flatten())
estimates.append(x_est.flatten())
measurements.append(y.flatten())
residuals.append(residual.flatten())
```

Uses predictions from the system dynamics to assess the state and adjusts the estimate based on incoming measurements. It reduces the effect of noisy measurements and helps detect abnormal behaviours caused by attacks. The residual represents the disparity between the forecasted and the actual measurement. A large residual indicates that the system is not behaving as expected, potentially due to an attack on the sensor or system.

5. ANALYSIS AND IMPLEMENTATIONS

Statistical analysis is a critical component of identifying and detecting false data injection cyber-attacks in smart grids. By applying a combination of descriptive statistics, time series analysis, hypothesis testing, and machine learning techniques, utilities can improve their capacity to recognise and react to malicious manipulations of grid data. Continuous monitoring and refinement of detection algorithms are essential to keep up with changing online risks, threats. Implementing such a real-time monitoring system requires integration with data streaming technologies and anomaly detection algorithms that can process incoming data rapidly and accurately. By continuously monitoring key metrics and real-time anomaly identification, utilities can improve their ability to discover and mitigate the false data injection attacks in smart grids. This can calculate metrics such as mean, standard deviation, and Z-Score to identify deviations from normal behavior. The below table that displays the statistical analysis results and visualize the data with anomalies highlighted.

Table 8. Statistical analysis result for mean, standard deviation, and Z-Score.

	Time Step	Sensor Data	Z-Score
count	1100.000000	1100.000000	1.100000e+03

mean	549.500000	102.212347	1.330653e-15
std	317.686953	12.093994	1.000455e+00
min	0.000000	67.587327	-2.864295e+00
25%	274.750000	94.239435	-6.595455e-01
50%	549.500000	101.138725	-8.881357e-02
75%	824.250000	108.428832	5.142480e-01
max	1099.000000	152.134055	4.129688e+00

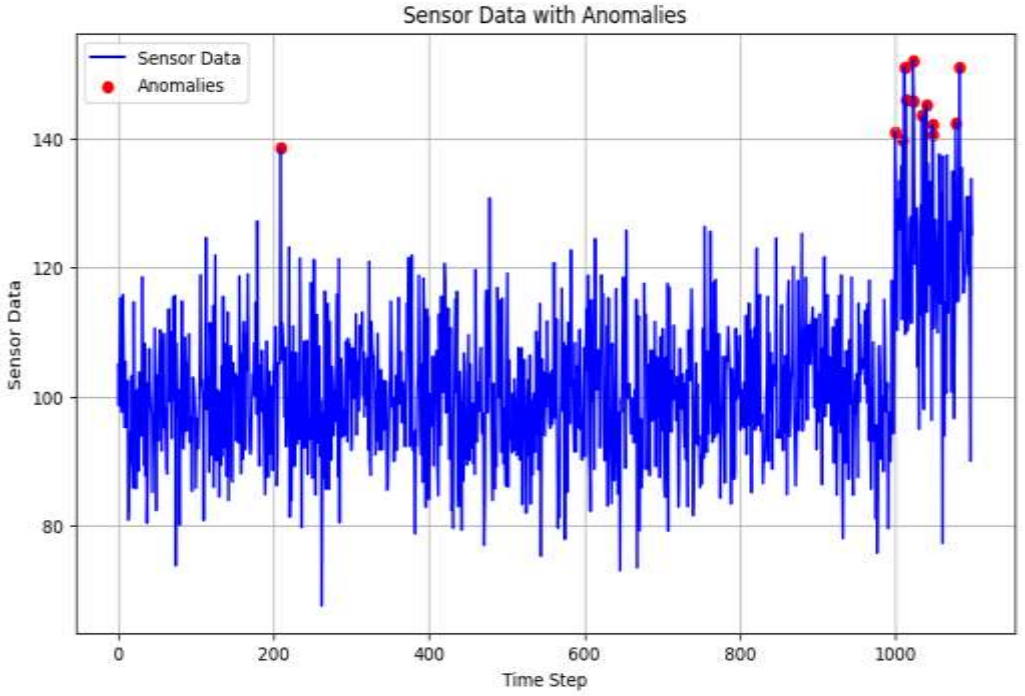

Fig.2. Detection of cyber anomalies in sensor data.

The statistical analysis table displays the summary of analysis includes various statistical measures, including count, mean, standard deviation, minimum, 25th percentile (Q1), median (50th percentile or Q2), 75th percentile (Q3), and maximum values pertaining to the sensor data and Z-Score. Anomalies are identified based on Z-Score exceeding a threshold of 3. The graph visualizes the sensor data over time, with anomalies highlighted in red. It provides a basic framework for statistical analysis and visualization of attack detection in a smart grid. And further enhance it by incorporating more sophisticated anomaly detection algorithms and real sensor data from smart grid systems. Anomaly detection in smart grid energy consumption is critical for maintaining system reliability and efficiency. This process involves identifying unusual patterns in energy usage that could indicate equipment failures, operational inefficiencies, or cybersecurity threats.

Imagine a scenario where there's a sudden, unexplained spike in energy consumption in a specific area of the grid. Anomaly detection systems would flag this pattern, triggering alerts. On investigation, it might be found that the spike is due to a malware-induced command to multiple smart meters, causing them to report or even physically draw more power.

Table 9. Dataset for cyber-attack event and its types based on various parameters.

Index	Device ID	CPU Usage %	Memory Usage %	Network Traffic In (KBps)	Network Traffic Out (KBps)	Error Rate %	Power Output	Event Type	Attack Type
0	D1001	54	10	357	907	0.300882	404	Normal	None
1	D1002	57	20	224	548	0.049289	558	Normal	None
2	D1003	74	53	198	530	2.788588	509	Anomaly	Data Injection
3	D1004	77	68	999	379	2.00975	487	Anomaly	DoS Attack
4	D1005	77	33	591	590	2.355459	563	Anomaly	Data Injection
5	D1006	19	69	629	259	0.84519	473	Normal	None
6	D1007	31	12	597	667	1.75923	583	Anomaly	Malware
7	D1008	46	72	857	946	0.191866	426	Normal	None
8	D1009	80	45	443	625	1.456883	518	Normal	None
9	D1010	22	77	123	66	2.932485	422	Anomaly	Malware

Simple thresholds based on historical consumption data can flag data points that exceed expected ranges. The techniques like k-means or DBSCAN can group similar data points together. Elements that do not belong to any specific cluster may be considered as anomalies. The predictive models estimate expected consumption based on factors like time of day, weather, and historical trends. Deviations from these predictions are potential anomalies. An advanced models such as Isolation Forests, Autoencoders, or One-Class SVM are designed to detect outliers or anomalous data points in large and complex datasets. In time series analysis the models like ARIMA or LSTM (a type of neural network) that are capable of capturing

temporal patterns and forecasting future values, thus identifying points where actual values deviate significantly from predicted ones.

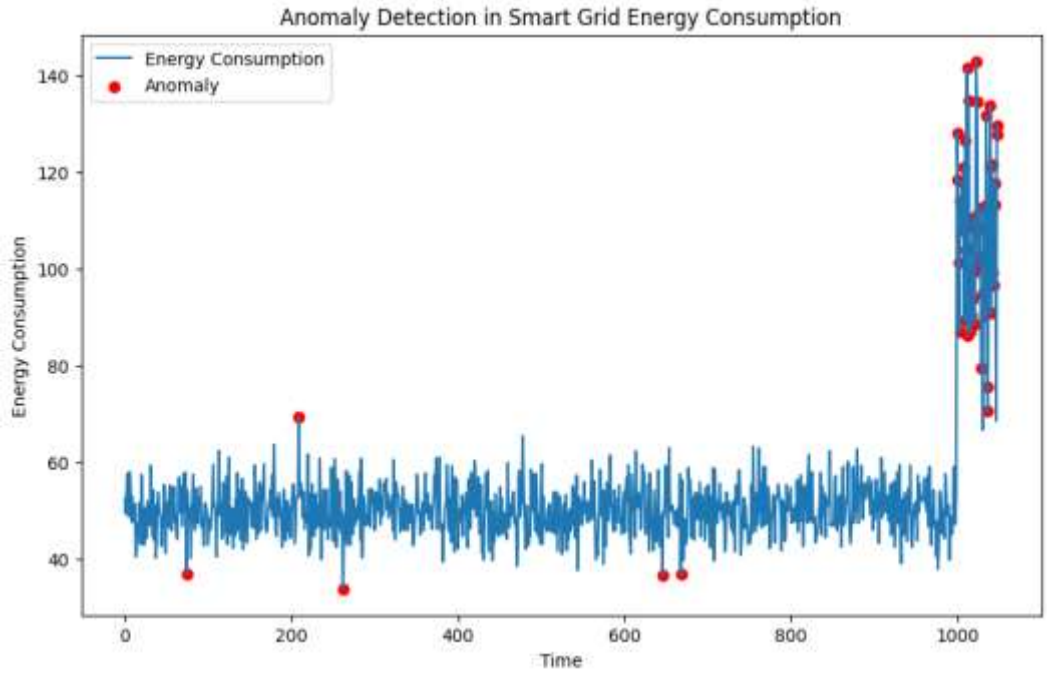

Fig. 3. Anomaly detection in smart grid energy consumption

In relation to smart grid cyberattack detection, monitoring packet size and request frequency over time can be crucial for identifying potential security incidents. These metrics provide valuable insights into network behavior, allowing operators to spot anomalies that could indicate malicious activity. Anomalously large packets may indicate that substantial amounts of data are being extracted from the system, which is common in data breach scenarios. Many types of malware send data in packets of specific sizes as they communicate with command and control servers. A small, unusually frequent packets could be a sign of a DoS attack intended to overwhelm network resources.

Table 10. Packet size and request frequency over various cyber attacks

Attack_Type	**Packet_Size**		**Request_frequency**	
	mean	**std**	**mean**	**std**
DoS	309.51902	50.749281	21.51129	4.552681
Data_theft	290.93605	46.308229	22.188919	5.468232
Data Integrity	119.59085	24.278461	4.95191	1.947501
False data injection	293.58729	29.7614	16.873161	6.351898

A sudden increase in the rate of requests might indicate scanning activities, where an attacker probes the network to identify vulnerabilities. High request frequencies can also be a sign of brute-force attacks, where attackers attempt to gain unauthorized access by trying many passwords or codes. It is regular but low-level increases in request frequency can suggest reconnaissance activities as attackers gather valuable network or device information.

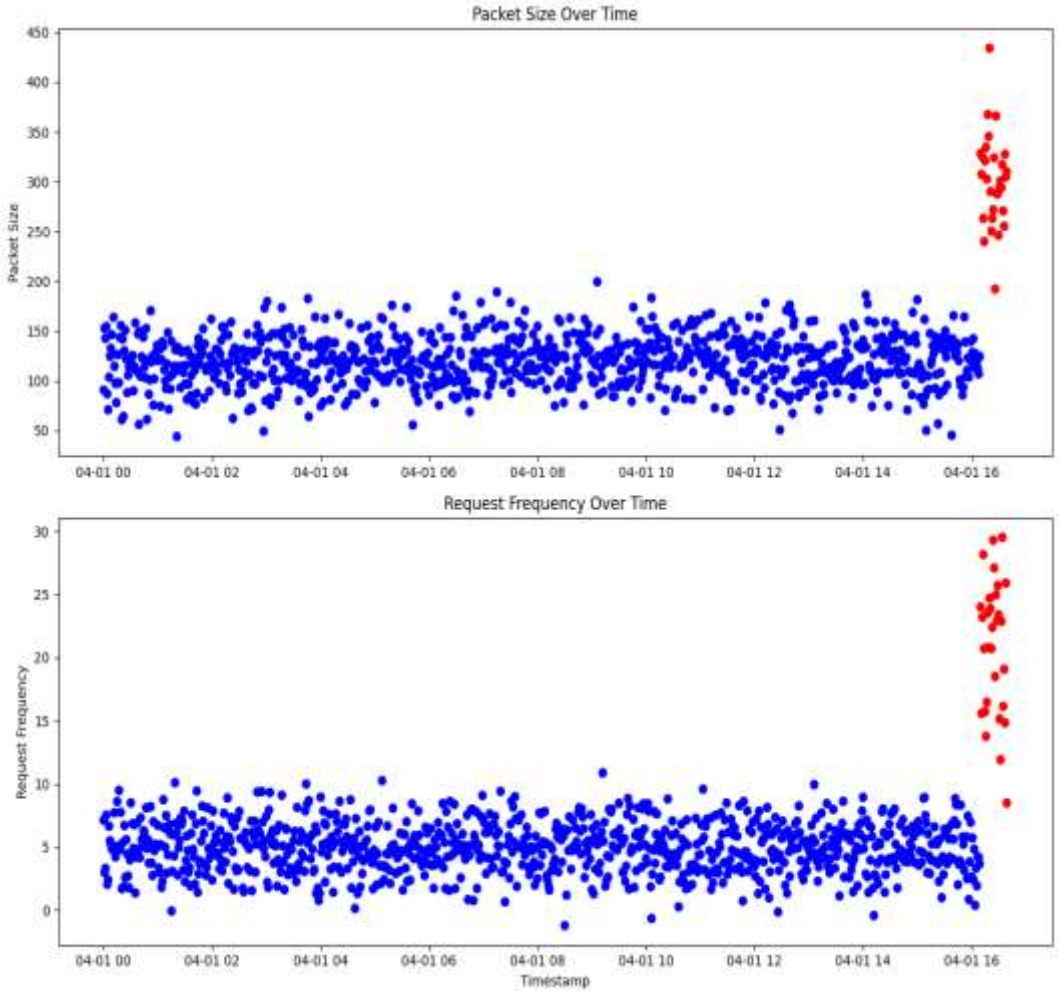

Fig. 4. The packet size and request frequency for cyber-attack detection

In a smart grid scenario, being vigilant about the network traffic by analysing packet size and request frequency is essential for maintaining system integrity and preventing disruptions. This method facilitates the prompt identification of advanced cyber threats that could evade conventional security protocols. By continuously monitoring these parameters, smart grid operators can swiftly react to emerging cyber threats, minimizing the risk to vital infrastructure and protection of reliability and security in the energy supply. This proactive

stance in cyber security is a key component in safeguarding against the transforming environment of cyber threats in smart grid environments.

6. Conclusion

This paper introduced novel approaches to enhancing Cyber-Physical System (CPS) security and cyber-attack detection in smart grids, with a particular focus on Networked Control Systems (NCS). The increasing reliance of smart grids on real-time data exchange and interconnected systems makes them vulnerable to cyber-attacks such as False Data Injection (FDI) and Denial of Service (DoS). To address these challenges, the proposed methodology integrated Kalman filter-based state estimation with machine learning-driven anomaly detection techniques. This combination provided a robust and dynamic framework for detecting cyber-attacks and mitigating their impact on grid stability. The implementation on the IEEE 39-bus system demonstrated the practical effectiveness of these techniques. The results showed that the proposed approach could successfully detect and mitigate various forms of cyber-attacks while maintaining system stability and ensuring continuous grid operation. The Kalman filter's role in accurately estimating the system's state, even under compromised measurement data, proved vital in maintaining reliable control. Furthermore, the use of machine learning models enhanced the system's ability to detect anomalies in real-time, offering an additional layer of security against sophisticated attacks.

The integration of these techniques contributes to the ongoing effort to secure critical infrastructure like smart grids, where the consequences of successful cyber-attacks can be devastating. This research provides a pathway for improving resilience, reliability, and security in the face of evolving cyber threats. Future work could further refine these techniques by exploring more advanced machine learning models, improving detection accuracy, and enhancing response mechanisms. Additionally, extending the implementation to other complex grid models and incorporating real-time testing environments could help in generalizing the approach to broader applications within smart grid systems, thereby providing a comprehensive solution for the cybersecurity challenges facing modern energy infrastructures.

References

1. H.Zhang, Bo Liu, Hongyu Wu., "Smart Grid Cyber-Physical Attack and Defense: A Review", IEEE Access, Volume: 9, 2021.
2. M. S. Al-kahtani, and L. Karim, "A Survey on Attacks and Defense Mechanisms in Smart Grids," International Journal of Computer Engineering and Information Technology, vol. 11, no. 5, pp.94-100, 2019.
3. G.Liang, J.Zhao, F.Luo, R. Weller, Z.Y. Dong., "A Review of False Data Injection Attacks Against Modern Power Systems", IEEE Transactions on Smart Grid, Vol.8, Iss.4, 2017.
4. Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi. "Cyber-security in Smart Grid: Survey and Challenges," Computers and Electrical Engineering, vol. 67, pp.469-482, 2018.
5. M. Z. Gunduz, and R. Das, "Cyber-security on Smart Grid: Threats and Potential Solutions," Computer networks, Vol. 169, pp.107094, 2020.
6. Gupta, B.B. and Akhtar, T., "A Survey on Smart Power Grid: Frameworks, Tools, Security Issues, and Solutions", Annals of Telecommunications, Vol.72, pp.517-549, 2017.

7. Ye Yan, Yi Qian, H. Sharif, David Tipper., "A Survey on Cyber Security for Smart Grid Communications", IEEE Communications Surveys & Tutorials, Vol.14, Iss.4, 2012.
8. Md Usama, Md N.Aman., "Command Injection Attacks in Smart Grids: A Survey", IEEE Open Journal of Industry Applications, Vol.5, 2024.
9. K. Manandhar, X. Cao, Fei Hu, Yao Liu, "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter", IEEE Transactions on Control of Network Systems, Vol. 1, Iss. 4, 2014.
10. Y.Kim, S.Hakak, A.Ghorbani, "Smart grid security: Attacks and defence techniques", IET Smart Grid, Vol.6, pp.103–123, 2023.
11. D.E.Whitehead, K.Owens, Dennis G, J.Smith., "Ukraine cyber-induced power outage: analysis and practical mitigation strategies", In: Proc. Int. Conf. Protective Relay Engineers, pp. 1–8, 2017.
12. Al-kahtani, M.S. and Karim, L., "A Survey on Attacks and Defense Mechanisms in Smart Grids" International Journal of Computer Engineering and Information Technology, Vol.11, pp.94-100, 2019.
13. V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G.P. Hancke., "Smart grid technologies: communication technologies and standards", IEEE Trans. Ind. Inf., Vol.7(4), pp. 529-539, 2011.
14. J.Liu, Y.Xiao, S.Li, W.Liang., "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials", Vol.14, Iss.4, 2012.
15. Y.Li, J.Yan., "Cybersecurity of Smart Inverters in the Smart Grid: A Survey", IEEE Transactions on Power Electronics, Vol.38, Iss.2, 2023.
16. L.Kotut, L.A.Wahsheh., "Survey of cyber security challenges and solutions in smart grids", Cybersecurity Symposium (CYBERSEC), pp.32-37, 2016.
17. El Mrabet, Z., Kaabouch, N., El Ghazi, H. and El Ghazi, H., "Cyber-Security in Smart Grid: Survey and Challenges", Computers and Electrical Engineering, Vol.67, pp.469-482, 2018.
18. Peng, C., Sun, H., Yang, M. and Wang, Y., "A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks", IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol.49, pp.1554-1569, 2019.
19. He, H. and Yan, J., "Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. IET Cyber-Physical Systems: Theory & Applications", Vol.1, pp.13-27, 2016.
20. Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S. and Martin, A., "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues", Communications Surveys and Tutorials, Vol.21, pp.2886-2927, 2019.
21. A.O. Otuoze, M.W. Mustafa, R.M. Larik, "Smart grids security challenges: classification by sources of threats", J. Electr. Syst. Inf. Technol., Vol.5(3), pp. 468-483, 2018.
22. A.S.Musleh, G.Chen, Z.Y.Dong., "A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids", IEEE Transactions on Smart Grid, Vol.11, Iss.3, 2020.
23. S.Vahidi, M.Ghafouri, M.Au, M.Kassouf, Arash M, "Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities", IEEE Communications Surveys & Tutorials, Vol.25, Iss.2, 2023.
24. Mo, Yilin, Tiffany Hyun-Jin Kim, Kenneth Brancik, "Cyber–physical security of a smart grid infrastructure", Proc IEEE, Vol.100, pp.195-209, 2011.
25. M.H.Cintuglu, O.A. Mohammed, K.Akkaya, A.S.Uluagac., "A Survey on Smart Grid Cyber-Physical System Testbeds", IEEE Communications Surveys & Tutorials, Vol.19, Iss.1, 2017.
26. Alvin H., S.Mrdović, K.Bicakci, S.Uludag., "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid", IEEE Access, Vol.8, 2020.
27. N.Sahani, R.Zhu, J-H.Cho., "Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey", ACM Transactions on Cyber-Physical Systems, Vol. 7, No. 2, 2023.

28. J.Zhang, L.Pan, Q-L Han, C.Chen, Wen, Y.Xiang., "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey", IEEE/CAA Journal of Automatica Sinica, Vol.9, Iss.3, 2022.
29. P. Eder-Neuhauser, T. Zseby, J. Fabini, G. Vormayr, "Cyber-attack models for smart grid environments Sustain. Energy Grid", Sustainable Energy, Grids and Networks, Vol.12, pp. 10-29, 2017.
30. S.Tan, D.De, W-Z.Song, J.Yang, S.K.Das.: "Survey of Security Advances in Smart Grid: A Data Driven Approach", IEEE Communications Surveys & Tutorials, Vol.19, Iss.1, 2017.
31. X.Xia, Y.Xiao, W.Liang, Jiangtao Cui, "Detection Methods in Smart Meters for Electricity Thefts: A Survey", Proceedings of the IEEE, Vol.110, Iss.2, 2022.
32. R.Deng, G.Xiao, R.Lu, H.Liang, A.V. Vasilakos., "False Data Injection on State Estimation in Power Systems - Attacks, Impacts, and Defense: A Survey", IEEE Transactions on Industrial Informatics, Vol.13, Iss.2, 2017.
33. B.Rossi, S.Chren, "Smart Grids Data Analysis: A Systematic Mapping Study", IEEE Transactions on Industrial Informatics, Vol.16, Iss.6, 2020.
34. Chhaya, L,Sharma P, Bhagwatikar, G., Kumar, A., "Wireless sensor network based smart grid communications: Cyber-attacks, intrusion detection system and topology control", Electronics, Vol.6, Iss.5, 2017.
35. J.Xiao, L.Wang, Z.Qin, P.Bauer., "Detection of cyber-attack in smart grid: A Comparative Study", IEEE 20th International Power Electronics and Motion Control Conference (PEMC), 2022.
36. G Liang, S R Weller, J Zhao., "The 2015 ukraine blackout: Implications for false data injection attacks", IEEE Transactions on Power Systems, Vol. 32, no. 4, pp. 3317-3318, 2016.
37. R.Deng, G.Xiao, R.Lu., "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey", IEEE Transactions on Industrial Informatics, Vol.13, Iss.2, 2017.
38. Y Liu, P Ning and M K. Reiter, "False data injection attacks against state estimation in electric power grids", ACM Transactions on Information and System Security (TISSEC), Vol. 14, no. 1, pp. 1-33, 2011.
39. M.N.Kurt, O.Ogundijo, C.Li, X.Wang., "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach", IEEE Transactions on Smart Grid, Vol.10, Iss.5, 2019.
40. D.B. Rawat, C. Bajracharya., "Detection of False Data Injection Attacks in Smart Grid Communication Systems", IEEE Signal Processing Letters, Vol.22, Iss.10, 2015.
41. S.H.Mohammed, A.Al-Jumaily, M.S.Jit Singh, V.P.Gil Jiménez, A.S. Jaber, "A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid", IEEE Access, Vol.12, 2024.
42. Colak I, Sagiroglu S, Fulli G, Yesilbudak M, Covrig C., "A survey on the critical issues in smart grid technologies", Renewable and Sustainable Energy Reviews, Vol.54, pp.396–405, 2016.
43. N.Tatipatri, S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security", IEEE Access, Vol.12, 2024.
44. M.Necip Kurt, Y.Yılmaz, X.Wang, "Distributed Quickest Detection of Cyber-Attacks in Smart Grid", IEEE Transactions on Information Forensics and Security, Vol.13, Iss.8, 2018.
45. Dou An, F.Zhang, O.Yang, "Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures", IEEE Transactions on Automation Science and Engineering, Vol.19, Iss.3, 2022.
46. M.Amin, F.M.El-Sousy, G.A. Abdel Aziz, "CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review", IEEE Access, Vol.9, 2021.

47. S.Vahidi, M.Ghafouri, Minh Au, M.Kassouf, "Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities", IEEE Communications Surveys & Tutorials, Vol.25, Iss.2, 2023.
48. An, Y., Liu, D., "Multivariate Gaussian-Based False Data Detection against Cyber-Attacks", IEEE Access, Vol.7, pp.119804–119812, 2019.
49. Md Usama, Md N.Aman., "Command Injection Attacks in Smart Grids: A Survey", IEEE Open Journal of Industry Applications, Vol.5, 2024.
50. Wang, W.; Lu, Z., "Cyber Security in the Smart Grid: Survey and Challenges", Comput. Netw., Vol.57, pp.1344–1371, 2013.
51. Qi Liu, V.Hagenmeyer, H.B.Keller, "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids", IEEE Access, Vol.9, 2021.
52. U.Adhikari, Thomas Morris, Shengyi Pan., "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining", IEEE Trans. Smart Grid, Vol. 8(6), pp.2744–2753, 2016.
53. Dou An, Q.Yang, W.Liu, and Y. Zhang., "Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach", IEEE Access, Vol.7, pp.110835–110845, 2019.
54. Fazel Mohammadi., "Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review", Energies, Vol.14(5), p.1380, 2021.
55. Aoufi, S., Derhab, A., Guerroumi, M., "Survey of False Data Injection in Smart Power Grid: Attacks, Countermeasures and Challenges", J. Inf. Secur. Appl. Vol.54, p.102518, 2020.
56. Kurt, M.N., Ogundijo, O., Li, C., Wang, X., "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach", IEEE Trans. Smart Grid, Vol.10, pp.5174–5185, 2019.
57. Moslemi, R., Mesbahi, A., Velni, J.M., Fast, A., "Decentralized Covariance Selection-Based Approach to Detect Cyber Attacks in Smart Grids", IEEE Trans. Smart Grid, Vol.9, pp.4930–4941, 2018.
58. Zhao, J., Mili, L., Wang, M., "A Generalized False Data Injection Attacks against Power System Nonlinear State Estimator and Countermeasures", IEEE Trans. Power Syst, Vol.33, pp.4868–487, 2018.
59. Deng, R., Zhuang, P., Liang, H., "False Data Injection Attacks Against State Estimation in Power Distribution Systems", IEEE Trans. Smart Grid, Vol.10, 2871–2881, 2019.
60. J-J Yan, G-H Yang, Yu Wang., "Dynamic Reduced-Order Observer-Based Detection of False Data Injection Attacks with Application to Smart Grid Systems", IEEE Transactions on Industrial Informatics, Vol. 18, Iss. 10, 2022.