Review

Cybersecurity and Major Cyberthreats of Smart Meters: A Systematic Mapping Study

Jones Márcio Nambundo *, Otávio S. M. Gomes, Adler Diniz de Souza, Raphael Carlos Santos Machado

Posted Date: 18 February 2025

doi: 10.20944/preprints202502.1399.v1

Keywords: smart meters; CyberSecurity; CyberThreats; smart grids; vulnerabilities

Article

Cybersecurity and Major Cyberthreats of Smart Meters: A Systematic Mapping Study

Jones Márcio Nambundo [1,*,†], Otávio S. M. Gomes [1,†], Adler Diniz de Souza [2,†] and Raphael Carlos Santos Machado [3,†]

[1] Postgraduate Program in Electrical Engineering, Federal University of Itajubá (UNIFEI), Avenida BPS, 1303, Pinheirinho – 37540-903 – Itajubá, MG, Brazil
[2] Postgraduate Program in Science and Technology of Computing, Federal University of Itajubá (UNIFEI), Avenida BPS, 1303, Pinheirinho – 37540-903 – Itajubá, MG, Brazil
[3] Clavis Segurança da Informação, R. Aloísio Teixeira, 278 - Prédio 3 - Sala 307 – 25250050 - Rio de Janeiro, RJ, Brazil
* Correspondence: jonesnambundo@hotmail.com
† These authors contributed equally to this work.

Abstract: Smart meters are a vital part of the smart grid, enabling energy management, real-time control, and data collection. Despite advances in technology, there is still a lack of content and limited understanding of the specific cybersecurity threats facing these devices, as well as the effectiveness of existing mitigation strategies. This study analyzed 41 articles sourced from three academic databases (Scopus, Web of Science and IEEE Xplore). A cutting-edge study was conducted, including a comprehensive review of relevant literature on smart meters, cybersecurity vulnerabilities, and mitigation strategies. Elements were selected based on pre-assessment and classification processes, and the data were extracted and combined to provide detailed insights into the new devices. The study identified several significant cybersecurity risks for smart meters, including data breaches, unauthorized access, data manipulation, denial of service (DoS) attacks, and malware introduction. The study also highlighted the vulnerabilities exploited by these threats, such as undocumented communications, weak authentication, and outdated software. Recommended mitigation strategies include strengthening access and authentication mechanisms, securing communication systems, regular software updates, code management, anomaly detection, and access control. The findings indicate that, although there are good strategies and methods to mitigate these cyber threats, significant research gaps remain. These gaps include design requirements, software and firmware updates, physical security, the use of big data to detect vulnerabilities, user data privacy, and inconsistencies in machine learning algorithms. Future research should focus on these aspects to improve the stability and reliability of smart meters.

Keywords: smart meters; CyberSecurity; CyberThreats; smart grids; vulnerabilities

1. Introduction

Advances in technology and the digitalization of energy systems have made smart grids an innovative strategy to to maximize the amount of electricity consumed and distributed. While technological advancements and the digitalization of energy systems are promising, there are also technical challenges. One of these challenges is cybersecurity, especially when it comes to protecting the data generated by smart meters. Smart meters collect detailed information about energy use. This information is useful for improving distribution and efficiency, but it can also be an attractive target for cybercriminals. Therefore, protecting this information is very important. That's why protecting this sensitive information is of utmost importance. The expectation is that the use of smart meters by the end of 2023 will become increasingly more of a priority. There are around 29.5 million smart meters in operation in the UK [1]. In the United States, the number is even higher, with around 128 million smart meters by the end of 2023. But this technological advancement is not without competition.

Cybersecurity has become a major issue, especially when it comes to protecting data collected by smart meters. The relationship between various devices and systems also poses significant problems.

 doi:10.20944/preprints202502.1399.v1

The lack of common standards can hinder effective communication between different devices and systems. Connecting these devices to networked communications exposes systems to multiple threats and highlights the importance of a secure cybersecurity strategy to ensure data integrity and known and owned privacy [3]. The introduction of smart meters represents a major advancement in energy consumption management and monitoring, providing a detailed overview of electricity consumption in real time. However, collecting and transmitting sensitive data through these devices creates vulnerabilities that can be exploited by hackers. Therefore, adequately protecting this information becomes an urgent task to ensure the reliability and security of the smart grid [4].

The systematic mapping study of cyberthreats to smart meters in smart grids is proposed in this paper. The major objectives are to identify the most significant cyberthreats to smart meter data, examine advanced metering infrastructure vulnerabilities that could be used in cyberattacks, evaluate the efficacy of cybersecurity protocols and measures, identify areas in need of more research, and identify gaps in the body of existing literature.

The work was structured into seven sections. Section 2, Related Work, reviewed previous research on the topic. Section 3 described the Research Methodology, including the criteria used to select and compare different articles. Section 4 presented and discussed the Main Findings. Section 5 addressed the Research Questions. Section 6 identified Gaps and suggested Future Research Directions. Finally, Section 7 concluded the paper by recapping the Principal Results.

2. Related Works

Different research on Systematic Mapping Studies (SMS) and Systematic Literature Reviews (SLRs) has been conducted in the field of cybersecurity for smart meters. In this section, we review relevant studies that address similar topics.

As mentioned in [5], it addresses cybersecurity vulnerabilities in smart grids, highlighting risks such as user awareness deficiencies and unauthorized access. It proposes mitigation techniques, including consumer education, system protection, and multi-factor authentication. The conclusion emphasizes the need for a collaborative approach to tackle security challenges during the transition to smart grids.

In [6], a literature review is conducted on key technologies for vulnerability mitigation, such as Cyber Threat Intelligence (CTI) sharing platforms, Artificial Intelligence, Natural Language Processing (NLP), detection and visualization models. It also discusses the use of risk assessment and management architectures, where semantic languages are used for threat information exchange, helping with dynamic risk assessment and improving vulnerability management.

In [7] presents an innovative solution that combines advanced cryptography and blockchain technology to strengthen the security and reliability of smart grids, addressing existing vulnerabilities and preparing the infrastructure for a more decentralized and secure future. The solution utilizes a hybrid authentication and handshake algorithm (BSHAHA), which employs both symmetric and asymmetric cryptography. BSHAHA demonstrates itself to be a robust solution for authentication and data security in smart grids.

The paper [8] does not single out one solution as best for all smart grid security scenarios, but emphasizes the importance of an integrated approach that incorporates multiple technologies and practices. Among the highlighted solutions, the use of blockchain, artificial intelligence (AI), and advanced encryption systems are often mentioned as effective methods for enhancing the security and resilience of smart grids. These technologies help ensure data integrity and security, detect abnormal attack patterns, and respond swiftly to cybersecurity incidents.

In [9] , the focus is on irregularities in smart meters, examining weaknesses such as data protection, errors caused by incorrect data entry, and inaccuracies that result in a lack of consistent data. To reduce these problems, it is suggested to review old data to detect significant discrepancies, and to apply machine learning models to interpret numerical data and discover atypical patterns.

 doi:10.20944/preprints202502.1399.v1

The paper in [10] addresses the concept of anomie as it relates to smart grids, focusing on the interplay between physical and network systems. This interoperability exposes the grid to cyber threats, including false data injection (FDI) attacks that can undermine the integrity of information processed by state estimation (SE) systems. To mitigate these vulnerabilities, the study recommends employing techniques for intrusion detection and localization, such as convolutional neural networks (CNN), alongside bad data detectors (BDD). In [11], a CTI model was proposed to enhance the security of an organization's core processes and strategies using AI, blockchain, and multi-factor authentication. The goal is to develop a robust organization against threats and encourage continuous information sharing to enhance security.

In [12] paper highlights the vulnerabilities in smart grids and suggests the implementation of technological strategies to mitigate these risks. The use of algorithms based on tree structures is emphasized, as they significantly improve the detection of attacks, allowing for more effective responses. The study also recommends the implementation of robust encryption and authentication mechanisms, aimed at preventing unauthorized access and data manipulation, ensuring the integrity and confidentiality of the information.

The paper in [13] focuses on detecting cyberattacks aimed at energy theft in renewable energy sources. To do this, it uses deep learning tools to combine data from smart meters, weather forecasts, and SCADA systems. This approach forces consumers to use smart meters, enabling them to report more accurate energy consumption. The mitigation process involves the use of deep neural networks, such as recurrent and convolutional networks, achieving a 99.3% detection rate and a 0.22% false negative rate. In [14], security and privacy threats are reviewed, and conventional and machine learning-based supervised and unsupervised countermeasures are discussed to identify patterns and anomalies indicating threats.

In [15], propose a robust design with multiple layers of security to safeguard against attacks, ensure data integrity, and prevent energy theft. The solution employs LoRaWAN, an ideal technology for IoT applications that prioritize energy efficiency and wide coverage, due to its long range and low power consumption. Security is significantly enhanced with the use of AES encryption, an advanced standard that protects information against unauthorized access. In addition, we have implemented unidirectional data transmission, a strategy that makes data interception and manipulation difficult, as the flow of information occurs in only one direction, making it more complex for an attacker to insert themselves into the communication. The system is also designed to mitigate Distributed Denial of Service (DDoS) attacks, which aim to destabilize the network by overloading devices with excessive traffic

3. Research Methodology

This research adhered to the guidelines outlined in [16] for conducting a SMS. The decision to use this method was motivated by a number of factors. It offers a structured and methodical approach to identifying, evaluating, and interpreting all pertinent studies pertaining to a specific research question, focus area, or phenomenon of interest. A SMS is a clearly defined and methodical method for reviewing and analyzing empirical evidence related to a particular method or technique, pinpointing existing research gaps and areas, and supplying the foundational knowledge necessary to guide future research endeavors for scholars or practitioners. In contrast to traditional literature reviews, systematic mapping studies demand more time and effort; however, they yield a more profound comprehension of the subject matter and a more robust groundwork for formulating research inquiries [17]. A standard systematic mapping research protocol typically involves five distinct stages:

1. Formulation of research questions.
2. Definition of the search process and search string.
3. Definition of the study selection process, including inclusion and exclusion criteria.
4. Extract data and map data to specific research questions.
5. Data analysis and results extraction.

 doi:10.20944/preprints202502.1399.v1

3.1. Definition of Research Questions

The first step in conducting a SMS is defining the research questions. This process is crucial for ensuring the appropriate selection of relevant articles. The aim of this study is to explore the cyber threats, vulnerabilities, and cybersecurity measures related to smart meter data within smart grids. With these objectives in mind, the following research questions were formulated to guide the study:

- QP1: What are the main cyberthreats to smart meter data in smart grids?
- QP2: What vulnerabilities in smart meter infrastructure can be exploited by cyber attacks?
- QP3: What are the common strategies and technologies used to mitigate cybersecurity risks in smart grids?
- QP4: What are the current research gaps in cybersecurity for smart meter data?

The first research question is to begin collecting information from the newspaper about the types of cybersecurity threats in order to determine which one is the most threatening in response to QP1 Subsequently, the second research question focuses on vulnerabilities within smart meter infrastructure that can be exploited by cyber attacks, aiming to identify the most susceptible areas to threats. The third research question evaluates the effectiveness of current cybersecurity measures and protocols in protecting smart meter data. This analysis aims to highlight practices that are working well and identify areas for improvement. The fourth research question aims to identify gaps in current research and suggest areas for future research, thereby providing further directions for research in this rapidly developing field. Finally, the fifth research question offers recommendations to enhance cybersecurity for smart meter data in smart grid networks, ensuring robust protection against emerging threats.

3.2. Seach Protocol and Selection

To conduct an effective systematic review, it is essential to establish a robust search protocol and clear article selection criteria. This protocol needs to be carefully outlined to ensure the inclusion of pertinent and high-quality studies. In this study, the PICOC strategy (Population, Intervention, Comparison, Outcome, Context) will be adopted to guide the search and selection process, as detailed below:

- **Population**: Smart meters used in smart grids.
- **Intervention**: Cybersecurity measures and strategies implemented to protect data.
- **Comparison**: Comparison of different cybersecurity strategies and their effectiveness.
- **Outcome**: Identification of threats, vulnerabilities, effectiveness of security measures, and research gaps.
- **Context**: Cybersecurity in the context of smart grids.

The research was done in the Scopus, Web of Science, and IEEE Xplore chosen for their comprehensiveness and relevance in the fields of technology and cybersecurity. The search string is specific to ensure comprehensive and targeted article collection, as shown in Table 1.

These search strategies were chosen to ensure the inclusion of relevant studies published over a 10-year period from 2013 to 2024. The article selection process will be conducted in several stages. Initially, a preliminary search will be conducted to identify all potentially relevant articles. Next, the titles and abstracts of these articles will be reviewed for initial screening, eliminating those that are clearly unrelated to the research questions. The remaining articles will be fully assessed for relevance and methodological quality. Inclusion and exclusion criteria will be applied rigorously as shown in Table 2 and Table 3. Inclusion criteria encompass articles published in peer-reviewed journals or recognized conferences. Opinion articles, non-peer-reviewed studies, and non-academic publications will be excluded.

 doi:10.20944/preprints202502.1399.v1

Table 1. Repositories and Search String.

Repositories	Search String
Scopus	TITLE-ABS-KEY ((“smart meters” AND cybersecurity) OR (“smart meters” AND “cyber threats”) OR (“smart grids” AND cybersecurity) OR (“smart meters” AND vulnerabilities”)) AND PUBYEAR > 2013
Web of Science	(“smart meters” AND cybersecurity) OR (“smart meters” AND “cyber threats”) OR (“smart grids” AND cybersecurity) OR (“smart meters” AND vulnerabilities)
IEEE Xplore	(“smart meters” AND cybersecurity) OR (“smart meters” AND “cyber threats”) OR (“smart grids” AND cybersecurity) OR (“smart meters” AND vulnerabilities)

Table 2. Set of Inclusion Criteria.

Criteria	Description
CI-01	Articles focused on the cybersecurity aspects of smart meter data
CI-02	Articles addressing cybersecurity in smart grids
CI-03	Studies published in peer-reviewed journals or conferences
CI-04	Research discussing threats, vulnerabilities, and mitigation strategies
CI-05	Publications from the last 10 years to ensure relevance

Table 3. Set of Exclusion Criteria.

Criteria	Description
CE-01	Duplicate Articles
CE-02	Articles not specifically focused on smart meters
CE-03	Articles not related to cybersecurity of smart meter data
CE-04	Articles not focusing on smart grid cybersecurity
CE-05	Publications older than 10 years

The initial search resulted in a total of 2,910 articles, distributed across the IEEE (1,161 articles), Scopus (1,352 articles), and Web of Science (397 articles) repositories. This resulted in many duplicates and false positives, as shown in Table 4.

Table 4. Summary of the Article Selection Process.

Accepted	Rejected	Duplicate	Selected
291	1,219	1,400	41

Next, specific inclusion and exclusion criteria were applied, as illustrated in Figure 1, reducing the set to 41 selected articles. This search reflects the necessary comprehensiveness to capture a full spectrum of research related to the topic. However, the application of rigorous inclusion and exclusion criteria was essential to ensure the relevance and quality of the studies considered in the final analysis. The process of reducing the number of articles followed a structured protocol, which included screening titles and abstracts, followed by a full reading of the remaining articles. During this initial screening, many articles were excluded (rejected) for not directly addressing the research questions or for presenting redundant studies or studies of lower methodological quality. Additionally, it was crucial to conduct a qualitative assessment of the selected articles to ensure that only relevant studies were retained and contributed to the objectives of the SMS. Our objective scoring system

 doi:10.20944/preprints202502.1399.v1

ensured a fair and transparent selection process, resulting in 41 articles representing the most relevant and methodologically sound research. This rigorous approach reduced the number of studies and strengthened the foundation of the conclusions.

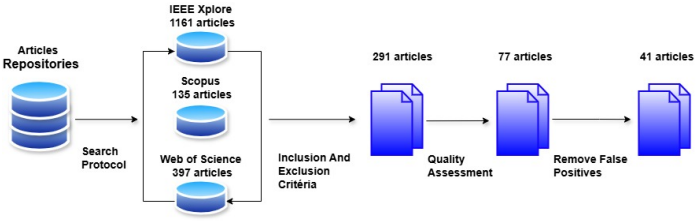

Figure 1. Search methodology used for systematic mapping.

To ensure the quality and reliability of the selected articles, we conducted a rigorous quality assessment process. This assessment focused on the relevance of the work to the research field. We asked ourselves:

- Does this article significantly contribute to advancing knowledge in the area of study?
- Publication in a relevant journal or conference: Was the article published in a prestigious journal or conference recognized in the field of study?

These questions helped ensure that only the most relevant and reliable articles were considered in the final analysis.

3.3. Data Extration

After selecting 41 papers included in this study, data extraction was conducted to answer the original research questions. The main information extracted is as follows:

- Study title
- Authors
- Publication year
- Objectives
- Methodology
- Key findings
- Cybersecurity threats identified
- Security measures discussed
- Effectiveness of measures
- Identified gaps
- Recommendations

Each category of information was carefully documented to allow for detailed analysis and comprehensive synthesis of the data. This meticulous process ensures that all research questions are addressed thoroughly and accurately, providing a solid foundation for the conclusions and recommendations of this study. The selected articles are placed in the Table 5 where we can see their name and publication year.

Table 5. Articles selected through systematic Mapping of Literature.

Title	Ref	Year
A review of anomaly detection techniques in advanced metering infrastructure	[18]	2020
A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence	[19]	2024
A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security	[20]	2024

 doi:10.20944/preprints202502.1399.v1

Table 5. *Cont.*

Title	Ref	Year
A Deep Learning Framework to Identify Remedial Action Schemes Against False Data Injection Cyberattacks Targeting Smart Power Systems	[21]	2024
A Novel Approach for Detection of Cyber Attacks in Microgrid SCADA System	[22]	2023
A Novel False Data Method Targeting on Time-Series in Smart Grid	[21]	2023
A Review of Cyber–Resilient Smart Grid	[23]	2022
A Review of Features, Vulnerabilities, Cyber-Attacks and Protective Actions in Smart Grid Systems	[24]	2023
A Review of Various Modern Strategies for Mitigation of Cyber Attacks in Smart Grids	[25]	2019
A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems	[26]	2017
A Survey on Smart Grid Metering Infrastructures: Threats and Solutions	[27]	2015
Analyzing Attack Resilience of an Advanced Meter Infrastructure Reference Model	[28]	2016
Anomaly Detection in Smart Meters: Analytical Study	[29]	2022
Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks	[30]	2015
Cyber Security Vulnerabilities of Smart Metering Based on LPWAN Wireless Communication Technologies	[31]	2020
Real-Time Detection of Cyber-Attacks in Modern Power Grids with Uncertainty using Deep Learning	[32]	2022
Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges	[33]	2018
Security Aspects in Smart Meters: Analysis and Prevention	[34]	2020
Smart Meter Vulnerability Assessment Under Cyberattack Events – An Attempt to Safeguard	[35]	2023
Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures	[36]	2019
Using Smart Meter Data to Predict and Identify Consumer Vulnerability	[37]	2023
Cyber-Physical Vulnerability Assessment in Smart Grids Based on Multilayer Complex Networks	[38]	2021
Invasion Analysis of Smart Meter in AMI System	[39]	2021
Smart Meter Data Privacy: A Survey	[40]	2017
Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism	[41]	2017
Simulation of SCADA System for Advanced Metering Infrastructure in Smart Grid	[42]	2020
Intrusion Detection Tool for Residential Consumers Equipped with Smart Meters	[43]	2023
Smart Meters: Cyber Security Issues and Their Solutions	[44]	2023
Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection	[45]	2023
Intrusion Detection System for Smart Meters	[46]	2020
Semi Supervised Cyber Attack Detection System for Smart Grid	[47]	2022
Security and Privacy Challenges, Solutions, and Open Issues in Smart Metering: A Review	[48]	2021
Securing the Smart Grid: A Comprehensive Analysis of Recent Cyber Attacks	[49]	2024
Smart Meter Data Analytics for Load Prediction using Extreme Learning Machines and Artificial Neural Networks	[50]	2019
Cyber Security Enhancement of Smart Grids via Machine Learning - A Review	[51]	2020
Cybersecurity Threats, Detection Methods, and Prevention Strategies in Smart Grid: Review	[52]	2023
Smart Meter Modbus RS-485 Intrusion Detection by Federated Learning Approach	[53]	2023
Non-Intrusive Load Monitoring based Demand Prediction for Smart Meter Attack Detection	[54]	2021
Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges	[55]	2012
Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)	[56]	2022

 doi:10.20944/preprints202502.1399.v1

4. Results

4.1. Cyber Threats and Vulnerabilities in Smart Meters in Smart Grids

In this section, the main findings obtained after reviewing the selected articles in Section 2 will be discussed. An initial analysis identified the primary cyber threats and vulnerabilities, comparing their frequency across the selected articles for this systematic mapping. Various cybersecurity threats and security vulnerabilities were discussed, as illustrated in Tables 6 and 7. Threats are actions aimed at taking advantage of security flaws in a system, causing negative impacts. As shown in [27] analyzes the main threats to advanced measurement infrastructures in smart grids and the solutions proposed to mitigate them. Threats include physical attacks, network attacks (such as DoS and eavesdropping), data integrity attacks, and privacy attacks. Physical attacks involve direct manipulation of smart grid hardware components. This could include damage to smart meters, data concentrators or communications links. The impact of physical attacks can be significant, as they can disrupt the flow of information and lead to incorrect billing or even service interruptions.

Table 6. Cyber Threats.

Threats	References
Data tampering/manipulation	[18,21,23,36,38,41]
Unauthorized access	[18,27,29,36,38]
Privacy breaches	[18,22,28,36]
Denial of Service (DoS) / Distributed DoS (DDoS)	[26,29,37,44]
Malware	[19,32,37]
Phishing	[37]
Insider threats	[32,39]
Advanced persistent threats (APTs)	[20,39]
Cyber espionage	[25,40]
Ransomware	[25,40]
Intrusion attacks	[31,34,41]
False data injection	[21,29,41]
Eavesdropping	[19,42]
Replay attacks	[19,42]
Energy theft	[22,43]
Data spoofing	[43]
Machine learning model attacks	[32,45]
Data poisoning	[32,45]
Cyber–Physical attacks	[20,26]
SCADA attacks	[22,25,30]

A vulnerability is a flaw in a system or its design that allows malicious actors to execute unauthorized commands, access confidential information, or perform denial of service attacks. Such breaches enable attackers to exploit electronic data, potentially tracking customer behavior and compromising their privacy.

Figure 2 shows the main cyber threats (PQ1) identified in the systematic mapping study. The first column in the table outlines the most prevalent threats, where "Data tampering/manipulation" appeared in 91.67% of the studies, followed by "Unauthorized access" in 75.00%, and "Privacy breaches" in 58.33%. Data manipulation can have devastating consequences, including falsification of energy consumption readings. Unauthorized access poses a significant risk as attackers can remotely control the advanced metering infrastructure.

 doi:10.20944/preprints202502.1399.v1

Table 7. Vulnerabilities in Advanced Metering Infrastructure.

Vulnerabilities	References
Weak encryption	[18,19,36,42]
Poor authentication mechanisms	[18,22,36]
Insecure communication protocols	[19,37,41]
Outdated software	[19,37]
Insufficient data protection	[18,26,38]
Lack of access control	[18,32,38,43]
Insider access	[20,39]
Lack of anomaly detection	[21,34,39,43]
Unpatched systems	[20,40]
Weak network security	[19,40]
Insecure Modbus protocol	[41]
Lack of intrusion detection systems (IDS)	[34,41]
Insufficient monitoring	[42]
Insecure network architecture	[20,44]
Lack of redundancy	[44]
Model bias	[45]
Insufficient model robustness	[45]

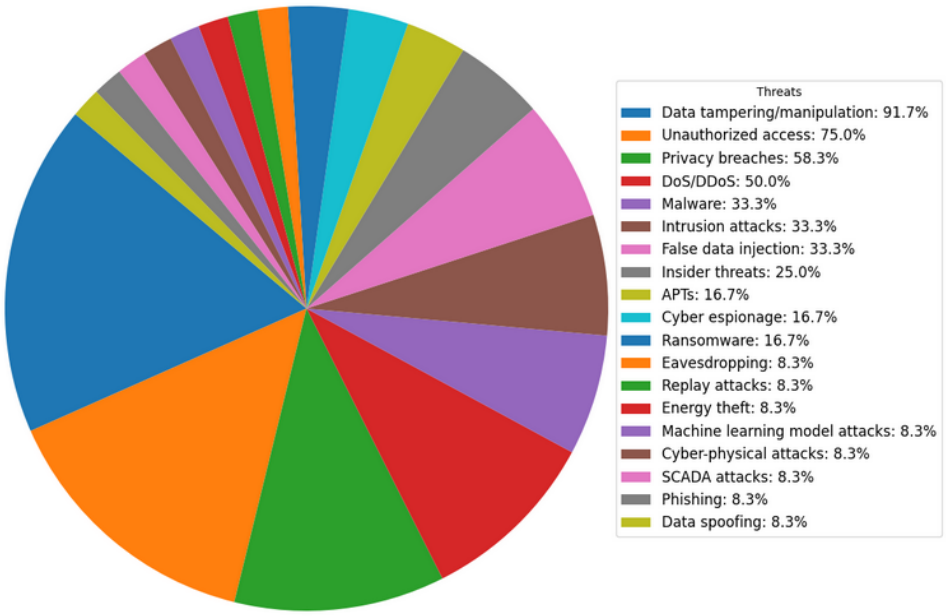

Figure 2. Most Frequent Threats in Articles.

Figure 3 shows the main security vulnerabilities of advanced metering infrastructures (PQ2) identified in the systematic mapping study. Column 1 of the table lists the most frequent vulnerabilities, with "Weak encryption" standing out at 58.33%. This vulnerability is highlighted as the most common, indicating that many smart meter systems may be vulnerable to attacks due to the use of weak encryption algorithms or inadequate implementation of encryption to protect sensitive data. "Poor authentication mechanisms" is present in 50.00% of the articles, suggesting that many smart meters may not have robust methods to properly verify and authenticate the identity of users and devices accessing the system. "Insecure communication protocols," appearing in 41.67% of the articles, points to the use of communication protocols that are not adequately secure, leaving transmitted data vulnerable to interception and manipulation by attackers.

 doi:10.20944/preprints202502.1399.v1

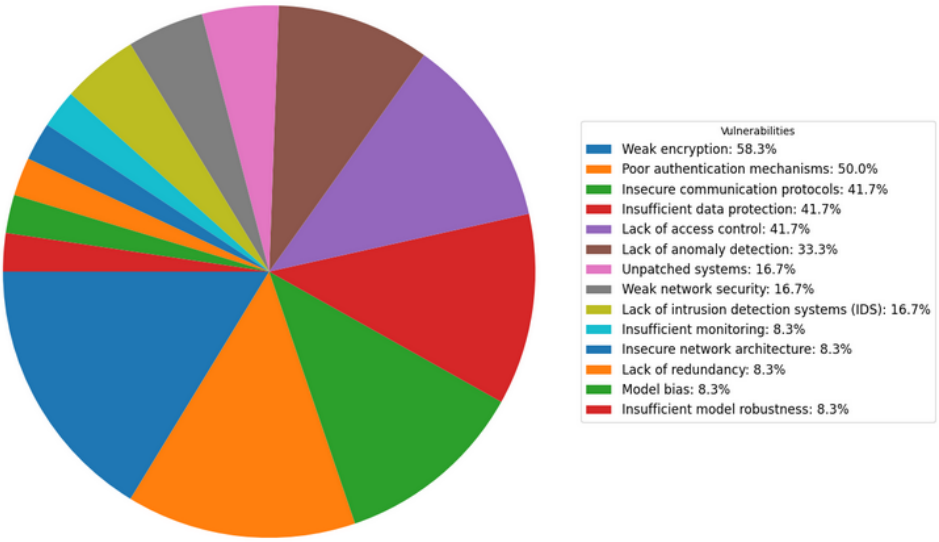

Figure 3. Most Frequent Vulnerabilities in Articles.

4.2. Attack Mitigation Techniques

Attack mitigation techniques in smart grids, as presented in Table 8, are crucial for protecting advanced metering infrastructure from threats and vulnerabilities. Several articles propose solutions to mitigate risks such as False Data Injection Attacks (FDIA), Denial of Service (DoS) attacks, data manipulation in smart meters, and SCADA system invasions. For FDIA, deep learning models are used to detect anomalies in real-time, while network segmentation and redundant systems limit the impact of DoS attacks. Data manipulation in smart meters is mitigated using machine learning techniques and intrusion detection tools. In the case of SCADA systems, multilayer networks and semi-supervised detection prevent invasions. Additionally, smart meter data privacy is protected through anonymization and encryption techniques. These strategies, listed in Table 8, address critical vulnerabilities in smart grids, enhancing security and aligning with the cybersecurity risk mitigation strategies outlined in QP3.

These mitigation techniques range from traditional methods such as encryption and authentication mechanisms to more advanced approaches such as using machine learning and neural networks for anomaly and intrusion detection. In [34] proposes preventive measures for security aspects in smart meters, including the use of encryption to protect sensitive data and ensure the integrity of communications in the smart metering infrastructure. In [30] emphasizes the importance of securely managing cryptographic keys, continually educating employees on cybersecurity practices, and creating an organizational culture focused on security awareness. These measures are designed to maintain integrity, take measures in smart plans, ensure reliability in operations, and ensure management of important information.

Table 9 summarizes some of the deep learning and machine learning techniques that have proven effective in detecting anomalies and intrusions in smart grids. This table is a useful tool for comparing different DL and ML methods and understanding the most commonly used methods in the smart grid field. Each method has its own strengths and limitations, and the choice of method can vary depending on the type of data and the specific problem being solved.

Various flaw detection methods, including statistical approaches, machine learning algorithms, and data analysis techniques, are discussed in [18]. These methods are employed to identify anomalies in the data collected by Advanced Metering Infrastructure (AMI) systems, ensuring data integrity and security. In [27], various techniques are being studied to mitigate threats to advanced accounting infrastructure. These include encryption and digital signatures to ensure the security and authenticity of measurement data. It also discusses advanced anomaly detection techniques to identify unusual patterns that may indicate attacks or failures. Network segmentation is also considered a containment

 doi:10.20944/preprints202502.1399.v1

measure to protect critical parts of the infrastructure while exposing them to potential attacks. This combined strategy aims to increase the resilience of smart networks to cyber and operational threats.

Table 8. Mitigation Techniques Used in Different Articles.

Mitigation Techniques	Articles
Encryption	[18,23,24,28,31,37,42]
Authentication mechanisms	[18,22,24,26,27,30,33,45]
Secure communication protocols	[19,23,30,33,37,41]
Software updates	[19,32,37,40,45]
Data protection	[18,22,25,26,31,34]
Access control	[18,25,27,32,36,43]
Anomaly detection	[21,23,34,39,43,44,49]
Patching systems	[20,29,40]
Network security	[19,28,33,40,45]
Intrusion detection systems (IDS)	[21,27,34,41,44]
Monitoring systems	[31,36,42,49]
Network architecture	[20,26,33,44]
Redundancy	[23,29,44]
Model robustness	[31,34,45]
Bias mitigation in models	[31,34,45]

Table 9. Effective Deep Learning and Machine Learning Techniques for Detecting Anomalies and Intrusions in Smart Networks.

Techniques	Description	Articles
Deep Learning (DL)	Algorithms that learn hierarchical data representations, capable of identifying complex patterns and anomalies.	[18,21,28,35]
Machine Learning (ML)	An algorithm that can learn from data and make predictions or decisions independently.	[25,27,35,53]
Convolutional Neural Networks (CNN)	CNNs and neural networks that excel at processing image and time-series data, identifying patterns across space and time.	[34,41,46,47]
Autoencoders	Autoencoders and neural networks used in unsupervised learning are adept at compressing data and detecting anomalies.	[18,23,31]
Support Vector Machines (SVM)	Classification algorithms that identify the best hyperplane to separate different classes in a dataset.	[26,31,40,44]
Random Forest	An ensemble of decision trees that work together for classification and regression, being resistant to overfitting and efficient with large datasets.	[22,24,30,39]
Recurrent Neural Networks (RNN)	Neural networks designed to process sequential data, used to detect patterns in time series.	[20,29,33,37]

5. Discussion

The results and answers to the research questions in Chapter 3 are discussed below.

QP1: What are the main cyberthreats to smart meter data in smart electrical grids?

The main cybersecurity threats to smart meter data in smart grids, as presented in table 6, were identified based on a systematic review of several articles. These threats can significantly compromise the security and efficiency of these networks. Among the most highlighted threats in the selected articles, four stand out: Data tampering/manipulation with 91.67. Unauthorized access with 75% frequent in articles, Privacy leaks: with 58.33% Denial of Service (DoS) / Distributed Denial of Service (DDoS): with 50.00%. These threats were selected from several discussed in the articles reviewed, standing out for their potential impact and the frequency with which they were mentioned in the

 doi:10.20944/preprints202502.1399.v1

literature. The systematic analysis reinforces the importance of mitigating these threats to ensure the security and efficiency of smart grids.

QP2: What vulnerabilities in smart meter infrastructure can be exploited by cyber attacks?

Based on the frequency of occurrence identified in the reviewed articles, and as shown in the Tables 6 and 7 analyzing the frequent data, it is clear that vulnerabilities in smart meter infrastructure represent serious security risks cybernetics. The high incidence of issues related to weak encryption, poor authentication, insecure communication protocols, and inadequate data protection reflects the widespread vulnerability of these systems. These issues are discussed in multiple studies due to their critical importance for the integrity and security of data in smart meters. Therefore, mitigating these vulnerabilities is essential to protect these systems against potential cyberattacks and ensure the reliability of smart grids.

QP3: What are common strategies and technologies used to mitigate cybersecurity risks in smart grids?

To answer this question about common strategies and technologies used to mitigate cybersecurity risks in smart electrical grids, considering the data provided by the selected articles summarized in the Table 8 and 9. Common strategies include using advanced deep learning techniques (such as Convolutional Neural Networks and Autoencoders) and machine learning (such as Support Vector Machines and Random Forest) for anomaly detection and prediction of anomalous behavior.

Encryption is crucial for protecting sensitive data, and vulnerability analysis, anomaly detection, and thorough security testing are essential methods for identifying and addressing weaknesses before they are exploited by cyberattacks. For example, one of the major vulnerabilities in smart grids is false data injection (FDIA), as discussed in [20]. This type of attack can severely compromise the integrity and operation of energy systems. To mitigate this threat, we can implement deep learning methods described in [21] and [41]. In this study, we propose creating a model that learns common data patterns and detects anomalies that indicate attacks, which can identify and mitigate FDIA attacks in real time. Another important vulnerability is the vulnerability of the power grid to Denial of Service (DoS) attacks, as detailed in [23]. These attacks can disrupt the control and communication systems. To address this issue, [25] proposes network segmentation and defense-in-depth techniques to limit the impact of such attacks, while [49] proposes the use of redundant networks and the implementation of a fast recovery system to improve resilience against DoS attacks, minimizing downtime and damage. Furthermore, manipulation of metering data from smart meters is a significant vulnerability, as discussed in [34]. To mitigate this vulnerability, [18] proposes the implementation of machine learning and statistical anomaly detection methods that can identify anomalous patterns in measurement data. Complementing this approach, [43] proposes developing a dedicated intrusion detection tool for smart meters that monitors data traffic and detects manipulation attempts in real time. Some mitigation solutions have been proposed in the literature regarding intrusions and manipulations of SCADA systems in microgrids, as discussed in [22]. For instance, [38] suggests the evaluation of cyber and physical vulnerabilities through complex multilayer networks, identifying critical points that require additional protection to prevent intrusions. Similarly, [47] proposes the development of semi-supervised detection systems that combine supervised and unsupervised machine learning to identify intrusion attempts in SCADA systems of microgrids.

Finally, the exposure to privacy attacks in smart meters, as reviewed in [40], is a growing concern. To mitigate this vulnerability, [33] suggests the implementation of data anonymization and aggregation techniques, which protect user privacy by preventing direct association between the collected data and specific individuals. Additionally, [48] proposes the use of advanced encryption and access control techniques to ensure that only authorized users can access measurement data, thereby protecting consumer privacy.

QP4: What gaps exist in current research on the cybersecurity of smart meter data?

 doi:10.20944/preprints202502.1399.v1

Analyzing the previous questions and the data provided by the Tables 6, 7 and 8 (QP4) of the articles selected in the systematic mapping, we identified some gaps in current research on the cybersecurity of smart meter data such as:

Efficiency and Scalability: Many cybersecurity techniques are computationally intensive, which can limit their applicability to large smart meter networks. It is necessary to develop more efficient and scalable methods to deal with the growing volume of data generated by these systems. in [19] explores the efficiency and scalability of these approaches, crucial for dealing with the complexity and volume of data generated by smart grids. Furthermore, the article discusses the application of these techniques in real scenarios, highlighting their practical advantages and limitations. [19] Real-Time Detection: The ability to detect real-time anomalies and intrusions in meter data is crucial to mitigating damage to the electrical grid.

As seen in [20], this research is important and reflects the importance of today's thinking about the critical security issues facing modern electronic systems. A coordinated and flexible approach is essential to protecting critical systems from growing cyber threats. The research examines the use of technologies such as behavioral analysis and network monitoring, as well as artificial intelligence such as neural networks and machine learning vacuum algorithms. This system aims to identify negative patterns that may indicate a threat and provide a response to mitigate the damage. As cyberattacks become more sophisticated, preventing advanced attacks becomes more important. Ensuring a strong security defense and the ability to respond to emerging threats is crucial. The research focuses on developing strategies that can prevent advanced attacks. [21] proposed a new concept based on deep learning, such as convolutional neural network (CNN) and recurrent neural network (RNN), to detect and mitigate misinformation attacks in smart electronics.

The main focus is to develop effective methods of identifying corrective action schemes that can neutralize these attacks, allowing power systems to automatically implement corrective measures or alert operators for immediate human intervention.

These gaps indicate critical areas where additional research can significantly contribute to strengthening the cybersecurity of smart meters and ensuring the reliability of smart grids in the future.

6. Research Gaps and Proposals for Future Work

The analysis of the main cyber threats to smart meters highlighted several areas for attention, but also revealed significant gaps that still need to be addressed by the academic and industrial communities.

One of the most notable gaps is the lack of consensus on unified security standards for smart meters. Although there are several proposals for security protocols and cyberattack mitigation mechanisms, such as advanced encryption and anomaly detection [27,29], these mechanisms have not yet been widely and uniformly implemented in the industry. The development of internationally recognized security standards specifically aimed at protecting smart meters would be an important contribution to increasing the security of smart grids. Future work could explore the creation of such standards, collaborating with regulatory bodies and critical infrastructure industries.

Another gap identified is the lack of studies focused on the resilience of systems in large-scale attack scenarios. While the paper discusses the dangers of DDoS and malicious command injection attacks [32], there were few studies investigating system recovery after successful attacks. Future work could focus on developing and testing recovery strategies that allow smart metering systems to quickly restructure after a security breach, minimizing the impact on consumers.

In addition, the paper presents a number of known attacks and vulnerabilities [34], but does not delve deeply into emerging vulnerabilities associated with new technologies integrated into smart grids, such as edge computing and 5G. These new technologies offer benefits of reduced latency and increased connectivity, but they also introduce new attack vectors that need to be understood and mitigated. Future studies can examine how these technologies affect smart meters and propose solutions to protect networks that include these innovations.

 doi:10.20944/preprints202502.1399.v1

Finally, it is important to note the lack of end-user-centric studies, especially with regard to awareness and education about the cyber risks associated with smart meters. While the main focus of the research is on the infrastructure and technical aspects of threat mitigation, future work could explore the impact of security awareness programs aimed at end users, helping them better understand how to protect their devices and data in smart grids. In summary, the following future work is suggested:

1. Developing unified security standards for smart meters, in collaboration with regulatory agencies.
2. Studies on system resilience and recovery after large-scale cyberattacks.
3. Investigating emerging vulnerabilities associated with technologies such as edge computing and 5G, within the context of smart grids.
4. Creating security awareness programs to educate end users on how to protect their data in smart meter networks.

These areas represent significant gaps in the field of smart meter cybersecurity, and by addressing them, future work could significantly contribute to the security and reliability of these networks.

7. Conclusion

This systematic review of cybersecurity and the main cyber threats to smart meters revealed that, although technological advances offer many benefits to smart grids, they also introduce a number of vulnerabilities that have yet to be fully addressed. The threats discussed, such as DDoS attacks, malicious command injection, and the exploitation of authentication and encryption flaws [32,34], demonstrate that smart meters remain an attractive target for cybercriminals, especially in critical infrastructures.

The implication of the findings is that, although many solutions have been proposed in the literature, such as advanced search engines and advanced encryption techniques, their implementation still faces challenges. The lack of standardization and isolation of solutions across different vendors and geographies is a key issue to ensure consistent security of smart metering. Furthermore, these networks increasingly rely on new technologies such as 5G and edge computing, which add new challenges to the security balance [28,29] . Research should focus on the following areas:

1. **Standardization and regulation**:Creating a unified set of security standards to protect smart meters is critical to ensuring compliance and security across all connected devices. Future work could include working with international regulators to create clear guidelines and connections around the security of smart solutions from manufacturing to operations.
2. **Resilience and post-attack recovery**: The ability to recover quickly after a successful cyberattack remains an uncharted area. Future research could focus on developing recovery strategies and procedures that will enable smart countermeasures to return to work quickly and efficiently while also minimizing the impact on used assets.
3. **Security in emerging technologies**: The use of 5G and edge computing is increasing, but these technologies also bring new challenges. Discovering the unique vulnerabilities of this technology and developing security solutions to prevent smart metering in high-connectivity, low-latency environments should be a priority note for future research.
4. **End User Awareness and Education**: While technology security is important, end users play a significant role in protecting their devices. Future research could explore improving security awareness and education to help users understand how to protect their smart devices and personal data.

These areas of research are essential to strengthening the security of smart meters and the energy grid as a whole. By implementing more robust and standardized solutions, it will be possible to mitigate the risks associated with these cyber threats, ensuring the reliability and resilience of the smart metering infrastructure.

 doi:10.20944/preprints202502.1399.v1

8. Conclusions

This systematic review of cybersecurity and the main cyber threats to smart meters revealed that, although technological advances offer many benefits to smart grids, they also introduce a number of vulnerabilities that have yet to be fully addressed. The threats discussed, such as DDoS attacks, malicious command injection, and the exploitation of authentication and encryption flaws [32,34], demonstrate that smart meters remain an attractive target for cybercriminals, especially in critical infrastructures.

The implication of the findings is that, although many solutions have been proposed in the literature, such as advanced search engines and advanced encryption techniques, their implementation still faces challenges. The lack of standardization and isolation of solutions across different vendors and geographies is a key issue to ensure consistent security of smart metering. Furthermore, these networks increasingly rely on new technologies such as 5G and edge computing, which add new challenges to the security balance [28,29] . Research should focus on the following areas:

1. **Standardization and regulation**:Creating a unified set of security standards to protect smart meters is critical to ensuring compliance and security across all connected devices. Future work could include working with international regulators to create clear guidelines and connections around the security of smart solutions from manufacturing to operations.
2. **Resilience and post-attack recovery**: The ability to recover quickly after a successful cyberattack remains an uncharted area. Future research could focus on developing recovery strategies and procedures that will enable smart countermeasures to return to work quickly and efficiently while also minimizing the impact on used assets.
3. **Security in emerging technologies**: The use of 5G and edge computing is increasing, but these technologies also bring new challenges. Discovering the unique vulnerabilities of this technology and developing security solutions to prevent smart metering in high-connectivity, low-latency environments should be a priority note for future research.
4. **End User Awareness and Education**: While technology security is important, end users play a significant role in protecting their devices. Future research could explore improving security awareness and education to help users understand how to protect their smart devices and personal data.

These areas of research are essential to strengthening the security of smart meters and the energy grid as a whole. By implementing more robust and standardized solutions, it will be possible to mitigate the risks associated with these cyber threats, ensuring the reliability and resilience of the smart metering infrastructure.

Author Contributions: Conceptualization, J.M.N. and O.S.M.G.; methodology, J.M.N.; software, J.M.N.; validation, J.M.N., O.S.M.G., and A.D.S.; formal analysis, J.M.N.; investigation, J.M.N.; resources, O.S.M.G.; data curation, J.M.N.; writing—original draft preparation, J.M.N.; writing—review and editing, O.S.M.G. and A.D.S.; visualization, J.M.N.; supervision, O.S.M.G.; project administration, O.S.M.G.; funding acquisition, A.D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by FADCOM – Communications Development Support Fund, presidential decree no. 264/10, November 26, 2010, and by CNPQ.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. UK Government Publishing Service, "Smart Meter Statistics in Great Britain: Quarterly Report to end December 2023," 2023.

2. IoT Analytics, "Smart Meter Adoption," 2023. [Online]. Available: https://iot-analytics.com/smart-meter-adoption/
3. M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart Meter Data Privacy: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.
4. D. Alahakoon and X. Yu, "Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 425–436, 2016.
5. P. Autor, S. Autor, and T. Autor, "Cybersecurity Threats, Detection Methods, and Prevention Strategies in Smart Grid: Review," in *2023 IEEE International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 10073843, IEEE, 2023. doi: 10.1109/ICAIS56108.2023.10073843.
6. S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, 2023. doi: 10.3390/s23167273
7. A. Bedi, J. Ramprabhakar, R. Anand, U. Kumaran, V. Meena and I. A. Hameed, "A Novel Blockchain Supported Hybrid Authentication and Handshake Algorithm for Smart Grid," in IEEE Access, vol. 12, pp. 177589-177608, 2024, doi: 10.1109/ACCESS.2024.3505535
8. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkawsi, G.; Alsayaydeh, J.A.J.; Gaid, A.S.A. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. Energies 2025, 18, 141. https://doi.org/10.3390/en18010141
9. D. Singhal, L. Ahuja and A. Seth, "Anomaly Detection in Smart Meters: Analytical Study," 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2022, pp. 1-5, doi: 10.1109/PARC52418.2022.9726670.
10. R. dos Santos Costa, J. A. S. Aranda, V. W. de Vargas, P. R. da S. Pereira, J. L. V. Barbosa, and M. P. Vianna, "Data Analysis Techniques Applied to Distribution Systems: A Systematic Mapping Study," *Electric Power Components and Systems*, vol. 51, no. 5, pp. 452–467, 2023. doi: 10.1080/15325008.2023.2175927.
11. K. Ashok, M. J. Reno, L. Blakely and D. Divan, "Systematic Study of Data Requirements and AMI Capabilities for Smart Meter Analytics," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 53-58, doi: 10.1109/SEGE.2019.8859916.
12. Paul B, Sarker A, Abhi SH, Das SK, Ali MF, Islam MM, Islam MR, Moyeen SI, Rahman Badal MF, Ahamed MH, Sarker SK, Das P, Hasan MM, Saqib N. Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. Heliyon. 2024 Sep 16;10(19):e37980. doi: 10.1016/j.heliyon.2024.e37980. PMID: 39398004; PMCID: PMC11470553.
13. M. Ismail, M. F. Shaaban, M. Naidu and E. Serpedin, "Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation," in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428-3437, July 2020, doi: 10.1109/TSG.2020.2973681.
14. Haji Mirzaee, P.; Shojafar, M.; Cruickshank, H.; Tafazolli, R. Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). IEEE Access 2022, 10, 52922–52954.
15. H. A. Hseiki, A. M. El-Hajj, Y. O. Ajra, F. A. Hija and A. M. Haidar, "A Secure and Resilient Smart Energy Meter," in IEEE Access, vol. 12, pp. 3114-3125, 2024, doi: 10.1109/ACCESS.2023.3349091
16. K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering, Swindon, United Kingdom, 2008, pp. 68–77.
17. K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," Information and Software Technology, vol. 64, pp. 1–18, Aug. 2015.
18. Al-Ghaili, Abbas M., et al. "A Review of anomaly detection techniques in advanced metering infrastructure." Bulletin of Electrical Engineering and Informatics 10.1 (2021): 266-273.
19. Guato Burgos, M.F.; Morato, J.; Vizcaino Imacaña, F.P. A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence. Appl. Sci. 2024, 14, 1194. https://doi.org/10.3390/app14031194
20. N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," in IEEE Access, vol. 12, pp. 18147-18167, 2024, doi: 10.1109/ACCESS.2024.3361039.
21. E. Naderi and A. Asrari, "A Deep Learning Framework to Identify Remedial Action Schemes Against False Data Injection Cyberattacks Targeting Smart Power Systems," in IEEE Transactions on Industrial Informatics, vol. 20, no. 2, pp. 1208-1219, Feb. 2024, doi: 10.1109/TII.2023.3272625.

 doi:10.20944/preprints202502.1399.v1

22. M. Tripathy, R. Niyogi, P. S. Kumar, G. B. Kumbhar, R. Singh and V. Thakur, "A Novel Approach for Detection of Cyber Attacks in Microgrid SCADA System," 2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET), Bhubaneswar, India, 2023, pp. 1-6, doi: 10.1109/SeFeT57834.2023.10245046.
23. F. Mohammadi, M. Saif, M. Ahmadi and B. Shafai, "A Review of Cyber–Resilient Smart Grid," 2022 World Automation Congress (WAC), San Antonio, TX, USA, 2022, pp. 28-35, doi: 10.23919/WAC55640.2022.9934511.
24. Z. Yongjie, W. Zidong, L. Jingxia, F. Zhongming, J. Ling and C. Kai, "A Review of Features, Vulnerabilities, Cyber-Attacks and Protective Actions in Smart Grid Systems," 2023 IEEE 6th International Electrical and Energy Conference (CIEEC), Hefei, China, 2023, pp. 171-176, doi: 10.1109/CIEEC58067.2023.10166872.
25. M. Saad, S. B. A. Bukhari and C. H. Kim, "A review of various modern strategies for mitigation of cyber attacks in smart grids," 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), Seogwipo, Korea (South), 2019, pp. 1-7, doi: 10.1109/ITEC-AP.2019.8903798.
26. M. M. Pour, A. Anzalchi and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," SoutheastCon 2017, Concord, NC, USA, 2017, pp. 1-4, doi: 10.1109/SECON.2017.7925278.
27. R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," 2015 IEEE International Conference on Electro/Information Technology (EIT), Dekalb, IL, USA, 2015, pp. 386-391, doi: 10.1109/EIT.2015.7293374.
28. R. Blom, M. Korman, R. Lagerström and M. Ekstedt, "Analyzing attack resilience of an advanced meter infrastructure reference model," 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, 2016, pp. 1-6, doi: 10.1109/CPSRSG.2016.7684095.
29. D. Singhal, L. Ahuja and A. Seth, "Anomaly Detection in Smart Meters: Analytical Study," 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2022, pp. 1-5, doi: 10.1109/PARC52418.2022.9726670.
30. Abdullah, Muhammad Daniel Hafiz, et al. "Attacks, vulnerabilities and security requirements in smart metering networks." KSII Transactions on Internet & Information Systems 9.4 (2015).
31. Zaraket, Carine, et al. "Cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies." AIP Conference Proceedings. Vol. 2307. No. 1. AIP Publishing, 2020.
32. M. Mohammadpourfard, F. Ghanaatpishe, Y. Weng, I. Genc and M. T. Sandıkkaya, "Real-Time Detection of Cyber-Attacks in Modern Power Grids with Uncertainty using Deep Learning," 2022 International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, Netherlands, 2022, pp. 1-6, doi: 10.1109/SEST53650.2022.9898413.
33. Y. Wang, Q. Chen, T. Hong and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3125-3148, May 2019, doi: 10.1109/TSG.2018.2818167.
34. Díaz Redondo, Rebeca P., Ana Fernández-Vilas, and Gabriel Fernández dos Reis. "Security aspects in smart meters: Analysis and prevention." Sensors 20.14 (2020): 3977.
35. Khattak, Asad Masood, Salam Ismail Khanji, and Wajahat Ali Khan. "Smart meter security: Vulnerabilities, threat impacts, and countermeasures." Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 13. Springer International Publishing, 2019.
36. Khattak, Asad Masood, Salam Ismail Khanji, and Wajahat Ali Khan. "Smart meter security: Vulnerabilities, threat impacts, and countermeasures." Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 13. Springer International Publishing, 2019.
37. R. Wadsworth, Z. Hodgins, M. Ellis and L. Troshka, "Using smart meter data to predict and identify consumer vulnerability," 27th International Conference on Electricity Distribution (CIRED 2023), Rome, Italy, 2023, pp. 786-790, doi: 10.1049/icp.2023.0515.
38. Cyber-Physical Vulnerability Assessment in Smart Grids Based on Multilayer Complex Networks. https://www.mdpi.com/1424-8220/21/17/5826
39. S. M. Alfassa, S. Nagasundari and P. B. Honnavalli, "Invasion Analysis of Smart Meter In AMI System," 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 2021, pp. 831-836, doi: 10.1109/MysuruCon52639.2021.9641595.
40. M. R. Asghar, G. Dán, D. Miorandi and I. Chlamtac, "Smart Meter Data Privacy: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820-2835, Fourthquarter 2017, doi: 10.1109/COMST.2017.2720195.

41. Y. He, G. J. Mendis and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505-2516, Sept. 2017, doi: 10.1109/TSG.2017.2703842
42. P. Gupta C.R., A. Ramesh, D. Satvik, S. Nagasundari and P. B. Honnavalli, "Simulation of SCADA System for Advanced Metering Infrastructure in Smart Grid," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 1071-1077, doi: 10.1109/ICOSEC49089.2020.9215432.
43. A. Sharma, V. K. Saini, R. Kumar, A. S. Al-Sumaiti and E. Heydarian-Forushani, "Intrusion Detection Tool for Residential Consumers Equipped with Smart Meters," 2023 IEEE International Conference on Energy Technologies for Future Grids (ETFG), Wollongong, Australia, 2023, pp. 1-6, doi: 10.1109/ETFG55873.2023.10408544.
44. D. Parida and U. Bhanja, "Smart Meters:Cyber Security Issues and Their Solutions," 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 2023, pp. 1-6, doi: 10.1109/ViTECoN58111.2023.10157938.
45. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. https://www.mdpi.com/1996-1073/16/4/1651
46. C. -C. Sun, D. J. Sebastian Cardenas, A. Hahn and C. -C. Liu, "Intrusion Detection for Cybersecurity of Smart Meters," in IEEE Transactions on Smart Grid, vol. 12, no. 1, pp. 612-622, Jan. 2021, doi: 10.1109/TSG.2020.3010230
47. R. Sharma, A. M. Joshi, C. Sahu, G. Sharma, K. T. Akindeji and S. Sharma, "Semi Supervised Cyber Attack Detection System For Smart Grid," 2022 30th Southern African Universities Power Engineering Conference (SAUPEC), Durban, South Africa, 2022, pp. 1-5, doi: 10.1109/SAUPEC55179.2022.9730715.
48. L. L. Win and S. Tonyalı, "Security and Privacy Challenges, Solutions, and Open Issues in Smart Metering: A Review," 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 2021, pp. 800-805, doi: 10.1109/UBMK52708.2021.9558912.
49. M. S. Qureshi, I. Ullah Khan and K. Kim, "Securing the Smart Grid: A Comprehensive Analysis of Recent Cyber Attacks," 2023 5th International Conference on Electrical, Control and Instrumentation Engineering (ICECIE), Kuala Lumpur, Malaysia, 2023, pp. 1-6, doi: 10.1109/ICECIE58751.2024.10457427.
50. S. M. Sulaiman, P. Aruna Jeyanthy, D. Devaraj, S. S. Mohammed and K. V. Shihabudheen, "Smart Meter Data Analytics for Load Prediction using Extreme Learning Machines and Artificial Neural Networks," 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES), Krishnankoil, India, 2019, pp. 1-4, doi: 10.1109/INCCES47820.2019.9167736.
51. P. U. Rao, B. Sodhi and R. Sodhi, "Cyber Security Enhancement of Smart Grids Via Machine Learning - A Review," 2020 21st National Power Systems Conference (NPSC), Gandhinagar, India, 2020, pp. 1-6, doi: 10.1109/NPSC49263.2020.9331859.
52. K. D. Kumar, M. A. Jawale, M. Sujith and D. B. Pardeshi, "Cybersecurity Threats, Detection Methods, and Prevention Strategies in Smart Grid: Review," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 1609-1614, doi: 10.1109/ICAIS56108.2023.10073843.
53. M. D. Hossain, H. Ochiai, L. Khan and Y. Kadobayashi, "Smart Meter Modbus RS-485 Intrusion Detection by Federated Learning Approach," 2023 15th International Conference on Computer and Automation Engineering (ICCAE), Sydney, Australia, 2023, pp. 559-564, doi: 10.1109/ICCAE56788.2023.10111132.
54. N. Iliaee, S. Liu and W. Shi, "Non-Intrusive Load Monitoring based Demand Prediction for Smart Meter Attack Detection," 2021 International Conference on Control, Automation and Information Sciences (ICCAIS), Xi'an, China, 2021, pp. 370-374, doi: 10.1109/ICCAIS52680.2021.9624524.
55. X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," in IEEE Communications Magazine, vol. 50, no. 8, pp. 38-45, August 2012, doi: 10.1109/MCOM.2012.6257525
56. P. Haji Mirzaee, M. Shojafar, H. Cruickshank and R. Tafazolli, "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," in IEEE Access, vol. 10, pp. 52922-52954, 2022, doi: 10.1109/ACCESS.2022.3174259.