INTERNATIONAL JOURNAL OF SUSTAINABLE CONSTRUCTION ENGINEERING AND TECHNOLOGY
VOL. 14 NO. 3 (2023) 210-220

IJSCET

http://publisher.uthm.edu.my/ojs/index.php/ijscet

ISSN : 2180-3242 e-ISSN : 2600-7959

International Journal of Sustainable Construction Engineering and Technology

Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach

Fiza Abdul Rahim[1,3*], Nur Azfahani Ahmad[2,3], Pritheega Magalingam[1], Norziana Jamil[4], Zaihisma Che Cob[5], Lizawati Salahudin[6]

[1]Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia Jalan Sultan Yahya Petra, 54100, Kuala Lumpur, MALAYSIA

[2]Programme of Building Surveying, Department of Built Environment Studies and Technology,
College of Built Environment, Universiti Teknologi MARA, 32610, Perak Branch, Perak, MALAYSIA

[3]Green Safe Cities (GreSafe) Research Group, Department of Built Environment Studies and Technology,
College of Built Environment, Universiti Teknologi MARA, 32610, Perak Branch, Perak, MALAYSIA

[4]Department of Information System and Security,
United Arab Emirates University, Al-Ain, 15551, UNITED ARAB EMIRATES

[5]College of Computing and Informatics,
Universiti Tenaga Nasional, Putrajaya Campus, Jalan IKRAM-UNITEN, 43000, Kajang, Selangor, MALAYSIA

[6]Department of Software Engineering, Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Jalan Hang Tuah Jaya, 76100, Melaka, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/ijscet.2023.14.03.018
Received 22 August 2023; Accepted 22 August 2023; Available online 21 September 2023

Abstract: Cybersecurity is a growing concern for smart grids, especially with the integration of solar photovoltaics (PVs). With the installation of more solar and the advancement of inverters, utilities are provided with real-time solar power generation and other information through various tools. However, these tools must be properly secured to prevent the grid from becoming more vulnerable to cyber-attacks. This study proposes a threat modeling and risk assessment approach tailored to smart grids incorporating solar PV systems. The approach involves identifying, assessing, and mitigating risks through threat modeling and risk assessment. A threat model is designed by adapting and applying general threat modeling steps to the context of smart grids with solar PV. The process involves the identification of device assets and access points within the smart grid infrastructure. Subsequently, the threats to these devices were classified utilizing the STRIDE model. To further prioritize the identified threat, the DREAD threat-risk ranking model is employed. The threat modeling stage reveals several high-risk threats to the smart grid infrastructure, including Information Disclosure, Elevation of Privilege, and Tampering. Targeted recommendations in the form of mitigation controls are formulated to secure the smart grid's posture against these identified threats. The risk ratings provided in this study offer valuable insights into the cybersecurity risks associated with smart grids incorporating solar PV systems, while also providing practical guidance for risk mitigation. Tailored mitigation strategies are proposed to address these vulnerabilities. By taking proactive measures, energy sector stakeholders may strengthen the security of their smart grid infrastructure and protect critical operations from potential cyber threats.

Keywords: Cybersecurity, solar PV, sustainable energy, resilience, STRIDE, DREAD, Microsoft Threat Modeling Tool

**Corresponding author: fiza.abdulrahim@utm.my*

1. Introduction

The quick development and integration of technology in the energy sector have undergone radical changes the way electricity is generated, distributed, and utilized. Smart grids, which leverage advanced communication and control systems, play a pivotal role in optimizing the efficiency and reliability of electricity grids (Inayat et al., 2022). Solar photovoltaic (PV) systems have become a well-known solution for sustainable power generation as the world turns to renewable energy sources (Gupta et al., 2020). However, the integration of solar PV into smart grids also brings with it additional difficulties, particularly in terms of cybersecurity.

It is essential to have a complete understanding of the potential cybersecurity vulnerabilities related to this complex infrastructure given the connectivity of smart grids with solar PV systems. Threat modeling and risk assessment methodologies provide valuable frameworks for systematically identifying and analyzing these vulnerabilities, allowing stakeholders to put into place effective mitigation measures (Holik et al., 2022). This study present an in-depth exploration of threat modeling and risk assessment methods designed specifically for smart grids with solar PV systems.

Given that malicious actors may target smart grids with solar PV systems to take advantage of vulnerabilities for personal gain, service disruptions, or sabotage, it is necessary to assess the cybersecurity risks of these systems (Bailey et al., 2020). Successful cyber attacks on a smart grid equipped with solar PV systems have the potential to have far-reaching effects, including compromised electricity generation, unstable grids, unauthorized access to private data, and privacy violations. PV systems may also serve as a launchpad for larger attacks on the electrical grid due to the interconnectedness of the energy infrastructure.

A thorough understanding of potential attack vectors and system weaknesses is necessary to assess the cybersecurity vulnerabilities of smart grids with solar PV installations. Analysis of software vulnerabilities, communication protocols, system configurations, and human factors that could leave a system vulnerable to cyber threats are all part of this process. The integrity, reliability, and resilience of smart grids with solar PV systems can be protected by stakeholders by identifying and assessing these vulnerabilities and then developing comprehensive risk management strategies and putting them into action.

This paper aims to address the need to examine the cybersecurity vulnerabilities of smart grids with solar PV systems using threat modelling and risk assessment. This study helps to create secure and resilient smart grids with solar PV systems by identifying vulnerabilities and suggesting suitable mitigation techniques, ensuring the continuous expansion and acceptance of solar power securely and sustainably.

The paper is organized as follows: Section 2 gives a brief introduction to cybersecurity and examines the potential cyberattacks associated with smart grids with solar PV systems. The methodology employed in this study is outlined in Section 3. Section 4 presents the proposed threat model, which evaluates attack probabilities. Additionally, Section 5 describes how the consequences of the identified security vulnerabilities contribute to the study's result.

2. Cybersecurity in Smart Grids with Solar PV Integration

This section provides a review of cybersecurity research in smart grids with solar PV in general and provides an overview of the threat assessment model for PV systems. Numerous studies have addressed the cybersecurity challenges in smart grids incorporating PV systems. Mrabet et al. (2018) conducted an extensive survey that examined the cybersecurity landscape of smart grids, including those associated with solar PV integration. They identified various attack vectors such as denial of service (DoS), replay attack, and integrity violation. Hasan et al. (2023) conducted a review specifically on securing smart grids against cyber-physical attacks. They highlighted the vulnerabilities introduced by smart grid and emphasized countermeasures including authentication mechanisms, encryption techniques, and intrusion detection systems.

Similarly, Chehri & Fofana (2021) explored smart grid critical infrastructures, including solar PV systems. They proposed qualitative risk assessment methods based on the documentary review on some methodologies implemented to evaluate cybersecurity risk applied to supervisory control and data acquisition (SCADA). In another study, Teymouri et al. (2018) examined the impact of cyber attacks on voltage regulation problem in distribution grids with PV units capable of reactive power generation. They analyzed potential threats to voltage sensors and suggested defense strategies, such as selecting PV inverters with sufficient capacity to minimize real power curtailment.

In a study conducted by Walker et al. (2021) that specifically examined cybersecurity in PV operations, notable challenges were identified, including a shortage of personnel with cybersecurity expertise and inadequate cyber hygiene practices. To address these concerns, the study proposed comprehensive plans that encompassed the expanded threat landscape, emphasized training programs for staff, and recommended implementing certifications for security systems as proactive measures to mitigate these risks.

Addressing the issue of physical layer security, Islam et al. (2019) explored the vulnerabilities and threats present in components of smart energy systems, such as Internet of Things (IoT) enabled devices, and exploring the associated communication standards. They identified significant security vulnerabilities at the physical layer, conducted a

thorough threat analysis, and proposed a framework that incorporates advanced security techniques to enhance the physical layer security of the smart energy system.

While the previous studies have provided valuable insights into different attack vectors and effective security measures, this study focuses on exploring emerging cyber threats and vulnerabilities that have not been extensively covered. Particular emphasis is placed on ensuring the secure implementation and operation of smart grids with solar PV systems.

To provide a visual representation, Fig. 1 illustrates the diagram depicting the smart grids with solar PV integration, adapted from the work of (Li et al., 2020). This diagram serves as a reference to visually comprehend the interconnectedness and components of the distribution power grids integrated with solar farms, setting the stage for a deeper analysis of security vulnerabilities and potential countermeasures.

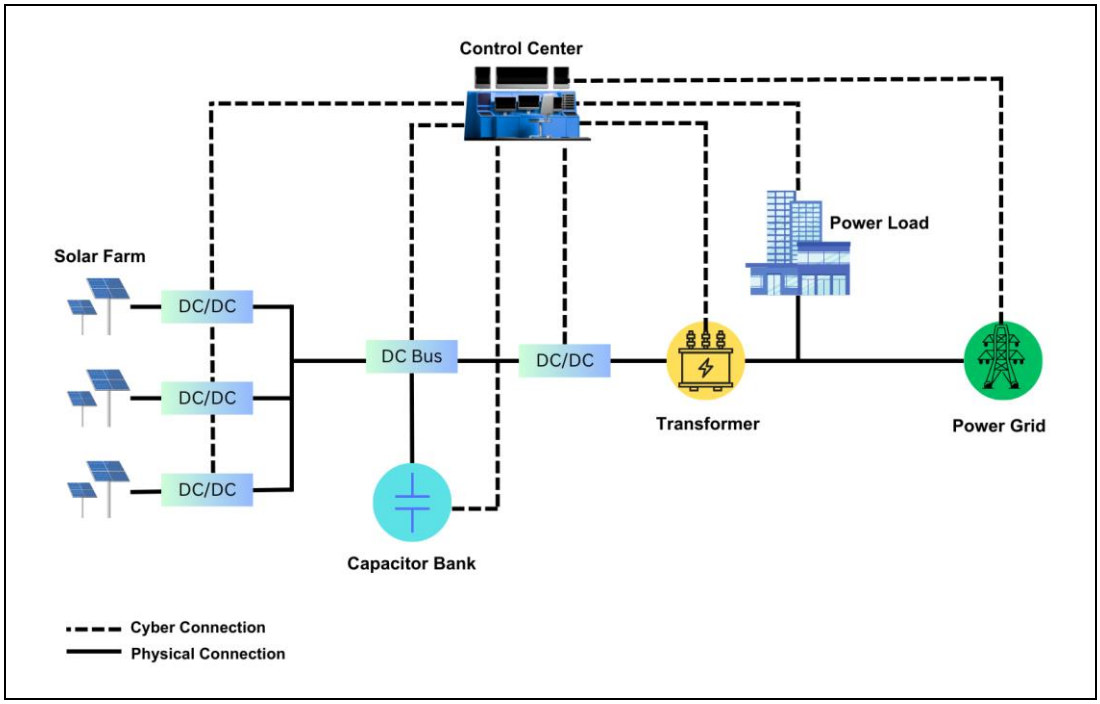

Fig. 1 - Smart grid with solar PV integration architecture (Li et al., 2020)

The solar farm is physically interconnected with the distribution grid through a series of components including DC/DC and DC/AC converters, as well as grid-connected transformers. Additionally, the major components and control center are linked through cyber networks. The control center is connected to the solar farm through the DC/DC converters and the DC Bus. The DC/DC converters facilitate the conversion of direct current (DC) power generated by the solar panels into a suitable voltage level for transmission. They ensure efficient power transfer from the solar farm to the control center. The DC Bus serves as a central connection point for the DC power coming from the solar panels and other power sources within the system. It acts as a distribution hub, allowing the control center to receive and monitor the DC power generated by the solar farm.

From the control center, various components, including capacitor banks, transformers, power loads, and the power grid, can be monitored and managed. Capacitor banks can be controlled and regulated to optimize power factor and voltage stability within the solar farm and the overall distribution system. Transformers connected to the DC Bus enable voltage stepping as necessary for efficient power transmission and distribution. The control center can monitor and control the operation of these transformers to maintain voltage regulation and address any issues that may arise.

Furthermore, the control centre oversees and manages the power loads connected to the solar farm. Real-time monitoring of power consumption allows the control centre to balance the supply and demand of electricity, prevent overloading, and ensure efficient power distribution within the solar farm. Additionally, the control centre, connected to the power grid, can monitor grid performance, detect faults or abnormalities, and coordinate grid operations to maintain stability and ensure reliable power supply to consumers.

3. Methodology

A threat model in this paper is developed by adapting the general steps of threat modelling as outlined in Alhassan et al., (2016); Meier et al., (2003); and Omotosho et al., (2019). It features as follows:

(a) the identification of assets,

(b) identification of device's access points,
(c) classification of threats,
(d) rating of the identified threats, and
(e) proposal of countermeasures to mitigate each threat.

3.1 Identification of Assets

Since assets are the primary targets of assaults, identifying them is the most important phase in the threat modelling process. Attackers are individuals or systems that pose a risk to the asset within the system or environment in which it is used. Any important system component that belongs to the organisation and is of interest to attackers is considered an asset. Assets in the environment could change over time and need for security measures to adapt to circumstances that aren't typically anticipated during the design process (De Faveri & Moreira, 2016). Table 1 lists the assets of smart grids with solar PV integration.

Table 1 - Assets of smart grids with solar PV integration

Asset	Details
Solar Panel	Solar panels convert sunlight into electrical energy, providing a renewable and clean source of power. The solar PV systems generate electricity at the point of consumption, reducing the reliance on traditional centralized power generation and transmission infrastructure.
DC/DC converters	Enable the conversion of DC power generated by the solar panels to the appropriate voltage level for transmission and distribution. They ensure efficient power transfer from the solar panels to the grid-connected components.
Control Center	It serves as the central hub for monitoring, managing, and controlling the operations of the PV system. The control center oversees the performance of the solar panels, monitors power generation, manages grid connectivity, and coordinates various grid operations.
Capacitor Banks	Used to improve power factor and voltage stability within the smart grid. They compensate for reactive power and help maintain a balanced power factor, reducing line losses and enhancing overall system efficiency.
Transformers	Ensuring compatibility between different parts of the grid through voltage level adjustments. They facilitate efficient power transmission and distribution by adjusting the voltage to suitable levels for different parts of the grid.
Power Load	Represents the total electrical demand and consumption within the smart grid. It includes residential, commercial, and industrial loads. Managing and balancing the power load is essential to ensure stable and reliable electricity supply to consumers.
Power Grid	Encompassing the interconnected network of power generation, transmission, and distribution infrastructure. It includes substations, transmission lines, distribution lines, and other components that enable the flow of electricity within the grid.

3.2 Device Access Points Identification

Access points serve as interfaces through which potential attackers can gain unauthorized access to valuable system assets. These access points can take various forms in smart grid with solar PV integration, including the physical connections of solar panels to DC/DC converters or inverters, the interface ports of DC/DC converters connected to the solar panels and the DC Bus, the connection points of the DC Bus for power distribution, network interfaces and communication ports of the control center, the terminals of capacitor banks for power regulation, the terminals or connectors of transformers for voltage conversion, the electrical outlets or connectors for power loads, and the connection points of the power grid for import or export of electricity.

Once identified, access points allow for the establishment of trust boundaries within the system, indicating areas where the level of trust fluctuates (Kaur & Kaur, 2014). Trust boundaries define areas where the level of trust may fluctuate, indicating potential points of vulnerability or increased risk.

For example, within the smart grid, trust boundaries may be defined to differentiate between internal and external networks. The internal network, which includes the control center and sensitive components, would have stricter access controls and higher levels of trust. In contrast, the external network, which may include connections to the power grid or communication with external systems, would have lower levels of trust and stronger security measures to prevent unauthorized access.

3.3 Classification of Threats

The next step is to categorize the potential threats that could target these access points in a smart grid system with solar PV integration after the access points have been identified. By categorizing the threats, more effective strategies

for mitigating risks and controlling the security of the system can be created. Threat categorization allows for the recognition of the various types of threats that could affect a smart grid system.

The STRIDE model is used in this study to categorize the threats in a smart grid system that integrates solar PV. In order to fully comprehend the security concerns, the STRIDE model offers a structured framework for classifying potential threats into six different categories. The STRIDE model divides potential risks into six different categories, each of which corresponds to a particular security issue (Sharma et al., 2023):

- Spoofing: This category deals with the possibility of identity or data spoofing, in which an attacker tries to impersonate a genuine user or device. Spoofing threats could involve falsifying the identity of a solar PV device or altering data to deceive the control center.
- Tampering: Threats from tampering entail the unintentional modification or manipulation of data or devices. Tampering threats may include physical tampering with components or access points, unauthorized changes to software or firmware, malicious manipulation of configuration files, and malicious manipulation of firmware.
- Repudiation: Threats of repudiation concern the capacity to deny or falsely refute actions or events. Repudiation threats can entail an attacker altering or fabricating records, logs, or audit trails in order to conceal their activity or accuse trustworthy users or devices of malicious actions.
- Information Disclosure: Threats involving unauthorized access to, or disclosure of sensitive information are the main emphasis of this category. Threats to information disclosure could come in the form of unauthorized access to customer data, the disclosure of system flaws, or the leakage of private operational data.
- Denial of Service: Denial of service threats aim to disrupt or impair the availability or performance of a system or service. Threats to denial of service could involve flooding the network or control centre with requests, which would result in a degraded or unresponsive service.
- Elevation of Privilege: Unauthorized escalation of user privileges or access rights constitutes an important danger to the security of a system. These dangers can include an attacker acquiring unrestricted administrative access to the control centre, evading access constraints, or taking advantage of flaws to elevate their privileges within the system.

The application of the STRIDE model enables a systematic analysis and classification of potential threats, organizing them into distinct categories. This approach helps identify and prioritize the specific security concerns that need to be addressed in the smart grid system. Understanding the different types of threats allows for the development of targeted mitigation strategies and the implementation of appropriate security controls to safeguard against each category of threat.

3.4 Rating of Identified Threats

After categorizing the potential threats, the risk assessment process moves on to assigning risk ratings using the threat-risk ranking DREAD model. The DREAD model is a widely used framework to evaluate and analyze the severity and possible impact of each identified threat.

The DREAD model uses five criteria to assess threats:

- Damage Potential: Evaluates the potential harm that might result from an exploited threat. It considers the extent of harm to the system, data, or operations.
- Reproducibility: Evaluates how easily a danger may be duplicated or exploited. It establishes if the threat is one-time only or if an attacker has the ability to repeat it.
- Exploitability: Evaluates the level of expertise or effort needed by an attacker to successfully exploit the vulnerability and carry out the threat.
- Affected Users: Evaluates on the number or proportion of users or assets that would be impacted by the threat, which helps to assess the potential scale of the impact.
- Discoverability: Evaluates that either attackers or defenders will become aware of the threat. It takes into account how quickly the threat may be detected or identified.

Each of these criteria is assigned a rating, usually on a scale of 0 to 10, with 10 denoting the highest level of severity or impact. The overall risk rating for the threat is then calculated by adding the ratings for each criterion. Risk ratings from 12 to 15 are categorized as high risk, ratings from 8 to 11 are categorized as medium risk, and ratings from 5 to 7 are categorized as low risk.

The risk rating obtained through the DREAD model provides a quantitative assessment of the severity and potential impact of each threat. This rating helps prioritize and allocate resources based on the level of risk posed by different threats. Higher-rated threats require more immediate attention and greater investment in mitigation measures.

3.5 Proposing Countermeasures to Mitigate Threats

Once potential threats have been identified and their risk ratings assessed, the next crucial step is to propose effective countermeasures that target the mitigation of these threats within the smart grid system integrated with solar

PV. Countermeasures encompass a range of proactive measures and strategic approaches implemented to minimize both the likelihood and potential consequences of the identified threats.

By proposing and implementing appropriate countermeasures, organizations can significantly reduce the vulnerabilities and risks associated with potential threats. This proactive approach strengthens the security posture of the smart grid system, enhances resilience, and ensures the reliable and secure operation of the system in the face of evolving cyber threats.

4. Threat Modeling and Risk Assessment for Smart Grids with Solar PV Integration

This section provides a comprehensive analysis and evaluation of the process of threat modeling and risk assessment is presented, specifically tailored to the distinctive context of smart grids integrated with solar PV. The focus lies on the effective utilization of techniques like the STRIDE model, enabling the identification and classification of potential threats. Subsequently, the discussion transitions to the implementation of the DREAD model, which facilitates the assessment of threat severity and impact, facilitating prioritization and optimal allocation of resources. Moreover, considerable emphasis is placed on the proposal of targeted countermeasures to mitigate these threats, highlighting the importance of proactive strategies that minimize risks and fortify the overall security, resilience, and reliability of the smart grid system.

4.1 Threat Modeling

Threat modelling generally seeks to identify threats and vulnerabilities in IT-related system architectures. Additionally, it assists in implementing security and privacy from design into practice. The Microsoft Threat Modelling Tool is utilised in this study since it is one of the techniques most frequently used to assess the risk of a specific threat (Zhang et al., 2022). It gives information about risks based on the STRIDE model and operates on the basis of data flow diagrams that define data stores, processes, and communication lines. Different trust zones are identified in the model itself based on layers.

Figure 2 illustrates the threat model that is built upon the architecture depicted in Figure 1. The threat model system encompasses a data flow diagram representing the architecture. Through the process of modeling the architecture and evaluating the risks, a total of 220 threats were identified. These threats were subsequently classified according to the STRIDE model, and the classification results are presented in Table 2.

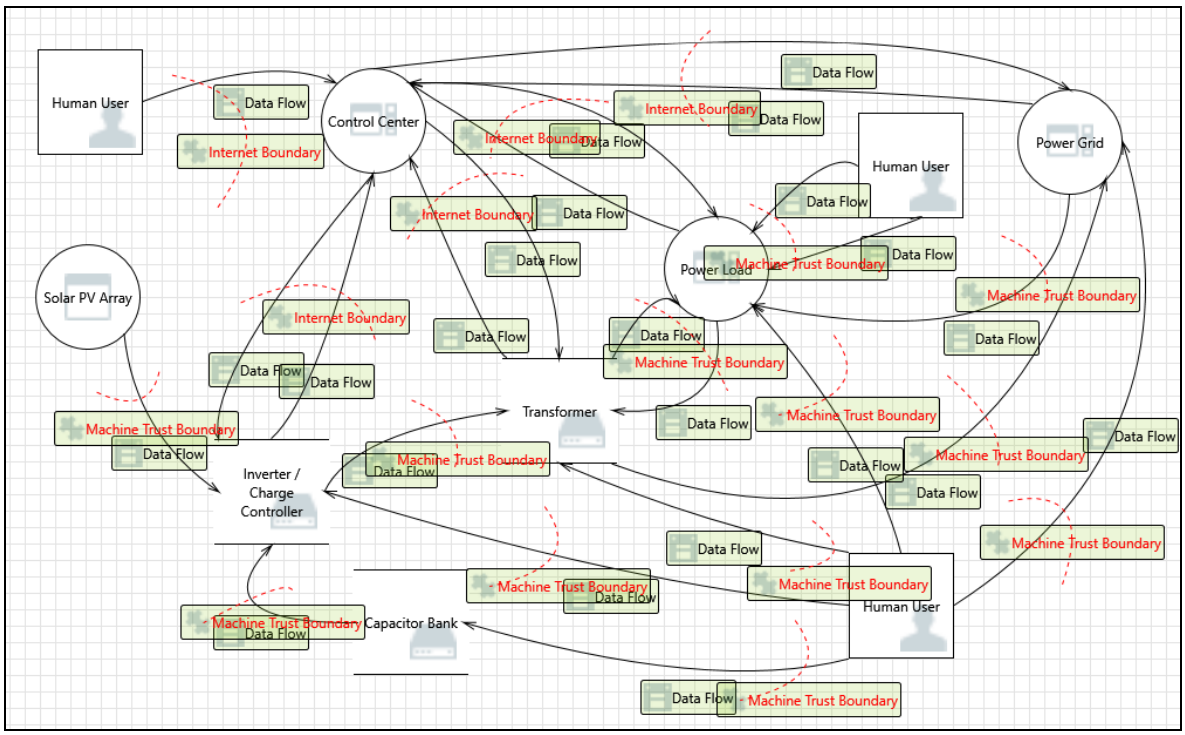

Fig. 2 - Data flow diagram of smart grid with solar PV integration

Table 2 - Threat assignment to category

Threat	Amount
Spoofing	21
Tampering	55
Repudiation	23
Information Disclosure	29
Denial of Service	54
Elevation of Privilege	38

The identified threats served as a foundation for determining security-focused countermeasures and establishing the necessary protocols to prevent them. These threats demonstrated the potential methods through which different attacks could exploit specific vulnerabilities within the system. During the assessment process, our focus was solely on the threats presented in Table 3.

Table 3 - List of threats

ID	Threats	Category	Description
12	Spoofing of Source Data Store Transformer	Spoofing	An attacker has the potential to spoof a transformer, resulting in the delivery of erroneous data to the Control Center.
36	Potential Excessive Resource Consumption for Power Load or Transformer	Denial Of Service	Potential excessive resource consumption in Power Loads or Transformers within a smart grid system can lead to performance degradation and instability.
39	Weak Access Control for a Resource	Information Disclosure	Inadequate data protection measures for Transformers can enable unauthorized access by attackers, potentially resulting in the unauthorized disclosure of sensitive information.
41	Replay Attacks	Tampering	Malicious interception and retransmission of legitimate data packets, allowing an attacker to manipulate or deceive the communication between the two entities.
42	Collision Attacks	Tampering	Deliberate creation of data collisions or conflicts during communication, potentially leading to data corruption or disruption of the communication channel.
44	Weak Authentication Scheme	Information Disclosure	The authentication mechanisms employed in a system are insufficient or easily bypassed, potentially allowing unauthorized access to sensitive resources or data.
51	Elevation Using Impersonation	Elevation Of Privilege	An unauthorized user pretends to be a legitimate user with higher privileges to gain elevated access and control within a system or network.
58	Spoofing the Human User External Entity	Spoofing	An attack where an adversary impersonates a human user, deceiving the system or network into granting unauthorized access or privileges.
83	Power Grid Process Memory Tampered	Tampering	The unauthorized alteration or manipulation of the memory of power grid processes, which can disrupt their normal operation and potentially lead to system instability or vulnerabilities.
90	Authenticated Data Flow Compromised	Tampering	An authorized and validated data transfer process is compromised or manipulated, potentially leading to unauthorized access, data alteration, or misuse of sensitive information.
116	Potential Lack of Input Validation for Control Center	Tampering	The risk of inadequate checks and verification on incoming data, which can result in the acceptance of malicious or incorrect input, compromising the integrity and reliability of the system.
117	Potential Data Repudiation by Control Center	Repudiation	The risk of the Control Center being unable to provide verifiable evidence or deny involvement in certain data-related activities, potentially leading to disputes or lack of accountability.
151	Potential Process Crash or Stop for Control Center	Denial Of Service	The risk of the Control Center software or system encountering issues or failures that could lead to its abrupt termination or unresponsiveness.
153	Data Store Inaccessible	Denial Of Service	Preventing access to the data storage system, hindering the retrieval or modification of stored information.
154	Control Center May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	The possibility of an attacker exploiting vulnerabilities in the Control Center system remotely, allowing them to gain elevated privileges and unauthorized access to critical functions and data.

157	Data Store Denies Transformer Potentially Writing Data	Repudiation	The data store restricts or denies the transformer's ability to write or update data, which can hinder the proper functioning and operation of the system.
181	Elevation by Changing the Execution Flow in Power Grid	Elevation Of Privilege	An attacker may manipulate the normal sequence of operations within the power grid system, potentially gaining unauthorized access and control over critical components, leading to disruptive and potentially harmful consequences.
198	Weak Credential Transit	Information Disclosure	Inadequate security measures may expose the sensitive information during the authentication process.
205	Data Flow Sniffing	Information Disclosure	Unauthorized interception and capture of data packets transmitted over a network.
270	Potential Process Crash or Stop for Power Grid	Denial Of Service	Disruption or failure in the operation of the power grid system could lead to significant consequences such as power outages or system instability.

4.2 Threat Rating

After identifying the threats using the STRIDE model, the next step involved applying the DREAD risk assessment model to categorize and evaluate the risks associated with each threat. The DREAD model facilitated the ranking of threats based on factors such as the potential for damage, reproducibility of the attack, ease of exploitation, impact on users, and exploitability of system vulnerabilities. By assessing threats against these five factors, the DREAD model generates a threat rating for each identified threat as shown in Table 4.

Three high-risk threats have been identified: Information Disclosure, Elevation of Privilege, and Tampering. The most critical threat is Information Disclosure, which arises due to a weak authentication scheme that can potentially grant unauthorized access to sensitive resources or data. The second significant threat is Elevation of Privilege, where an attacker can manipulate the normal sequence of operations within the power grid system, resulting in unauthorized access and control over critical components. Lastly, the third highest-rated threat is Tampering, associated with replay attacks that involves malicious interception and retransmission of legitimate data packets. Such attacks enable the attacker to manipulate or deceive communication between two entities.

This study reveals not only high-risk threats but also several medium-risk threats in the smart grid integrated with solar PV. While medium-risk threats may not immediately lead to severe consequences, they still possess the potential to compromise the security and functionality of the system and should not be underestimated or neglected. These threats may become the entry points for attackers to carry out more sophisticated and damaging attacks if left unaddressed. Hence, the proposed countermeasures will focus on addressing not just high-risk threats, but all type of threats, creating a comprehensive strategy that defends the smart grid against a wide range of potential cyber threats.

Table 4 - Threat rating using DREAD model

ID	Threats	Category	D	R	E	A	D	Total	Rating
12	Spoofing of Source Data Store Transformer	Spoofing	3	2	1	3	2	11	Medium
36	Potential Excessive Resource Consumption for Power Load or Transformer	Denial Of Service	2	2	2	3	2	11	Medium
39	Weak Access Control for a Resource	Information Disclosure	2	2	1	2	3	10	Medium
41	Replay Attacks	Tampering	3	2	2	3	2	12	High
42	Collision Attacks	Tampering	2	2	2	3	2	11	Medium
44	Weak Authentication Scheme	Information Disclosure	2	3	3	3	3	14	High
51	Elevation Using Impersonation	Elevation Of Privilege	2	2	1	2	3	10	Medium
58	Spoofing the Human User External Entity	Spoofing	2	2	2	2	2	10	Medium
83	Power Grid Process Memory Tampered	Tampering	2	2	2	2	3	11	Medium
90	Authenticated Data Flow Compromised	Tampering	2	2	1	2	3	10	Medium
116	Potential Lack of Input Validation for Control Center	Tampering	2	2	3	2	1	10	Medium
117	Potential Data Repudiation by Control Center	Repudiation	2	1	2	3	3	11	Medium
151	Potential Process Crash or Stop for Control Center	Denial Of Service	3	2	3	2	1	11	Medium

153	Data Store Inaccessible	Denial Of Service	2	3	2	2	2	11	Medium
154	Control Center May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	2	2	1	2	3	10	Medium
157	Data Store Denies Transformer Potentially Writing Data	Repudiation	2	2	3	2	2	11	Medium
181	Elevation by Changing the Execution Flow in Power Grid	Elevation Of Privilege	3	3	2	2	3	13	High
198	Weak Credential Transit	Information Disclosure	2	2	3	2	2	11	Medium
205	Data Flow Sniffing	Information Disclosure	2	2	2	2	2	10	Medium
270	Potential Process Crash or Stop for Power Grid	Denial Of Service	3	2	1	3	2	11	Medium

4.3 Proposed Countermeasures

Once the risk value is determined for each identified threat, appropriate mitigation controls can be developed to effectively reduce the associated risk. The risk rating also facilitates the establishment of a prioritized list of mitigation measures based on the level of risk they address. By utilizing the threat rating data presented in Table 4, mitigation strategies can be formulated to align with the classified threats. The list of threat assessments can then be organized according to their respective risk levels, allowing for the prioritization of higher-risk threats. To provide a practical illustration, Table 5 presents a set of proposed countermeasures aimed at mitigating the threats outlined in Tables 3 and 4.

Table 5 - Example of threat countermeasures

Threat Category	Threats	Countermeasures
Spoofing	Spoofing of Source Data Store Transformer	Strong authentication mechanisms, data integrity checks, secure communication channels
	Spoofing the Human User External Entity	User authentication and authorization, user awareness and training, monitoring and anomaly detection
Tampering	Replay Attacks	Message authentication, timestamps or sequence numbers, nonces or challenge-response mechanisms
	Collision Attacks	Strong cryptographic algorithms, key management practices, randomized techniques,
	Power Grid Process Memory Tampered	Memory protection mechanisms, encryption and integrity checks, secure boot and runtime integrity checks
	Authenticated Data Flow Compromised	Secure communication protocols, strong authentication mechanisms, data integrity checks
	Potential Lack of Input Validation for Control Center	Input validation routines, security testing and code reviews
Repudiation	Potential Data Repudiation by Control Center	Audit trails and logging, role-based access control, timestamps
	Data Store Denies Transformer Potentially Writing Data	Redundant data storage, error handling and logging, access control and permissions, data integrity checks
Information Disclosure	Weak Access Control for a Resource	Strengthen access control mechanism, regular access control audits, principle of least privilege

	Weak Authentication Scheme	Strong authentication protocols, secure communication channels, session management controls, security awareness training
	Weak Credential Transit	Secure communication protocols, strong and complex passwords for authentication
	Data Flow Sniffing	Encrypt sensitive data during transmission, network segmentation and access controls
Denial of Service	Potential Excessive Resource Consumption for Power Load or Transformer	Resource monitoring and capacity planning, load balancing and resource allocation
	Potential Process Crash or Stop for Control Center	Redundancy and backup systems, fault tolerance and error handling, system hardening, system monitoring and proactive maintenance
	Data Store Inaccessible	Redundant data storage, data backup and recovery, fault tolerance and load balancing
	Potential Process Crash or Stop for Power Grid	Redundancy and backup systems, monitoring and diagnostics
Elevation of Privilege	Elevation Using Impersonation	Predefined roles and responsibilities
	Control Center May be Subject to Elevation of Privilege Using Remote Code Execution	Regularly update and patch software and operating systems, strong access controls and user privileges
	Elevation by Changing the Execution Flow in Power Grid	Secure coding practices, anomaly detection systems

5. Conclusion

The threat modelling and risk assessment for integrated solar PV smart grids have been thoroughly examined in this study. The STRIDE model is utilized to categorize and identify potential risks, while the DREAD model is applied to determine risk ratings. The risk ratings derived from the evaluation are used to suggest targeted countermeasures to mitigate the identified threats. The findings reveal both high-risk and medium-risk threats, highlighting the importance of addressing all types of threats for a comprehensive defense strategy.

High-risk threats, including Information Disclosure, Elevation of Privilege, and Tampering, pose significant challenges and demand immediate attention. Additionally, several medium-risk threats are also discovered, which should not be underestimated, as they have the potential to compromise the system's security.

To secure the overall cybersecurity posture of the smart grid, the proposed countermeasures encompass both high and medium-risk threats. This approach safeguards critical infrastructure and sensitive data from potential breaches or disruptions. The proposed countermeasures are designed to strengthen the security, resilience, and reliability of the system, ensuring efficient power transmission and distribution while safeguarding against potential vulnerabilities and attacks.

Moreover, the study emphasizes the significance of proactive measures to mitigate vulnerabilities at all levels. Implementing robust authentication and resource control mechanisms, and secure data protection practices, routine security updates and employee awareness training are crucial steps to maintain the integrity and confidentiality of the system. By implementing the threat modeling and risk assessment methodologies presented in this study, organizations can improve the security posture of their smart grid systems, minimize potential risks, and ensure the reliable and secure operation of renewable energy infrastructure.

Acknowledgement

The study was funded by the Encouragement Research Grant (Vote No. Q.K130000.3856.20J96) awarded by Universiti Teknologi Malaysia.

References

Alhassan, J. K., Abba, E., Olaniyi, O. M., & Waziri, V. O. (2016). Threat Modeling of Electronic Health Systems and Mitigating Countermeasures. *International Conference on Information and Communication Technology and Its Applications (ICTA 2016)*.

Bailey, T., Maruyama, A., & Wallance, D. (2020). *The energy-sector threat: How to address cybersecurity*

vulnerabilities. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities#/

Chehri, A., & Fofana, I. (2021). Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability*, *13*(6), 1–19.

De Faveri, C., & Moreira, A. (2016). Designing Adaptive Deception Strategies. *Proceedings - 2016 IEEE International Conference on Software Quality, Reliability and Security-Companion, QRS-C 2016*, 77–84. https://doi.org/10.1109/QRS-C.2016.15

Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Computer Communications*, *153*(February), 406–440. https://doi.org/10.1016/j.comcom.2020.02.008

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*(August 2022), 103540. https://doi.org/10.1016/j.jnca.2022.103540

Holik, F., Flå, L. H., Jaatun, M. G., Yayilgan, S. Y., & Foros, J. (2022). Threat Modeling of a Smart Grid Secondary Substation. *Electronics (Switzerland)*, *11*(6), 1–21. https://doi.org/10.3390/electronics11060850

Inayat, U., Zia, M. F., Mahmood, S., Berghout, T., & Benbouzid, M. (2022). Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects. *Electronics (Switzerland)*, *11*(23), 1–16. https://doi.org/10.3390/electronics11233854

Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. *IEEE Transactions on Industrial Informatics*, *15*(12), 6522–6530. https://doi.org/10.1109/TII.2019.2931436

Kaur, N., & Kaur, P. (2014). Mitigation of SQL Injection Attacks using Threat Modeling. *ACM SIGSOFT Software Engineering Notes*, *39*(6), 1–6. https://doi.org/10.1145/2674632.2674638

Li, F., Valero, M., Zhao, L., Mahmoud, Y., Li, F. ;, Valero, M. ;, Zhao, L. ;, & Yousef, M. (2020). Cybersecurity Strategy against Cyber Attacks towards Smart Grids with PVs. *Research and Practice*, *1*. https://digitalcommons.kennesaw.edu/ccerphttps://digitalcommons.kennesaw.edu/ccerp/2020/Research/1

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). *Improving web application security: Threats and countermeasures*. Microsoft. https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

Mrabet, Z. El, Kaabouch, N., Ghazi, H. El, & Ghazi, H. El. (2018). Cyber-security in smart grid: Survey and challenges. *Computers and Electrical Engineering*, *67*, 469–482. https://doi.org/10.1016/j.compeleceng.2018.01.015

Omotosho, A., Ayemlo Haruna, B., & Mikail Olaniyi, O. (2019). Threat modeling of Internet of Things health devices. *Journal of Applied Security Research*, *14*(1), 106–121. https://doi.org/10.1080/19361610.2019.1545278

Sharma, K. R., Chiu, W.-Y., & Meng, W. (2023). Security Analysis on Social Media Networks via STRIDE Model. *19th International Conference on Networking and Services (ICNS 2023)*. http://arxiv.org/abs/2303.13075

Teymouri, A., Mehrizi-Sani, A., & Liu, C. C. (2018). Cyber security risk assessment of solar PV units with reactive power capability. *Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, *1*(October), 2872–2877. https://doi.org/10.1109/IECON.2018.8591583

Walker, A., Desai, J., Saleem, D., & Gunda, T. (2021). *Cybersecurity in Photovoltaic Plant Operations*. www.nrel.gov/publications.

Zhang, L., Taal, A., Cushing, R., de Laat, C., & Grosso, P. (2022). A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*, *21*(3), 509–525. https://doi.org/10.1007/s10207-021-00566-3