sustainability

MDPI

Article

Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability

Alexandre Rekeraho *, Daniel Tudor Cotfas, Titus C. Balan, Petru Adrian Cotfas, Rebecca Acheampong and Emmanuel Tuyishime

Electronics and Computers Department, Transilvania University of Brasov, 500036 Brasov, Romania
* Correspondence: alexandre.rekeraho@unitbv.ro

Abstract: The integration of Internet of Things (IoT) technologies into solar energy systems has transformed them into smart solar energy systems, enabling advanced real-time monitoring, control, and optimization. However, this connectivity also expands the attack surface, exposing critical components to cybersecurity threats that could compromise system reliability and long-term sustainability. This study presents a comprehensive cybersecurity threat modeling analysis for IoT-based smart solar energy systems using the STRIDE threat model to systematically identify, categorize, and assess potential security risks. These risks, if unmitigated, could disrupt operations and hinder large-scale adoption of solar energy. The methodology begins with a system use case outlining the architecture and key components, including sensors, PV modules, IoT nodes, gateways, cloud infrastructure, and remote-access interfaces. A Data Flow Diagram (DFD) was developed to visualize the data flow and identify the critical trust boundaries. The STRIDE model was applied to classify threats, such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege across components and their interactions. The DREAD risk assessment model was then used to prioritize threats based on the Damage Potential, Reproducibility, Exploitability, Affected Users, and Disability. The results indicate that most threats fall into the high-risk category, with scores ranging from 2.6 to 2.8, emphasizing the need for targeted mitigation. This study proposes security recommendations to address the identified threats and enhance the resilience of IoT-enabled solar energy systems. By securing these infrastructures, this research supports the transition to sustainable energy by ensuring system integrity and protection against cyber threats. The combined use of STRIDE and DREAD provides a robust framework for identifying, categorizing, and prioritizing risks, enabling effective resource allocation and targeted security measures. These findings offer critical insights into safeguarding renewable energy systems against evolving cyber threats, contributing to global energy sustainability goals in an increasingly interconnected world.

Keywords: cybersecurity; IoT security; sustainable energy; energy resilience; threat model; STRIDE; solar energy; renewable energy; smart solar energy; DREAD

Academic Editors: Oussama Laayati, Ahmed Chebak and Ahsen Maqsoom

Received: 15 January 2025
Revised: 6 March 2025
Accepted: 6 March 2025
Published: 9 March 2025

Citation: Rekeraho, A.; Cotfas, D.T.; Balan, T.C.; Cotfas, P.A.; Acheampong, R.; Tuyishime, E. Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability. *Sustainability* **2025**, *17*, 2386. https://doi.org/10.3390/su17062386

1. Introduction

The increasing need to address climate change, along with the demand for energy security and economic stability, has accelerated the transition to renewable energy worldwide [1,2]. Previously seen as an option, renewable energy is now recognized as a crucial response for reshaping societal interactions with the environment, promoting economic

development, and attaining energy independence [3]. The forecasts indicate that by 2050, renewable energy may comprise as much as two-thirds of the global primary energy supply [4]. This significant increase encompasses several renewable sources such as solar, wind, hydro, and bioenergy, all of which have experienced considerable technological improvements, enhanced operating efficiency, and reduced costs [5]. Solar energy has emerged as an example, with the cost of solar photovoltaic (PV) electricity decreasing substantially owing to technological advancements and economies of scale [6] Consequently, solar energy has become a competitive alternative to traditional fossil fuels in many regions, further accelerating its worldwide adoption [7].

The integration of modern technologies, such as IoT, has enhanced the inherent advantages of solar energy systems, thereby improving their functions and efficiency [8,9]. The Internet of Things (IoT) is a network of interconnected devices capable of real-time communication and data sharing [10]. The integration of the IoT transforms solar energy systems into smart solar systems, facilitating enhanced monitoring, control, and optimization capabilities [11]. Incorporating the IoT into solar energy systems enables sensors to collect real-time data on energy generation, environmental factors, and system efficacy. These data are then transmitted to cloud platforms, facilitating remote monitoring and allowing operators to monitor and manage system performance without physical presence. A further benefit of the IoT is predictive maintenance. IoT-enabled sensors facilitate early detection of system failures [12] and immediately generate alerts, enabling operators to mitigate possible issues prior to experiencing substantial downtime. This enhances system reliability and prolongs the operating lifespan of solar installations. Furthermore, dynamic energy management is facilitated by real-time data analysis, enabling systems to adjust energy output and distribution in response to demand [13]. This feature facilitates smart grid integration, enabling solar energy systems to interact with extensive energy networks to enhance the energy management efficiency [14].

However, although IoT integration enhances the functionality of solar energy systems, it also significantly increases the attack surface of the system and introduces new cybersecurity vulnerabilities [15]. The interconnected nature of IoT devices, involving extensive data exchange between sensors, gateways, and cloud platforms, exposes critical components to a wider range of cyber threats [16]. Real-time data transmission and remote access create opportunities for attackers to intercept or manipulate data, whereas the distributed nature of IoT devices makes securing the entire infrastructure more complex. Additionally, weaknesses in the system that allow device spoofing, data tampering, and denial-of-service attacks can compromise the integrity and availability of the system [17]. Moreover, the vulnerabilities present in IoT-enabled systems can have severe consequences, including the potential for large-scale power disruption. A notable example of this occurred during cyberattacks on Ukraine's electricity grid in December 2015, where attackers managed to manipulate circuit breakers, causing power outages by injecting malicious firmware into the system [18]. In this incident, attackers also launched denial-of-service (DoS) attacks on telecommunication networks, effectively cutting off communication between consumers and the grid [19]. As more devices become connected, the risk of cyberattacks increases, making it essential to implement comprehensive security measures.

Given the increased attack surface in IoT-enabled solar PV systems, threat modeling is essential for identifying and addressing potential security risks. Threat modeling is a structured approach that helps analyze a system's components, data flows, and vulnerabilities, giving security teams the ability to anticipate how attackers might exploit their weaknesses [20]. In these connected systems, where real-time data exchange is critical, threat modeling allows for a deeper understanding of high-risk areas and guides security efforts in a focused manner. This enables a comprehensive analysis of possible attack

vectors and vulnerabilities, allowing for the implementation of targeted defenses early in the design process, ultimately improving the system's overall security and resilience. In this study, we performed cybersecurity threat modeling for IoT-based smart solar energy systems using the STRIDE threat model [21] to identify and assess potential threats to the system. STRIDE offered a comprehensive approach for analyzing various threats targeting critical system components, including sensors, IoT nodes, IoT field gateways, IoT cloud gateways, cloud services, and remote access devices such as PCs and mobile devices. The STRIDE framework, developed by Microsoft [22], is a well-established methodology for identifying and categorizing security threats. However, their application to IoT-enabled smart solar energy systems provides valuable insights into the unique challenges of these interconnected environments, which combine IoT devices, cloud services, and renewable energy infrastructure. These systems face distinct risks owing to diverse components, critical trust boundaries across zones, and their reliance on real-time data exchange for monitoring and control. By categorizing threats, STRIDE enables a detailed analysis of vulnerabilities and maps threats to specific components and interactions. Even though STRIDE is effective for identifying threats, it does not provide a quantitative measure of their severity or prioritize them based on their potential impact. To address this limitation, this study integrates the DREAD [23] risk assessment approach into the threat modeling process. DREAD evaluates threats based on five key categories: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability, providing a quantitative basis for prioritizing threats and allocating security resources effectively. Current research threat modeling techniques do not fully address the complex interactions between IoT devices, cloud services, and remote user access in solar networks. The core research challenge addressed in this study is the lack of a systematic, structured approach to identifying and mitigating cybersecurity threats in IoT-based smart solar energy systems. The key scientific contributions of this study are as follows:

1. Tailored threat modeling for IoT-based solar systems: this study applies the STRIDE threat model specifically to IoT-based monitored and controlled solar energy systems, providing a structured method for addressing the unique security challenges faced by these systems;
2. Enhanced understanding of key system vulnerabilities: this study identifies critical threats, such as spoofing, tampering, denial of service, repudiation, information disclosure, and elevation of privilege, and assesses their impact on key components, such as sensors, IoT nodes, IoT gateways, cloud services, and local and remote users;
3. Proactive threat mitigation: using STRIDE at the system design stage, this research offers a proactive method for identifying and addressing potential threats early, helping reduce the risk of cyberattacks;
4. Broader implications for cyber–physical systems (CPS): the methodology extends beyond solar energy systems and can be applied to other CPS environments, such as smart grids and industrial control systems, offering a model for securing interconnected infrastructure.

This study focuses on the systematic identification and classification of cybersecurity threats in IoT-enabled solar energy systems using the STRIDE threat model. This study introduces an enhanced approach by applying the STRIDE threat model to IoT-enabled smart solar energy systems, considering multi-zone interactions (local user, cloud, and remote users). Unlike prior studies that focus on device-specific vulnerabilities, our work provides a comprehensive system-level threat analysis using a Data Flow Diagram (DFD) to evaluate security risks at different interaction points. Additionally, this study uniquely integrates cloud security risks, including threats at the IoT cloud gateway and cloud-based services, which have been underexplored in IoT solar security research. Therefore,

by classifying threats into distinct zones, the local user zone, cloud services zone, and remote user zone, we systematically identify security risks across all layers of the system architecture. Recent advancements in optimization and decision-making techniques offer enhancements for IoT-integrated smart solar energy systems. Intuitionistic fuzzy multi-objective transportation models aid in resource allocation under uncertainty [24], while multi-choice fractional stochastic models provide insights into optimizing security resource prioritization [25]. Even though this study focuses on STRIDE-based threat modeling, future research could explore integrating these approaches to enhance security decision-making in IoT-enabled energy networks.

This study aims to provide a foundational threat landscape that can inform subsequent risk assessments and targeted mitigation strategies. The structure of this paper is as follows: Section 2 reviews related work, discusses existing approaches and their limitations, and highlights the need for a specialized threat modeling approach for IoT-based smart solar energy systems. Section 3 outlines the research methodology, including the system use case and development of a Data Flow Diagram to map data interactions between system components. Section 4 presents the findings of the threat analysis, along with a discussion of the identified vulnerabilities and security recommendations to address them. Finally, Section 5 concludes this paper and summarizes the key takeaways of the research.

2. Related Works

The rapid adoption of IoT technologies across diverse sectors, including renewable energy, has led to substantial improvements in system efficiency, automation, and data-driven operation. Recent advancements in decentralized optimization algorithms have demonstrated their potential to improve energy management efficiency and system resilience. For instance, the authors in [26] proposed a risk-averse decentralized energy management strategy for integrated electricity and heat systems (IEHSs) using the TSA-AD-ADMM algorithm. Their approach leverages intelligent buildings (IBs). In addition to addressing vertical heating imbalances, it incorporates a conditional value-at-risk (CVaR) method to mitigate renewable energy and price risks. IoT-integrated smart solar energy systems can benefit from decentralized algorithms to enhance energy management and resilience. However, this increased level of connectivity has also expanded the attack surface, thereby introducing new cybersecurity challenges. Researchers have intensively studied the vulnerabilities inherent in IoT ecosystems, with a particular focus on identifying security risks and proposing mitigation strategies. Recent advancements have introduced innovative tools and methodologies to address the evolving IoT security landscape. Machine learning (ML) has emerged as a powerful tool for real-time threat detection and anomaly detection in IoT systems [27,28]. Supervised learning models enhance intrusion detection systems (IDSs) by accurately classifying malicious and benign activities, whereas unsupervised approaches, such as clustering, are effective in identifying novel threats in dynamic environments. The authors in [29] investigated a Non-Orthogonal Multiple Access (NOMA)-assisted secure offloading scheme for vehicular edge computing networks. These techniques have improved the ability to detect and respond to threats in IoT ecosystems. Blockchain technology offers a decentralized and tamper-proof ledger that ensures data integrity, secure communication, and device authentication within IoT systems [30]. By eliminating the need for centralized control, blockchain strengthens trust in IoT networks, particularly in distributed environments, where devices exchange sensitive data.

Software-defined networking (SDN) enhances IoT security by providing centralized control over network traffic, enabling dynamic threat mitigation, and better resource allocation [31]. This allows real-time policy enforcement, effectively countering distributed denial-of-service (DDoS) attacks and other network-based threats. Edge computing con-

tributes to IoT security by processing data closer to the source, reducing latency, and enhancing privacy [32]. This approach protects sensitive information before it is transmitted to cloud systems, thereby minimizing the risks of data breaches and unauthorized access. Similarly, Artificial Immune Systems (AISs) are gaining attention owing to their adaptive, self-learning capabilities to detect and neutralize abnormal behavior in IoT networks [33].

Moreover, there has been a growing emphasis on securing cyber–physical systems (CPSs), such as smart grids and other critical infrastructures, by employing various threat modeling techniques to assess potential attack vectors and vulnerabilities, enabling the development of robust defense mechanisms.

To enhance the detection and prevention of cyber-attacks in CPSs, the researchers in [34] developed a threat modeling approach that builds upon key elements of MITRE's ATT & CK for the ICS framework, adding a new layer for more in-depth security assessments. This approach evaluates and ranks threats based on the potential damage they could cause to the CPS, focusing on their impact on system degradation. The threat model is divided into two main parts: the adversary model and attack model. The adversary model characterizes the attacker's abilities and profile, considering factors such as the resources at their disposal, their technical skills, knowledge of the system, access privileges, and the opportunities they have to launch an attack, including the number of unsuccessful attempts. The attack model looks at the specifics of malicious activities, such as how often the attack can be repeated, how easily it can be reproduced, the CPS components targeted, and the steps involved in compromising the system. Using this threat model, researchers have proposed a CPS framework that identifies the hardware, software, and simulation tools required to accurately model CPS environments. These high-fidelity models were used to assess the performance of the system under different attack scenarios, thereby providing insights into its vulnerabilities.

In [35], the researchers developed a detailed threat modeling method for cyber–physical systems using the STRIDE methodology. The paper begins by outlining a practical and efficient approach to applying STRIDE and then tests it in a real-world scenario using a synchrophasor-based islanding testbed in a laboratory setting. This study investigated the types of threats that could emerge in each system component, depending on the absence of specific security properties, and how vulnerabilities within individual components could compromise the security of the entire system. The researchers concluded that STRIDE is a lightweight and effective tool for threat modeling in CPSs. Its simplicity allows security analysts to identify vulnerabilities more easily and plan appropriate component-level security measures during the system design stage.

In [36], the authors utilized two security threat modeling methodologies, Confidentiality, Availability, and Authentication (CIAA) and STRIDE, to examine and analyze potential attackers and their capabilities, motivations, and a range of threats within the context of fog computing. They proposed that conducting a detailed and systematic evaluation of threat models for fog computing would aid security experts and researchers in developing more secure and dependable fog computing systems. By applying both modeling processes, the authors provided a comprehensive overview of the security challenges and identified critical vulnerabilities that need to be mitigated.

In [37], the authors focused on the security and privacy challenges faced by smart cities, which monitor residents in real-time and provide intelligent services in areas such as energy, transportation, healthcare, and governance. Given growing concerns about security and privacy, it is crucial to address these issues to build trust and confidence among citizens, thus encouraging their participation in smart city services. The authors applied STRIDE, a threat modeling technique developed by Microsoft, to identify and categorize security threats in the complex infrastructure of smart cities. They also proposed

possible countermeasures for each identified threat, with the aim of enhancing the overall security framework of smart city systems.

In [38], the researchers proposed a broad threat model that addresses the attack surfaces of visual sensor network applications and their various components. The threats identified in this model were organized using the STRIDE model, while the associated vulnerabilities were categorized through Common Weakness Enumeration (CWE), a standard system for classifying security flaws. As a suggestion for future work, the authors recommend expanding this approach to encompass cyber–physical systems to further extend its scope and applicability.

Compared with other threat modeling approaches, such as MITRE ATT & CK [39], PASTA [40], and OCTAVE [41], STRIDE offers distinct advantages that align closely with the goals of this study. Its structured and systematic categorization of threats makes it particularly effective for analyzing the diverse and interconnected components of IoT-enabled solar energy systems. Although MITRE ATT & CK provides a comprehensive repository of adversarial tactics and techniques, its focus is on post-compromise scenarios rather than proactive architecture-level threat identification [42]. Similarly, PASTA integrates business impact analysis with technical threat modeling, offering a detailed risk-driven approach [43]; however, its complexity and resource requirements make it more suitable for enterprise-level applications. On the other hand, OCTAVE prioritizes organizational risk management, focusing on critical assets and vulnerabilities [44], but lacks the component-level granularity necessary for IoT architectures. STRIDE's simplicity and emphasis on system design and data flow vulnerabilities position it as a practical and focused choice for the specific needs of this study.

This emphasis on STRIDE underscores the critical role of a targeted and systematic threat modeling approach in securing IoT-enabled systems. Without a well-structured threat modeling approach, it is challenging to effectively identify and address potential vulnerabilities. The studies summarized in Table 1 illustrate the diverse applications of threat modeling methodologies across IoT domains. These studies provide valuable insights; however, they often focus on specific components or layers, such as device-level vulnerabilities or domain-specific threats (e.g., smart cities, precision agriculture, and smart homes). Moreover, based on our review, no prior work has fully employed the STRIDE methodology to construct a comprehensive threat model tailored specifically to the unique architecture and security demands of IoT-based solar energy systems. Therefore, our study fills this gap by employing a customized STRIDE methodology to address the unique security demands of IoT-based solar energy systems.

Table 1. Comparison of related work on threat modeling in IoT systems.

References	Methodology	Focus Area	Key Contributions	Limitations
[45]	Quantitative Threat Modeling	Industrial CPS	Quantitative approach for threat analysis with case studies.	Focuses on path analysis; lacks broader IoT integration.
[46]	STRIDE	Precision Agriculture	Identified 58 threats and provided general mitigations.	Limited applicability to large IoT infrastructures.
[47]	Vulnerability and Threat Analysis	IoT Devices	Analyzed vulnerabilities and proposed device-level controls.	Lacks system-level integration for IoT system.
[37]	STRIDE	Smart Cities	Categorized security-related threats for smart cities using STRIDE; categorizes them and suggests general countermeasures for each threat.	Limited applicability to smart cities.

Table 1. *Cont.*

References	Methodology	Focus Area	Key Contributions	Limitations
[48]	STRIDE and DREAD	IoT-Based Smart Home Systems	Applies STRIDE to identify threats across IoT device, communication, and application layers; uses DREAD to rate risks and propose risk mitigation strategies.	Focused on layer-specific threats; lacks system-level view and no focus for solar energy system.
[38]	STRIDE and CWE	Visual Sensor Networks	Identifies attack surfaces in visual sensor networks using STRIDE and categorizes vulnerabilities with CWE.	Limited to sensor-specific threats.
[36]	STRIDE and CIAA	Fog Computing	Combines STRIDE and CIAA to evaluate security threats and vulnerabilities in fog computing architectures.	Limited to fog computing.
Our study	Customized STRIDE and DREAD	IoT-Based Smart Solar Systems	Comprehensive threat model tailored to the unique architecture and security demands of IoT-based solar energy systems.	Applies to IoT-based smart solar energy systems. Application to other IoT domains may require adaptation

3. Methodology and System Architecture

3.1. Methodology

The overall methodology followed in this study is illustrated in Figure 1, which provides a structured visualization of the step-by-step threat modeling process applied to an IoT-based smart solar energy system. This process begins with the development of a use-case scenario, outlining the system architecture and operational behavior. The system is then decomposed into key components, including IoT sensors, PV modules, data acquisition nodes, IoT gateways, cloud infrastructure, and remote user interfaces. A Data Flow Diagram (DFD) [49] was subsequently created to map the flow of data between components, highlighting critical interaction points and trust boundaries within the system.

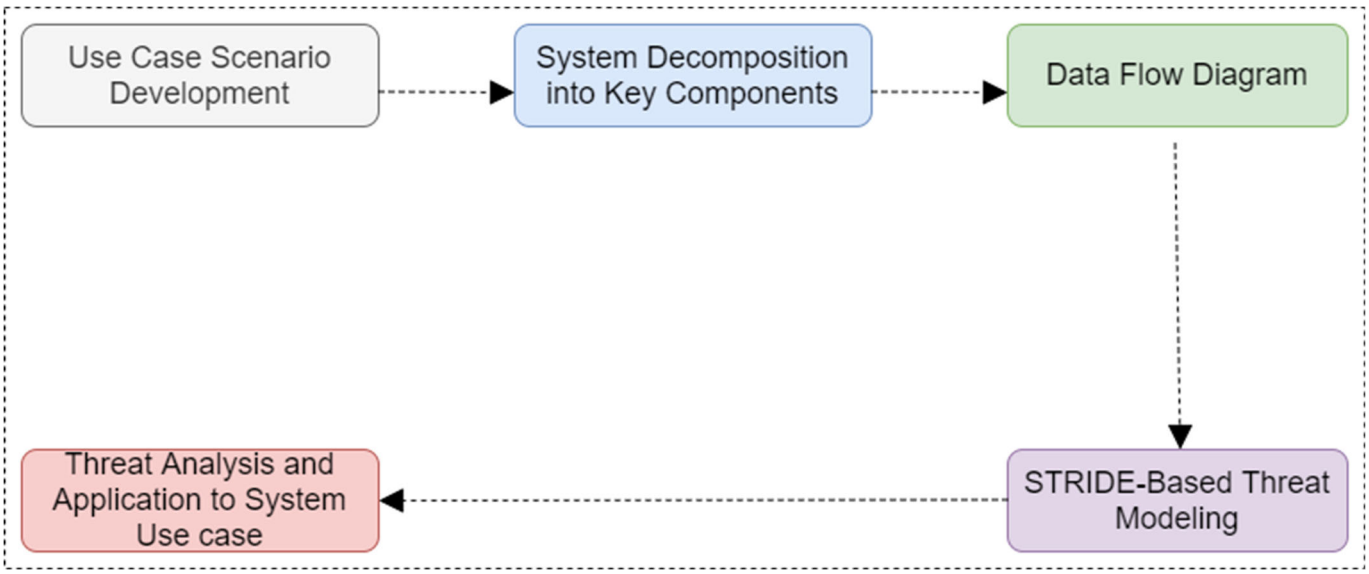

Figure 1. Methodology for cybersecurity threat modeling in IoT-based smart solar energy systems.

The STRIDE model was then applied to systematically identify potential security risks, including spoofing, tampering, repudiation, information disclosure, denial of service,

and elevation of privilege. The methodology ensures a comprehensive assessment of cybersecurity threats in IoT-enabled smart solar energy network.

3.2. System Use Case

Figure 2 outlines the architecture of a smart solar energy system, highlighting the integration of IoT devices, communication protocols, and cloud services. The system architecture was divided into four layers, each supporting real-time monitoring, control, and optimization to ensure scalability and functionality.

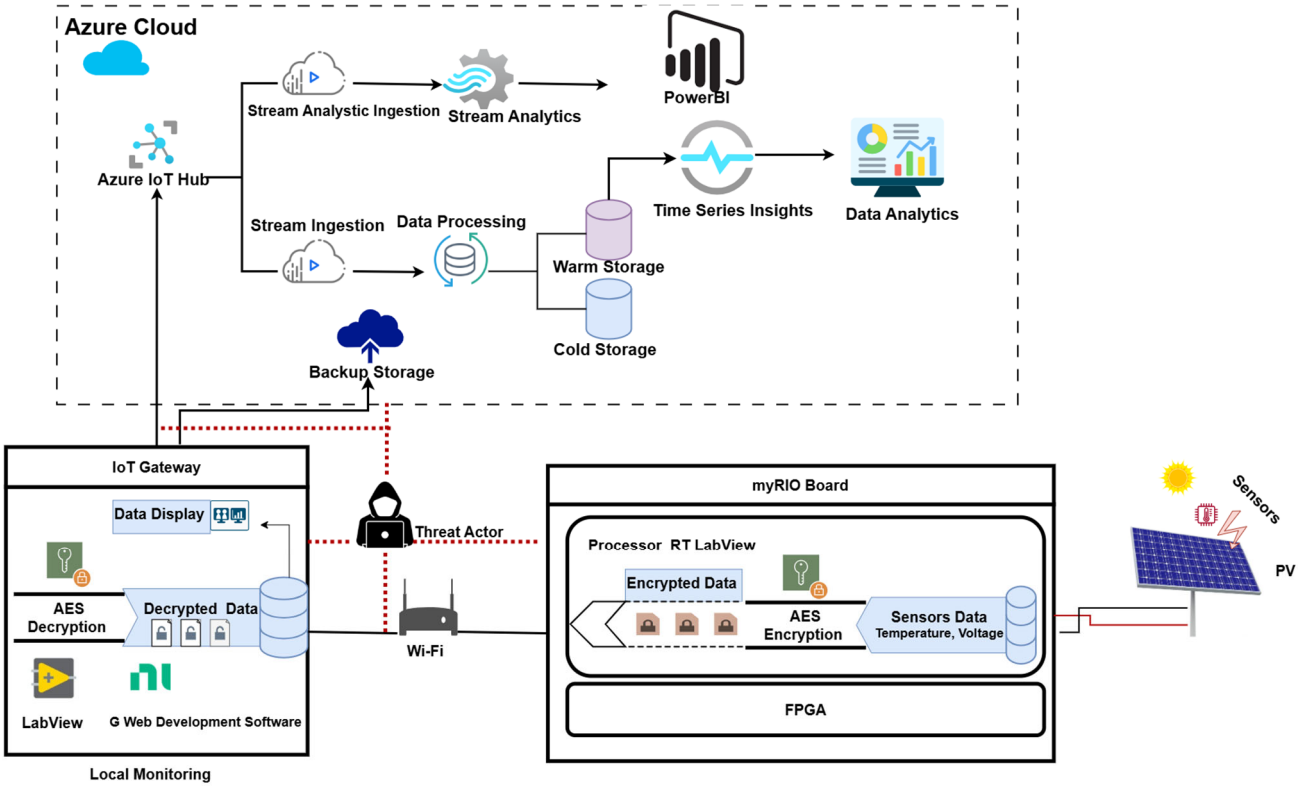

Figure 2. System architecture for the IoT-based smart solar energy system use case.

- The physical layer consists of PV modules and sensors that monitor key variables such as temperature, humidity, and voltage generated by the PV;
- The IoT node layer uses a myRIO device to collect and process sensor data in real time, performing localized control to estimate energy generation based on environmental conditions;
- The communication layer serves as a bridge between the field operations and cloud-based analytics. The IoT gateway facilitates local monitoring and control, while transmitting data to the cloud for further analysis;
- The cloud layer processes, stores, and visualizes data. Using the Azure IoT Hub, the system analyzes data for anomalies and optimization, stores them in both warm and cold storage, and presents insights through user-friendly dashboards.

The system architecture incorporates two distinct data ingestion streams, collectively referred to as stream gestion, which serve different purposes and enhance system functionality. The first stream is dedicated to real-time data analysis and visualization, facilitating operational insights through the integration of the Azure IoT Hub, Azure Stream Analytics, and Power BI. In this configuration, a consumer group is created within an IoT Hub to handle real-time data streams. Azure Stream Analytics processes the incoming data from the IoT Hub and directs it to Power BI, where the data are visualized to provide immediate

feedback on the system performance. More information on connecting the Azure IoT Hub and PowerBI can be found in [50]. The second stream focuses on routing data from the IoT Hub to the Azure Storage and Time Series Insights (TSI). A separate consumer group is established to manage this data stream, ensuring that data destined for storage—cold storage for long-term archival and warm storage for direct querying by the TSI—is appropriately handled. The TSI fetches input data from the IoT Hub and processes it, providing a detailed view of the system's performance over time. More information on implementing time-series insights can be found [51].

The selected IoT-based solar energy system serves as a representative use case for broader IoT architectures due to its integration of commonly used components such as IoT sensors, gateways, cloud services, and real-time data visualization platforms. The security risks identified in this study apply to IoT-based smart solar energy systems, which rely on interconnected devices for monitoring and control. Past cybersecurity incidents, such as attacks on power grids, highlight the growing cyber threats in energy infrastructure. This study addresses these risks by applying STRIDE threat modeling to an IoT-enabled solar energy system, a methodology adaptable to other IoT-based critical infrastructures, including smart grids, industrial IoT, and smart cities. Secure data transmission and device authentication remain as key challenges across these domains. In a previous study [16], we implemented an IoT-based remote monitoring system for solar energy using a PV module, sensors, a myRIO board, a PC as the IoT field gateway, and SystemLink Cloud for monitoring. This system focused on the efficient and secure monitoring of PV parameters, such as voltage and temperature. The key features of this architecture include the use of Advanced Encryption Standards (AESs) for secure data transmission and Wi-Fi for wireless communication between the myRIO board and the IoT field gateway. The encrypted data were sent to a PC for local monitoring and transferred to the SystemLink Cloud for remote monitoring via a user-friendly web-based interface. This study focuses on a representative subset of IoT devices commonly found in smart solar energy systems, including sensors, IoT nodes, IoT field gateways, IoT cloud gateways, and cloud-based services. Though a wide range of IoT devices exist in the market, this paper analyzes security challenges specific to these key components due to their role in system monitoring, data transmission, and control for our use case. The findings and proposed security measures provide a structured approach that can be adapted to other IoT architectures with similar functionalities. This prior work demonstrates a practical example of IoT-enabled solar energy monitoring, addressing key challenges, such as secure data transmission and remote accessibility. This study builds on such systems by applying the STRIDE threat model to systematically identify and address potential vulnerabilities across various components. Therefore, the threat model presented in this study offers scalable security solutions that can enhance the resilience of similar architectures.

3.3. System Decomposition into Key Components

To better understand the architecture of the IoT-based smart solar energy system and its operation, the system was broken down into its key functional components. Each component plays a crucial role in ensuring that the system operates efficiently and supports its intended purpose. The main components are as follows:

- Sensors and PV modules: these devices are the starting point of the system, gathering essential data such as voltage, current, energy production, and environmental factors such as temperature and sunlight. This real-time information forms the basis for monitoring and managing the performance of the solar energy system;
- IoT nodes (myRIO Board): at the heart of local processing, the IoT node collects and processes data from the sensors. The myRIO board, an integral part of this

setup, extends beyond data aggregation by enabling control functions. For example, it allows direct system adjustments, such as fine-tuning operations, to maintain optimal performance;

- IoT gateways: these gateways act as a bridge between the local system and the cloud. They ensure that data from IoT nodes are transmitted securely and seamlessly to cloud services, where they can be further processed and stored. Moreover, the system can be locally monitored at this level;
- Cloud services: the cloud serves as the brain of the system, handling data storage, analytics, and visualization. It allows for real-time insights and long-term trend analysis, helping stakeholders make data-driven decisions regarding system operations and performance;
- Remote user interfaces: these interfaces are the point of interaction for end-users and administrators, providing access to monitor the system's performance and issue control commands when needed. They deliver real-time insights and actionable data through intuitive dashboards, thereby ensuring that the system remains efficient and responsive.

The local user zone, cloud services zone, and remote user zone are interconnected through a continuous flow of data and control commands. Data generated by sensors and IoT nodes in the local user zone are transmitted to the cloud services zone for storage, analysis, and visualization. These data are then accessed by remote users through cloud-based dashboards, enabling real-time monitoring and control. However, this interdependence introduces significant risks. For example, a breach in the cloud services zone could allow attackers to manipulate data sent to remote users, leading to incorrect system adjustments or even complete system shutdowns. Similarly, a compromised remote user device could be used to inject malicious commands into the cloud, which could then propagate to the local user zone, disrupting physical operations. Breaking the system into these components provides a clear and structured view of how each component contributes to its functionality. This understanding lays the foundation for further analysis.

3.4. Data Flow Diagram (DFD)

The DFD in Figure 3 provides a representation of the operation of the IoT-based smart solar energy system. It shows the flow of data between components and highlights the interactions that enable both the monitoring and control of the system. The process starts with data generated at the sensors and moves through various stages, including local processing, cloud storage and analysis, and user-driven actions. This ensures that the system operates efficiently while enabling real-time communication and decision-making.

At the starting point, sensors connected to the PV modules collect real-time operational data such as voltage, current, and temperature. These data are sent to an IoT node (myRIO), which processes the readings and prepares them for further use. The IoT node also plays a role in responding to control commands. For instance, a local user can send a command to recalibrate the sensors or adjust the system parameters to optimize the energy performance.

The data are then forwarded to the IoT field gateway, which serves as a bridge between the local system and the cloud. The field gateway transmits the processed data to the IoT cloud gateway (Azure IoT Hub), which is a key component that ensures reliable communication with the cloud infrastructure. This step is essential for transferring data and maintaining connectivity between the different parts of the system.

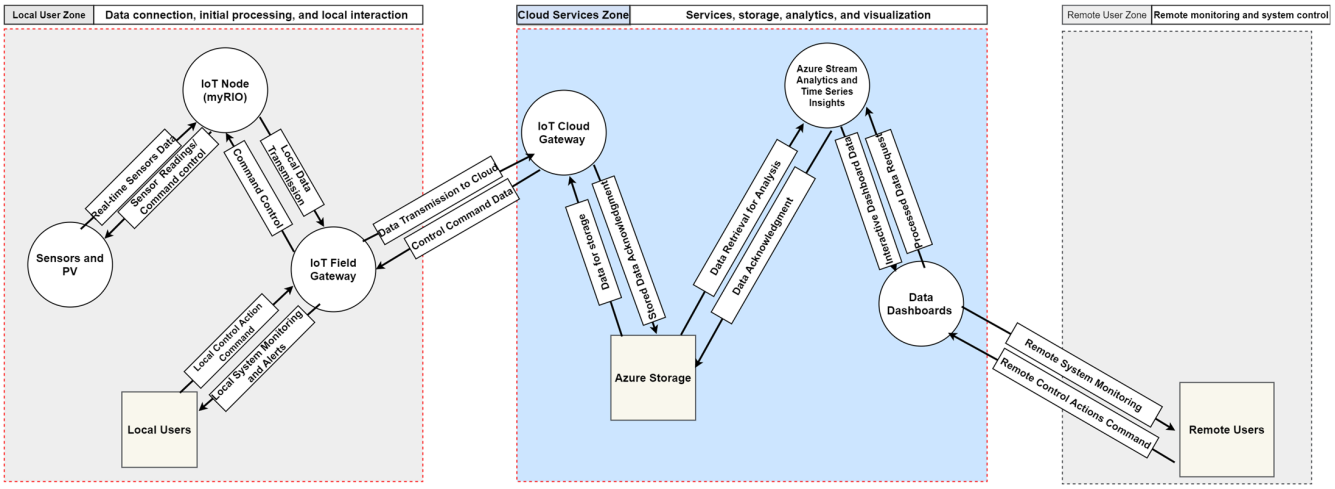

Figure 3. Data Flow Diagram.

Once in the cloud infrastructure, the data are stored in the Azure Storage. Storage is categorized as follows:

Cold storage: used for archiving historical data, which can later be analyzed for trends or system optimization;

Warm storage: allows for direct querying and real-time analysis through Azure Time Series Insights (TSI), enabling immediate monitoring and quick fault detection.

The stored data were further processed using tools such as Azure Stream Analytics and Time Series Insights, which analyze both real-time and historical data to identify performance trends, detect faults, and generate insights. The results of this analysis are presented on Interactive Dashboards, making the information accessible to users for decision making. These dashboards allow users to interact with the system effectively; a remote user might analyze the dashboard and spot a critical issue, such as unusual energy output. To prevent further damage, the user can send a command through the cloud to shut down the system or adjust operational parameters. Similarly, a local user can access real-time performance data and issue control commands via an IoT field gateway. For example, the user may reset the components or adjust the energy loads to restore the efficiency of the system. The overall flow of the data and control commands can be summarized as follows:

- Real-time data are generated by sensors and processed at an IoT node (myRIO);
- The IoT field gateway transmits these data to the Azure IoT Hub;
- Data are stored in Azure Storage (cold or warm) and analyzed using Stream Analytics and TSI;
- Results are displayed on Interactive Dashboards for users to monitor and evaluate;
- Users issue control commands that flow back through the IoT Hub and field gateway to the IoT node for execution.

The two-way flow of data and control commands ensures that the system is responsive, efficient, and adaptable. By allowing both local and remote users to monitor real-time performance, detect anomalies, and take immediate action, the system achieves a high degree of flexibility and reliability.

The system has been classified into three zones: the local user zone, cloud services zone, and remote user zone. This classification not only organizes the flow of data but also helps to systematically identify potential threats and risks within each zone. By analyzing these zones individually, it becomes easier to pinpoint vulnerabilities specific to local operations, cloud infrastructure, and remote interactions, ensuring a comprehensive assessment of security risks across the entire system

3.5. STRIDE Threat Analysis Process Methodology

Figure 4 illustrates the structured methodology for conducting the STRIDE threat analysis. The process begins by selecting a specific STRIDE threat for investigation, followed by choosing an element from the DFD for analysis. Each identified threat was analyzed to determine its potential impact on the system. This process is repeated for each DFD element and STRIDE threat until all components have been analyzed, ensuring comprehensive coverage of potential vulnerabilities.

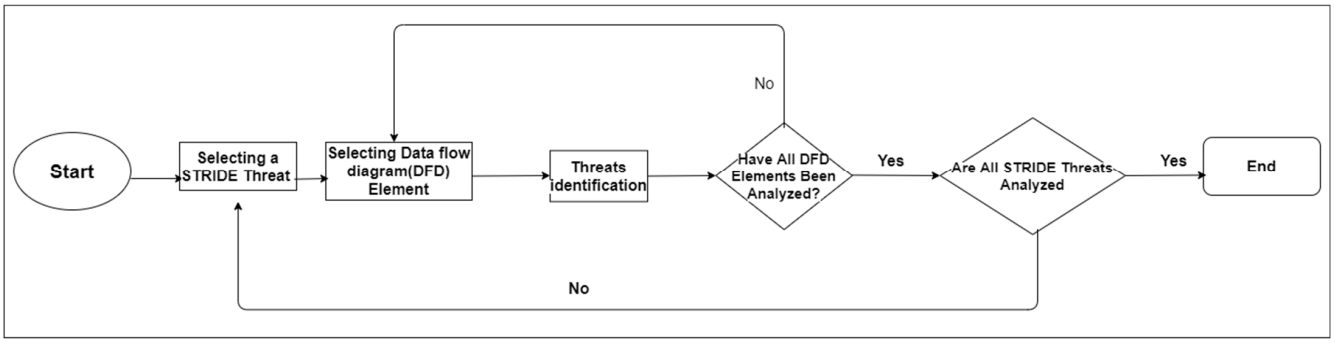

Figure 4. Flowchart of STRIDE threat analysis process.

3.6. Risk Assessment Using DREAD Approach

To complement the STRIDE threat modeling and provide a quantitative basis for prioritizing identified threats, this study employs the DREAD risk assessment model. DREAD [52] evaluates the severity of security threats based on five key categories: Damage Potential (D), Reproducibility (R), Exploitability (E), Affected Users (A), and Discoverability (D). Each category is scored on a scale of 1 (low) to 3 (high), and the overall risk score for a threat is calculated using the formula: Risk Score = (D + R + E + A + D)/5.

Damage Potential measures the severity of the impact if the threat is realized, with high scores indicating significant harm such as system failure or data corruption. Reproducibility evaluates how easily the attack can be reproduced, with high scores indicating that the attack can be consistently replicated with minimal effort. Exploitability assesses the effort and resources required to exploit the vulnerability, with high scores indicating that the attack can be executed with minimal technical skill or resources. Affected Users estimates the scale of the impact in terms of the number of users, devices, or systems affected, with high scores indicating a large portion of the system or user base could be impacted. Discoverability evaluates how easily the vulnerability can be discovered by attackers, with high scores indicating that the vulnerability is well documented, easily detectable, or publicly known. The overall risk score is categorized into three levels: Low (1.0–1.5) for minimal impact and low priority, Medium (1.6–2.5) for moderate impact and medium priority, and High (2.6–3.0) for severe impact and high priority. The DREAD framework was applied to each specific threat identified in the STRIDE analysis for the local user zone, cloud service zone, and remote user zone, enabling a structured approach to prioritizing threats and allocating security resources effectively. By integrating DREAD with STRIDE, this study provides a quantitative measure of threat severity.

4. Results and Discussion

Given the complex nature of our smart solar energy system, which spans local user interactions to cloud-based services, STRIDE threat modeling offers a systematic way to evaluate security risks across the entire system architecture. Each zone—local users, cloud services, and remote users—presents unique vulnerabilities. Using STRIDE, how data flows through these zones and where trust boundaries might expose the system to potential

threats were assessed. The primary goal of this evaluation is to develop targeted strategies to mitigate these risks and ensure that the system remains resilient to cyberattacks.

The STRIDE threat model categorizes security threats into six categories. Each of these categories affects a specific aspect of a system's security, including authentication, integrity, confidentiality, availability, and authorization.

- Spoofing threatens authentication by allowing attackers to impersonate legitimate users and devices;
- Tampering compromises integrity by enabling unauthorized changes to the data;
- Repudiation undermines non-repudiation and allows users to deny their actions or transactions;
- Information disclosure jeopardizes confidentiality by exposing sensitive information;
- Denial of service (DoS) affects availability, rendering services or systems inaccessible;
- The elevation of privileges bypasses authorization controls, allowing unauthorized actions or access.

4.1. Threat Analysis and Risk Assessment for Local User Zones in Smart Solar Energy Systems

The STRIDE threat model analysis in Table 2 identifies critical security risks within the local user zone of the smart solar energy system, encompassing components such as sensors, the IoT node, local users, and the IoT field gateway. Spoofing risks are identified when attackers impersonate legitimate sensors or users, potentially injecting false data or making unauthorized modifications. Tampering poses a threat by altering the data during transmission between the IoT node and the IoT field gateway, leading to incorrect system behavior. Repudiation risks arise from local users denying responsibility for system changes, complicating incident response and accountability. Information disclosure vulnerabilities expose sensitive operational data during transmission, thereby increasing the likelihood of further exploitation. DoS attacks can overwhelm critical components, such as the IoT node and gateway, disrupting system availability and hindering real-time operations. Finally, the elevation of privilege threats enable unauthorized users to gain administrative access, leading to harmful system modifications.

Table 2. STRIDE threat analysis for local user zone.

Threat Category/STRIDE	Component/Communication Flow	Identified Threat	Associated Risk
Spoofing (S)	Sensors to IoT Node	Sensor impersonation	Incorrect data leads to poor system actions, risking damage.
Spoofing (S)	Local User to IoT Field Gateway	Attacker posing as a legitimate user	Unauthorized access may alter system settings.
Tampering (T)	IoT Node to IoT Field Gateway	Data alteration during transmission	Manipulated data impacts energy management decisions.
Tampering (T)	Sensors	Physical manipulation of sensors	False readings disrupt system performance.
Repudiation (R)	Local User to IoT Node	Denial of responsibility for system changes	Lack of accountability hinders issue resolution.

Table 2. *Cont.*

Threat Category/STRIDE	Component/Communication Flow	Identified Threat	Associated Risk
Information Disclosure (I)	IoT Node	Exposure of sensitive system data	Leaked data exposes system vulnerabilities.
Information Disclosure (I)	Sensors to IoT Node	Data interception during transmission	Compromised data reveals critical information.
Denial of Service (D)	IoT Field Gateway	Overloading of gateway with excessive requests	Disrupted communication affects system control.
Elevation of Privilege (E)	Local User	Unauthorized elevation of user privileges	Unauthorized access allows harmful changes.

To further prioritize these threats and provide a quantitative basis for decision-making, the DREAD risk assessment framework was applied. DREAD evaluates each threat based on five key categories: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. The results of this assessment are presented in Table 3.

Table 3. Risk assessment for local user zone.

Threat Category	Specific Threat	Damage (D)	Reproducibility (R)	Exploitability (E)	Affected Users (A)	Discoverability (D)	Risk Score (Avg)	Risk Level
Spoofing (S)	Sensor impersonation	3	2	2	3	3	2.6	High
Spoofing (S)	Attacker posing as a legitimate user	3	2	2	3	2	2.4	Medium
Tampering (T)	Data alteration during transmission	3	3	2	3	2	2.6	High
Tampering (T)	Physical manipulation of sensors	3	2	2	3	2	2.4	Medium
Repudiation (R)	Denial of responsibility for changes	2	2	1	2	2	1.8	Medium
Information Disclosure (I)	Exposure of sensitive system data	3	2	2	3	3	2.6	High
Information Disclosure (I)	Data interception during transmission	3	2	2	3	3	2.6	High
Denial of Service (D)	Overloading of gateway with requests	3	3	3	3	2	2.8	High
Elevation of Privilege (E)	Unauthorized elevation of user privileges	3	2	2	3	2	2.4	Medium

The DREAD risk assessment reveals that several threats in the local user zone pose a High Risk, with risk scores ranging from 2.6 to 2.8. For example, sensor impersonation received a risk score of 2.6, reflecting its potential to cause significant damage through incorrect data inputs, its moderate Reproducibility, and its high Discoverability. Similarly, overloading the gateway with excessive requests (a specific instance of denial of service)

scored 2.8, the highest risk score in the local user zone. This threat poses a severe risk to system availability, as it can disrupt communication between critical components, rendering the system unresponsive. Other high-risk threats include data alteration during transmission and exposure of sensitive system data, both scoring 2.6.

In contrast, threats such as attacker posing as a legitimate user, physical manipulation of sensors, and unauthorized elevation of user privileges were categorized as Medium Risk (scores: 2.4), as they require more effort to exploit or have a more limited impact. Repudiation was also categorized as a Medium Risk (score: 1.8), as it primarily affects accountability rather than system functionality.

4.2. Cloud Services Zone Threat Analysis and Risk Assessment in Smart Solar Energy Systems

The cloud services zone is a crucial part of the smart solar energy system, managing the flow, storage, and analysis of data from IoT devices in the local user zone. This zone includes essential components, such as the IoT cloud gateway (Azure IoT Hub), Cloud Storage, Stream Analytics, and dashboards for user interaction and system control. The STRIDE-based threat analysis in Table 4 highlights the key vulnerabilities and the associated risks within this zone.

Table 4. STRIDE threat analysis for the cloud services zone.

Threat Category	Component/Communication Flow	Identified Threats	Associated Risk
Spoofing (S)	IoT Field Gateway to Cloud Gateway (Azure IoT Hub)	IoT field gateway may be impersonated by an attacker	Unverified devices could send false data, leading to inaccurate analytics or misconfigurations.
Tampering (T)	Data Flow from IoT Field Gateway to Cloud Gateway	Data interception or alteration during transmission	Modified data could cause inaccurate decisions or system errors.
Tampering (T)	Cloud Storage	Alteration of stored historical data	Changing stored data may result in faulty analytics and skew future predictions.
Information Disclosure (I)	IoT Field Gateway to Cloud Gateway	Exposure of sensitive data during transmission	Leaked data could reveal system weaknesses, aiding potential attackers.
Information Disclosure (I)	Cloud Storage	Unauthorized access to cloud-stored data	Leaked data could be used to launch more precise attacks.
Denial of Service (D)	Stream Analytics	Flooding the system with excess data	Overload may cause delays or failures in analytics, leading to system inefficiencies.
Elevation of Privilege (E)	Cloud Dashboard and Admin Control Access	Attackers could gain unauthorized admin access	Gaining higher access may allow attackers to alter system configurations or disable security controls.

Spoofing presents a significant risk where attackers can impersonate the IoT cloud gateway or remote users by injecting false data into the cloud. This can lead to incorrect analytics and system misconfigurations, ultimately affecting the system performance and reliability. Tampering during data transmission between the IoT cloud gateway and cloud

storage is another concern, as altered data can result in faulty decisions, disrupting both short-term operations and long-term optimization. Additionally, manipulating historical data stored in the cloud can compromise future system analyses and forecasts.

Repudiation is a risk when remote users access the system through dashboards, as users might deny making critical changes without adequate tracking, thus making it difficult to hold them accountable. Information disclosure poses a serious threat, especially if sensitive operational data are leaked during transmission owing to poor encryption, giving attackers valuable insights into system vulnerabilities.

DoS attacks targeting the IoT cloud gateway or Stream Analytics could overwhelm these systems, leading to delays or even outages, which could disrupt real-time control and monitoring. Lastly, elevation of privilege represents a high risk, as unauthorized access to administrative controls could allow attackers to make harmful changes across the system, compromising its overall security and stability.

To further assess the severity of these threats and optimize resource allocation, a risk assessment framework was utilized. DREAD evaluates threats across five key dimensions: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. The results of this assessment are summarized in Table 5. The findings indicate that most threats within the cloud services zone are categorized as High Risk, with scores ranging from 2.6 to 2.8. For example, the IoT field gateway impersonation threat received a score of 2.6, highlighting its ability to disrupt system operations by injecting false data, its moderate Reproducibility, and the high likelihood of being detected by attackers. Similarly, the denial-of-service (DoS) threat caused by flooding the system with excess data had the highest risk score of 2.8, reflecting its potential to overload cloud services, resulting in delays or failures in data processing and overall system functionality. Other high-risk threats include data interception or alteration and exposure of sensitive data during transmission, both scoring 2.6 due to their significant impact on data integrity and confidentiality.

Table 5. Risk assessment for cloud services zone.

Threat Category	Specific Threat	D	R	E	A	D	Risk Score (Avg)	Risk Level
Spoofing (S)	IoT field gateway impersonation	3	2	2	3	3	2.6	High
Tampering (T)	Data interception or alteration	3	3	2	3	2	2.6	High
Tampering (T)	Alteration of stored historical data	3	2	2	3	2	2.4	Medium
Information Disclosure (I)	Exposure of sensitive data during transmission	3	2	2	3	3	2.6	High
Information Disclosure (I)	Unauthorized access to cloud-stored data	3	2	2	3	3	2.6	High
Denial of Service (D)	Flooding the system with excess data	3	3	3	3	2	2.8	High

Table 5. *Cont.*

Threat Category	Specific Threat	D	R	E	A	D	Risk Score (Avg)	Risk Level
Elevation of Privilege (E)	Unauthorized admin access	3	2	2	3	2	2.4	Medium
Tampering (T)	Alteration of stored historical data	3	2	2	3	2	2.4	Medium

Conversely, threats such as alteration of stored historical data and unauthorized admin access were assessed as Medium Risk, each scoring 2.4. These threats still present notable security concerns; nevertheless, they are considered less critical than high-risk threats due to lower Exploitability or a more restricted impact. For instance, modifying historical data requires access to storage systems, whereas unauthorized admin access relies on exploiting specific vulnerabilities.

4.3. Remote User Zone Threat Analysis and Risk Assessment

In the remote user zone, individuals use PCs and mobile devices to monitor and control smart solar energy systems through cloud-based services. However, this setup introduces several security risks.

Spoofing: attackers can impersonate legitimate users by stealing or guessing credentials using techniques such as phishing [53], malware, or exploiting weak passwords. This can grant unauthorized access to cloud dashboards, enabling them to alter system configurations or steal sensitive data;

Tampering: unsecured communication channels between remote devices and cloud services are vulnerable to interception and modification. Attackers can manipulate data packets, resulting in incorrect commands or misleading analytics. In addition, compromised devices can send unauthorized instructions to the system, thereby affecting its operation;

Repudiation: without proper logging and tracking systems, users or attackers can deny their involvement in critical actions. This lack of accountability complicates efforts to trace unauthorized changes, respond to incidents, and undermine system security;

Information disclosure: unencrypted communication exposes eavesdroppers to critical data, such as system settings, operational metrics, and credentials. If devices are compromised, they can leak sensitive information, giving attackers further access to the system;

Denial of service: attackers can overwhelm cloud services or remote devices with excessive traffic, rendering them nonfunctional. This prevents legitimate users from controlling or monitoring the system, potentially causing operational problems;

Elevation of privilege: exploiting vulnerabilities in user accounts or devices enables attackers to gain unauthorized access levels. With administrative privileges, they can make unrestricted changes, thereby putting the system's stability and security at risk. Table 6 summarizes the threats in the remote user zone.

Table 6. STRIDE threat analysis for the remote user zone.

Threat Category (STRIDE)	Component/Communication Flow	Identified Threat	Associated Risks
Spoofing (S)	Remote User Devices (PC/Mobile)	Attackers steal credentials to impersonate users	Unapproved access leads to malicious actions or data breaches.
Spoofing (S)	Data Transmission between User Devices and Cloud	Data interception and manipulation	Altered data cause faulty system operations or inaccurate analytics.

Table 6. *Cont.*

Threat Category (STRIDE)	Component/Communication Flow	Identified Threat	Associated Risks
Tampering (T)	Remote User Devices	Malware changes apps or system settings	Unauthorized commands or data leaks can occur.
Repudiation (R)	User Actions on Cloud Dashboard	Users deny performing key actions due to lack of logging	Poor accountability makes auditing and incident response difficult.
Information Disclosure (I)	Unencrypted Communication Channels	Data are exposed during transmission	Attackers can access sensitive system data or credentials.
Information Disclosure (I)	Remote User Devices	Compromised devices expose credentials or data	Leaked information enables further system attacks.
Denial of Service (D)	Remote Access Services	Attackers flood cloud services used by remote users	Legitimate users lose access, disrupting system control.
Denial of Service (D)	Remote User Devices (PC/Mobile)	DoS attacks render devices inoperable	Users can not remotely monitor or control the system.
Elevation of Privilege (E)	Remote User Accounts	Attackers exploit vulnerabilities for higher privileges	Full administrative access allows system-wide control.

To further evaluate the severity of these threats, the DREAD risk assessment framework was applied. DREAD assesses threats across five dimensions: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. The outcomes of this assessment are detailed in Table 7. The DREAD assessment reveals that the majority of threats in the remote user zone are classified as High Risk, with scores ranging from 2.6 to 2.8. For example, attackers stealing credentials to impersonate users scored 2.8, the highest risk score in this zone. This threat poses a severe risk, as it allows attackers to gain unauthorized access, potentially leading to malicious actions or data breaches. Similarly, flooding cloud services with excessive requests (a denial-of-service threat) also scored 2.8, highlighting its potential to disrupt system access for legitimate users and compromise system control. Other high-risk threats include data interception and manipulation and exposure of sensitive data during transmission, both scoring 2.6 due to their severe impact on data integrity and confidentiality.

Table 7. Risk assessment for remote user zone.

Threat Category	Specific Threat	D	R	E	A	D	Risk Score (Avg)	Risk Level
Spoofing (S)	Attackers steal credentials to impersonate users	3	3	2	3	3	2.8	High
Spoofing (S)	Data interception and manipulation	3	2	2	3	3	2.6	High
Tampering (T)	Malware changes apps or system settings	3	2	2	3	2	2.4	Medium

Table 7. *Cont.*

Threat Category	Specific Threat	D	R	E	A	D	Risk Score (Avg)	Risk Level
Repudiation (R)	Users deny performing key actions due to lack of logging	2	2	1	2	2	1.8	Medium
Information Disclosure (I)	Data are exposed during transmission	3	2	2	3	3	2.6	High
Information Disclosure (I)	Compromised devices expose credentials or data	3	2	2	3	3	2.6	High
Denial of Service (D)	Attackers flood cloud services used by remote users	3	3	3	3	2	2.8	High
Denial of Service (D)	DoS attacks render devices inoperable	3	2	2	3	2	2.4	Medium
Elevation of Privilege (E)	Attackers exploit vulnerabilities for higher privileges	3	2	2	3	2	2.4	Medium

In contrast, threats such as malware changing apps or system settings, denial-of-service attacks rendering devices inoperable, and exploitation of vulnerabilities for higher privileges were rated as Medium Risk (scores: 2.4). Despite the fact that these threats still pose significant risks, they are less urgent than high-risk threats due to their lower Exploitability or more limited scope of impact. For instance, malware attacks require the installation of malicious software, and DoS attacks on individual devices affect only a subset of users. Notably, none of the threats in the remote user zone were classified as Low Risk (1.0–1.5), indicating that all identified threats require some level of attention. These findings emphasize the importance of implementing robust security measures to address the identified risks

The integration of the STRIDE threat modeling and DREAD risk assessment frameworks across the local user zone, cloud services zone, and remote user zone has provided a systematic prioritization of cybersecurity risks in IoT-enabled smart solar energy systems. The analysis revealed that the majority of threats fall into the high-risk category, with scores ranging from 2.6 to 2.8, even though a smaller subset was classified as Medium Risk, with scores between 1.8 and 2.4. Notably, no threats were identified as Low Risk, underscoring the critical need for comprehensive security measures.

The interdependence between the local user zone, cloud services zone, and remote user zone creates a complex risk landscape where vulnerabilities in one zone can cascade to others. For instance, if an attacker successfully spoofs a sensor in the local user zone, they can inject false data into the cloud services zone. These false data could lead to incorrect analytics, resulting in harmful control commands being sent back to the local system, potentially causing physical damage or operational disruptions. Similarly, a denial-of-service (DoS) attack on the cloud services zone could prevent remote users from accessing critical monitoring and control functions, leading to operational inefficiencies or even system failures. Furthermore, if a remote user's credentials are compromised, attackers could gain unauthorized access to the cloud services zone, allowing them to manipulate data or send malicious commands to the local user zone. These examples highlight the

necessity of a multi-layer defense approach, where security measures are implemented at each zone to mitigate the risk of cascading failures.

4.4. Security Controls Recommendations for IoT Based Smart PV System

1. Intrusion Detection and Prevention Systems

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are important for maintaining system integrity [54,55]. An IDS monitors operations, device behaviors, and network traffic to detect potential security breaches such as malware, unauthorized access, and abnormal activities [56]. They provide the early detection of threats and generate logs for post-incident analysis [57]. An IDS can be signature-based (for example, Zeek [58], Suricata [59], and Snort [60]), comparing activities against known patterns, or anomaly based, which detects deviations from normal behavior. In contrast, anomaly-based IDSs work by establishing a baseline of normal network behavior and then detecting deviations from this norm.

The IPS extends IDS functionality by not only detecting threats but also blocking suspicious traffic and isolating compromised devices [61]. This proactive approach reduces risks but may occasionally block legitimate actions, requiring careful configuration and monitoring. IDSs and IPSs are critical for intelligent PV systems, where large data flows from sensors and control systems require constant monitoring of irregularities. Regular updates to detection methods ensure that these systems remain effective in the dynamic cybersecurity landscape. Advancements in IDSs include hybrid systems that monitor both physical and cyber networks, offering comprehensive protection against cyber–physical attacks on distributed energy resources (DERs) [62].

The implementation of an IDS/IPS in IoT-enabled solar energy systems is a promising approach for enhancing cybersecurity. However, several challenges must be addressed to ensure that these systems are deployed effectively. One obstacle lies in the resource constraints inherent in IoT devices [63], such as sensors and gateways. These devices often have limited computational power and memory, rendering full-scale IDS/IPS solutions challenging. Lightweight frameworks specifically designed for such environments become important aspect in mitigating these limitations.

Another challenge is the complexity involved in configuring the anomaly-based IDS solutions. Although effective, these systems require extensive tuning to balance false positives and false negatives. This process demands not only technical expertise but also ongoing efforts, particularly in highly dynamic and interconnected IoT ecosystems, such as smart solar energy systems. Additionally, the financial costs associated with deploying advanced IDS/IPS solutions, including hardware, software licenses, and skilled personnel, can create barriers, particularly for smaller projects with budget constraints. Integration with the existing IoT infrastructure further complicates implementation. Many systems rely on legacy devices and protocols, necessitating significant customization to ensure compatibility. Such efforts often extend deployment timelines and demand additional resources, thus underscoring the need for strategic planning and incremental adoption.

Despite these challenges, there are viable strategies to enhance its feasibility. Lightweight IDS/IPS solutions designed for IoT environments can alleviate resource demands, whereas a phased implementation approach prioritizes critical components like gateways and cloud interfaces, enabling resource allocation to be managed effectively. Continuous updates to detection algorithms and staff training are essential for adapting to evolving threat landscapes and for maintaining system resilience. By carefully navigating these challenges and adopting targeted mitigation strategies, the benefits of the IDS/IPS can be realized, contributing to the development of secure and sustainable IoT-enabled solar energy systems.

2. Access Control and User Authentication

Incorporating IoT technology into smart PV systems requires strict access control and authentication mechanisms to protect the sensitive data. Access control restricts system access to authorized individuals, and user authentication verifies their identity. Role-based access ensures that users access only the functions necessary for their roles, thereby reducing insider threats.

Multifactor authentication (MFA) [64], robust password policies, and biometrics strengthen user authentication by requiring multiple verification methods. These mechanisms protect critical system data and components, and mitigate the risks associated with unauthorized access or malicious behavior. Proper planning, maintenance, and updates are crucial to ensure that these controls adapt to emerging cybersecurity threats.

Access control and user authentication are fundamental to securing IoT-enabled solar energy systems, as they prevent unauthorized access and ensure that only legitimate users can interact with critical system components. However, the implementation of these mechanisms in such environments poses several technical challenges.

One challenge arises from the compatibility with legacy devices. Many IoT-enabled solar energy systems involve older hardware and protocols that may not support modern authentication mechanisms such as biometrics or token-based systems. This limitation often necessitates custom integration efforts, which can increase deployment complexity and cost. To mitigate these challenges, lightweight and scalable access control systems tailored to the IoT environment are essential. Combining role-based access control with dynamic access policies can adapt permissions in real time based on the device or user behavior. Additionally, MFA solutions optimized for usability, such as push notifications or time-based one-time passwords (TOTPs), can enhance security without overburdening users.

For legacy systems, middleware solutions that act as authentication bridges can help integrate advanced mechanisms with the older infrastructure. Furthermore, implementing continuous authentication systems that monitor user activity for anomalies after the initial login can provide an additional protection layer. By adopting these strategies, access control and authentication mechanisms can be deployed effectively, ensuring the integrity and security of IoT-enabled solar energy systems without compromising operational efficiency.

3. Security Monitoring and Incident Response

Security monitoring ensures the constant monitoring of a smart PV system by detecting potential threats in real time. These include monitoring networks, sensors, and other system components for vulnerabilities and abnormalities. Incident response complements monitoring by containing threats, analyzing root causes, eradication, and ensuring compliance with regulations [65].

An effective incident response minimizes the impact of security breaches by facilitating quick recovery and implementing measures to prevent recurrence [66]. However, the complexity of smart PV systems with multiple interconnected components makes balancing false positives and false negatives a challenge, requiring sophisticated solutions and significant investment in technology and training.

Security monitoring and incident response are critical components of a comprehensive cybersecurity strategy for IoT-enabled solar energy systems. These systems, with their interconnected devices and reliance on real-time data, require robust mechanisms to promptly detect, analyze, and respond to security threats. However, implementing these measures in practice involves both technical and operational challenges. A primary challenge in security monitoring is balancing the volume of data generated by IoT devices with the ability to identify meaningful anomalies. The absolute volume of data streams from sen-

sors, gateways, and cloud systems can overwhelm monitoring tools, particularly when traditional methods are used. Advanced techniques such as machine learning and anomaly detection algorithms are necessary to filter noise and pinpoint genuine threats, but these require substantial computational resources and expertise for effective implementation.

An incident response faces its own set of challenges, particularly in coordinating actions across a distributed system. The decentralized nature of IoT-enabled solar energy systems, which span local devices, cloud platforms, and remote user interfaces, makes isolating and containing threats complex. Delayed responses owing to inadequate communication between components can worsen the impact of security breaches.

To overcome these challenges, security monitoring should leverage scalable and intelligent systems that can adapt to the dynamic behavior of IoT environments. Centralized dashboards integrated with advanced analytics tools can help security professionals visualize threats in real time, enabling faster decision-making. For incident response, automated mechanisms, such as playbooks for common threat scenarios and pre-configured isolation protocols for compromised devices, can significantly reduce response times. Furthermore, integrating monitoring and response systems with logging and auditing capabilities ensures that incidents are managed effectively and analyzed post-event for continuous improvement. By addressing these challenges with adaptive and integrated solutions, IoT-enabled solar energy systems can achieve resilient and proactive cybersecurity.

4. Data Encryption and Data Privacy

IoT-enabled PV systems generate significant amounts of data on energy production, system performance, and user interaction. Data encryption ensures that sensitive information is protected during transmission, thereby preventing unauthorized access. Encryption is the key to meeting data protection regulations and maintaining user trust. Nevertheless, balancing security and usability, particularly with effective key management, remains challenging.

Data encryption and privacy are critical for securing the vast amount of sensitive information generated by IoT-enabled solar energy systems. These systems rely on continuous data exchange between sensors, gateways, and cloud platforms, thereby protecting data in transit, and at rest is paramount. However, implementing encryption and ensuring privacy in these environments introduce specific technical challenges [67]. One key challenge is the processing overhead introduced by encryption algorithms. IoT devices, particularly those deployed in the field such as sensors and edge nodes, often have limited computational power and memory. Implementing robust encryption protocols, such as AESs, for data security can strain these devices and potentially impact real-time operations. It is necessary to optimize encryption schemes to balance security and performance.

Thus, effective key management poses a significant challenge. In distributed IoT systems, managing encryption keys securely across multiple devices and communication endpoints is becoming increasingly complex. Compromised keys can lead to unauthorized access, undermining the overall security of the system. Robust key rotation policies and secure storage mechanisms, such as hardware security modules (HSMs), are essential for mitigating these risks. Data privacy concerns are further complicated by regulatory requirements, such as GDPR or region-specific privacy laws. These regulations demand strict compliance in handling user data, including ensuring encryption, anonymization, and protection from unauthorized access. Achieving compliance and still maintaining system usability and efficiency adds an additional layer of complexity.

Addressing these challenges requires the adoption of lightweight encryption algorithms optimized for IoT devices alongside selective encryption techniques that prioritize the protection of sensitive data and reduce resource consumption. Integrating automated key management solutions can enhance security while minimizing human error. Addition-

ally, privacy-enhancing technologies such as data masking and differential privacy can help align system operations with regulatory mandates without compromising functionality. Advancements in quantum communication networks offer promising solutions to many IoT security challenges [68–70]. These include secure-transmission encryption, digital signatures, and strong identity authentication. For example, quantum key distribution has demonstrated effectiveness in secure transmission encryption [71], whereas quantum-based digital signatures provide enhanced authentication mechanisms [72]. Integrating these cutting-edge technologies into IoT-enabled solar energy systems can address the vulnerabilities that traditional cryptographic methods struggle to mitigate, particularly in the face of emerging quantum computing threats. While the current study focuses on conventional security measures, specific research works could explore the feasibility of incorporating quantum cryptography to enhance smart PV system resilience.

5. Regular Software Updates and Patch Management

Regular software updates are critical for addressing the vulnerabilities in the software ecosystem of smart PV systems. These updates deliver security patches, new functionalities, and performance enhancement. Patch management involves systematic identification, evaluation, and application of these updates to maintain system security and functionality. Effective patch management includes the following steps:

- First, patch prioritization to ensure critical vulnerabilities are addressed;
- Testing and validation of updates in controlled environments to prevent compatibility issues;
- Change control procedures to ensure safe and documented deployment of patches;
- Backup and rollback plan to restore systems if updates cause instability;
- Regular monitoring and compliance ensure that software updates are promptly applied, especially for systems that require strict adherence to industry standards.

Regular software updates and patch management are vital to ensure the security and reliability of IoT-enabled solar energy systems. However, challenges, such as operational disruptions, compatibility with legacy devices, and vulnerabilities during the update process, must be addressed. Disruptions may occur because of the necessity for uninterrupted system functionality; however, scattered ecosystems might hinder the implementation of patches across various components.

Secure update protocols, automated deployment systems, and pre-deployment testing are essential for risk mitigation. Compatibility issues can be addressed through middleware solutions or collaboration with vendors. In addition, backup and rollback mechanisms ensure system stability in the case of failures. These measures enable IoT-enabled solar systems to remain secure and functional while minimizing the operational impact.

6. Network Segmentation

Network segmentation enhances the security of smart PV systems by dividing the network into smaller, isolated segments, thereby limiting the lateral movement of the attackers. This reduces the scope of security breaches even if one segment is compromised. Network segmentation minimizes the impact of security events by separating components with different security levels. Access control measures, such as firewalls and authentication policies, govern traffic between segments, adhering to the principle of least privilege. Continuous monitoring detects abnormal activities within a segmented network, thereby enabling timely responses to potential attacks.

Network segmentation enhances the security of IoT-enabled solar energy systems by isolating components into distinct zones, thereby limiting the spread of the attacks. However, challenges include designing and maintaining complex segmentation policies, ensuring secure yet seamless communication between zones, and scaling networks as

new devices are added. Striking the balance between security and functionality requires advanced monitoring, dynamic traffic management, and regular audits.

Implementing micro-segmentation and centralized policy management can address these challenges by providing granular control and simplifying enforcement. These strategies improve system resilience to cyber threats, while supporting efficient and secure operations.

7. Vendor Security Evaluation

Vendor security is critical in IoT-enabled PV systems owing to their reliance on third-party components and services. Sensors, controllers, inverters, and cloud platforms from various vendors introduce security risks. Comprehensive security evaluations of vendor policies, data security strategies, and compliance with industry standards are essential. Vendor assessments focus on the encryption, access control, incident response, and security of hardware components. Ongoing evaluations ensure that vendors' security measures adapt to evolving threats while fostering strong collaboration between system operators and suppliers to maintain system integrity.

A vendor security evaluation is important for safeguarding IoT-enabled solar energy systems, as these systems rely heavily on third-party components [73]. Challenges include limited transparency from vendors, delayed security updates, and supply chain risks such as counterfeit hardware. Addressing these challenges requires organizations to conduct comprehensive vendor evaluations focusing on encryption, access control, incident response, and compliance with standards such as ISO/IEC 27001 [74]. Contractual agreements should include security requirements and obligations to ensure that vendors adhere to best practices. Periodic audits and continuous collaboration with vendors can help address vulnerabilities proactively, thereby enhancing the overall security of IoT-enabled solar energy systems.

8. Security Awareness and Training

Beyond technical measures, security awareness and training are crucial for protecting smart PV systems from cyber threats. Comprehensive training helps employees recognize and respond to cybersecurity risks such as phishing and social engineering attacks, fostering a culture of cybersecurity vigilance. Incident response training prepares employees to handle security breaches effectively, thereby ensuring timely and coordinated responses. Continuous education keeps staff updated on emerging threats, reinforcing the system's resilience against evolving cyber risk.

The security implications of IoT device diversity in smart solar energy systems stem from variations in hardware resources, software capabilities, and communication protocols. Although some IoT devices, such as field gateways, support stronger encryption and authentication mechanisms, others, like low-power sensors, may have limited computational capacity for advanced security features. Additionally, differences in firmware update mechanisms, authentication protocols, and data transmission security affect the overall security posture of the system. These variations require a structured security strategy that accounts for device-specific constraints and maintaining uniform protection across the entire system. In practical deployments, security solutions must be adaptable to heterogeneous device environments to ensure effective threat mitigation without disrupting system operations. Table 8 presents recommended security controls, highlighting their advantages, challenges, and optimal use cases

Table 8. Recommended security controls with advantages, challenges, and best-use scenarios.

Security Strategy	Advantages	Challenges	Best-Use Case
Intrusion Detection and Prevention (IDS and IPS)	Detects and blocks malicious activity in real-time, securing critical IoT systems	It can generate false positive alerts, requiring human intervention or tuning	Deploying machine learning-based IDS and IPS to adapt to IoT-specific traffic patterns, reducing false positives and improving detection accuracy
Access Control and User Authentication	Ensures only authorized users and devices can access the system, reducing risks of unauthorized access	Complex configuration and scalability issues for large IoT deployments	Using centralized access management systems with role-based access control (RBAC) and multi-factor authentication (MFA) for secure and scalable user/device authentication
Security Monitoring and Incident Response	Quickly detects and responds to potential attacks, reducing damage and downtime	Comprehensive tools can be resource-intensive to IoT systems and costly to implement and maintain	Integrating lightweight monitoring tools and automated incident response workflows to reduce costs and enhance response times
Data Encryption and Data Privacy	Ensures data confidentiality and integrity, protecting sensitive information	Encryption can demand significant processing power, which may strain low-resource IoT devices	Employing lightweight encryption for secure data transmission in low-resource IoT devices
Regular Software Updates and Patch Management	Keeps devices protected by addressing vulnerabilities as soon as they are discovered	Dependence on vendors for timely updates and patch availability	Automating patch deployment processes and establishing SLAs with vendors to ensure critical updates are delivered promptly
Network Segmentation	Limits the spread of attacks and isolates threats, protecting critical components	Requires careful design, proper configuration, and ongoing monitoring	Implementing software-defined networking (SDN) to dynamically and precisely isolate IoT sensors, control units, and external user networks
Vendor Security Evaluation	Reduces risks from insecure devices or software by ensuring suppliers meet security standards	Transparency and cooperation from vendors can vary, making evaluations inconsistent	Prioritizing vendors with recognized certifications (e.g., ISO 27001) and requiring security audits during the procurement process
Security Awareness and Training	Equips administrators and users with the knowledge to avoid common mistakes like phishing or weak configurations	Training effectiveness can decrease over time without regular updates or engaging content	Using interactive, scenario-based training to simulate IoT-specific threats, reinforcing secure practices for all stakeholders

The STRIDE model provides a structured and effective approach for identifying security threats, but it is important to acknowledge some of its limitations. For large

and complex systems, STRIDE can become time consuming because the detailed analysis required for each component may overwhelm teams managing extensive architectures. Another notable limitation is its focus on known threats, meaning that it may not effectively capture novel or sophisticated attacks that do not align with its predefined categories [75]. The effective application of STRIDE also depends on a solid understanding of both the system being analyzed and the threat modeling process itself, which can pose challenges for teams lacking sufficient security expertise. Additionally, STRIDE heavily emphasizes technical threats and may overlook broader business impacts or contexts that are crucial for comprehensive risk assessments. Despite the fact that STRIDE provides a structured approach to threat modeling, it does not account for the stochastic nature of cyberattacks. Scenario-based simulations can be explored to model the unpredictability of cyber threats in IoT-enabled smart solar energy systems. Stochastic approaches have been used in energy systems to handle uncertainty, such as in optimal allocation planning for intelligent buildings with energy storage sharing [76], and similar methodologies could be explored for cybersecurity risk modeling.

Despite these limitations, STRIDE remains a valuable tool, particularly in the design phase of IoT-enabled systems. Enhancing it with complementary methodologies, such as attack-tree analysis for visualizing attack paths or risk-prioritization frameworks for ranking threats, can help address these gaps. Together, these approaches provide a more adaptive and holistic strategy to manage threats in complex systems.

5. Conclusions

Integrating IoT technologies into solar energy systems has significantly enhanced their capabilities for real-time monitoring, control, and optimization. However, this increased connectivity also expands the system's attack surface, exposing the critical components to cybersecurity risks. This study conducted a thorough threat modeling analysis of IoT-based smart solar energy systems, utilizing the STRIDE threat model to systematically identify, categorize, and assess potential security threats. The methodology began with the creation of a detailed system use case, outlining key components, such as IoT sensors, PV modules, IoT nodes, communication gateways, cloud infrastructure, and remote access interfaces. A Data Flow Diagram was developed to map the interactions between these components, emphasizing the security zones where vulnerabilities are most likely to occur. The STRIDE threat model was then applied to classify and evaluate security threats, including spoofing, tampering, repudiation, information disclosure, DoS, and privilege elevation. The DREAD risk assessment model was then used to prioritize threats based on Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. The results indicate that most threats fall into the high-risk category, with scores ranging from 2.6 to 2.8, emphasizing the need for targeted mitigation. Each threat was examined in terms of its potential impact on the integrity, availability, and confidentiality of the system.

To mitigate these risks, the research discussed several technical security measures that have been proposed, including IDS, IPS, stronger authentication, end-to-end encryption for data transmission, security monitoring, incident response, comprehensive logging for auditing, and regular updates to address known vulnerabilities. These measures are key for improving the resilience and security of IoT-enabled solar energy systems. By adopting the proposed solutions, system operators can protect against advanced cyber threats and ensure the reliability and stability of solar energy infrastructure. The architectural approach adopted in this study highlights the need for secure design practices that account for vulnerabilities across data flows and system components. This study applies STRIDE-based threat modeling to IoT-enabled smart solar energy systems; however, its findings can be extended to other IoT domains that rely on real-time data exchange, cloud integration,

and remote monitoring. The proposed methodology provides a scalable approach to identifying cybersecurity threats in interconnected IoT infrastructures such as industrial IoT, smart cities, and energy monitoring networks. As demonstrated in our previous implementation of an IoT-based solar energy monitoring system, real-world applications of such architectures face security challenges such as ensuring encrypted data transmission or tampering threats. By employing the STRIDE threat model, this study provides a structured approach for identifying and mitigating threats that can be directly applied to such systems. Building on the findings of this study, future research should focus on the development of a security monitoring system capable of detecting and responding to threats in IoT-based solar energy systems. Such a system could combine Operational Technology (OT) and Information Technology (IT) security components, providing a unified approach for monitoring and securing both infrastructure layers. Moreover, integrating machine-learning techniques for real-time threat detection and adaptive responses could enhance the ability to dynamically address emerging threats. Additionally, future work could explore the integration of emerging technologies such as blockchain, software-defined networking, and edge computing to enhance system resilience. Investigating their applicability for mitigating specific cybersecurity threats in distributed solar energy networks could provide valuable insights for improving security frameworks in real-world deployments. Moreover, by expanding on this work by applying the proposed threat model with a real-world use case and testing its applicability in other IoT domains, such efforts would refine the findings and reinforce their relevance across diverse IoT-enabled applications. This work contributes to the broader field of cybersecurity in renewable energy systems, offering a structured and technical approach to securing IoT-based solar infrastructure against advanced and evolving cyber threats.

Author Contributions: Conceptualization, A.R. and D.T.C.; methodology, A.R. and T.C.B.; software, A.R. and R.A.; validation, T.C.B., D.T.C., and A.R.; formal analysis, A.R.; investigation, A.R. and E.T.; resources, P.A.C.; data curation, A.R.; writing—original draft preparation, A.R.; writing—review and editing, A.R., T.C.B., and D.T.C.; visualization, E.T. and R.A.; supervision, D.T.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in this article, further inquiries can be directed to the corresponding author/s.

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

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced Encryption Standard
CIAA	Confidentiality, Integrity, Availability, and Authentication
CPS	Cyber–Physical System
DFD	Data Flow Diagram
DERs	Distributed Energy Resources
DoS	Denial of Service
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability

HSM	Hardware Security Module
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
MFA	Multi-Factor Authentication
MITRE ATT & CK	Adversarial Tactics, Techniques, and Common Knowledge
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OT	Operational Technology
PASTA	Process for Attack Simulation and Threat Analysis
PC	Personal Computer
PV	Photovoltaic
RBAC	Role-Based Access Control
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TSIs	Time Series Insights
TOTP	Time-Based One-Time Password
TLS	Transport Layer Security

References

1. Hassan, Q.; Algburi, S.; Sameen, A.Z.; Al-Musawi, T.J.; Al-Jiboory, A.K.; Salman, H.M.; Ali, B.M.; Jaszczur, M. A comprehensive review of international renewable energy growth. *Energy Built Environ.* **2024**, *in press*. [CrossRef]
2. Mohammadi, E.; Moschopoulos, G.; Chen, A. Boosting Solar Sustainability: Performance Assessment of Roof-Mounted PV Arrays Under Snow Considering Various Module Interconnection Schemes. *Sustainability* **2025**, *17*, 329. [CrossRef]
3. Cotfas, P.A.; Cotfas, D.T. Comprehensive Review of Methods and Instruments for Photovoltaic–Thermoelectric Generator Hybrid System Characterization. *Energies* **2020**, *13*, 6045. [CrossRef]
4. Hassan, Q.; Viktor, P.; Al-Musawi, T.J.; Mahmood Ali, B.; Algburi, S.; Alzoubi, H.M.; Khudhair Al-Jiboory, A.; Zuhair Sameen, A.; Salman, H.M.; Jaszczur, M. The renewable energy role in the global energy Transformations. *Renew. Energy Focus* **2024**, *48*, 100545. [CrossRef]
5. Ang, T.-Z.; Salem, M.; Kamarol, M.; Das, H.S.; Nazari, M.A.; Prabaharan, N. A comprehensive study of renewable energy sources: Classifications, challenges and suggestions. *Energy Strategy Rev.* **2022**, *43*, 100939. [CrossRef]
6. Sayigh, A. Solar and Wind Energy Will Supply More than 50% of World Electricity by 2030. In *Transition Towards a Carbon Free Future: Selected Papers from the World Renewable Energy Congress (WREC) 2023*; Sayigh, A., Ed.; Springer Nature Switzerland: Cham, Switzerland, 2024; pp. 349–364. ISBN 978-3-031-61660-0.
7. Li, G.; Li, M.; Taylor, R.; Hao, Y.; Besagni, G.; Markides, C.N. Solar energy utilisation: Current status and roll-out potential. *Appl. Therm. Eng.* **2022**, *209*, 118285. [CrossRef]
8. Bhau, G.V.; Deshmukh, R.G.; Kumar, T.R.; Chowdhury, S.; Sesharao, Y.; Abilmazhinov, Y. IoT based solar energy monitoring system. *Mater. Today Proc.* **2023**, *80*, 3697–3701. [CrossRef]
9. Dobrilovic, D.; Pekez, J.; Desnica, E.; Radovanovic, L.; Palinkas, I.; Mazalica, M.; Djordjević, L.; Mihajlovic, S. Data Acquisition for Estimating Energy-Efficient Solar-Powered Sensor Node Performance for Usage in Industrial IoT. *Sustainability* **2023**, *15*, 7440. [CrossRef]
10. Ahmetoglu, S.; Che Cob, Z.; Ali, N. A Systematic Review of Internet of Things Adoption in Organizations: Taxonomy, Benefits, Challenges and Critical Factors. *Appl. Sci.* **2022**, *12*, 4117. [CrossRef]
11. Samosir, A.S.; Rozie, A.F.; Purwiyanti, S.; Gusmedi, H.; Susanto, M. Development of an IoT Based Monitoring System for Solar PV Power Plant Application. In Proceedings of the 2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE), Bandar Lampung, Indonesia, 27–28 October 2021; pp. 82–86. [CrossRef]
12. Spanias, A.S. Solar energy management as an Internet of Things (IoT) application. In Proceedings of the 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), Larnaca, Cyprus, 27–30 August 2017; pp. 1–4. [CrossRef]
13. Majee, A.; Bhatia, M.; Swathika, O.V.G. IoT Based Microgrid Automation for Optimizing Energy Usage and Controllability. In Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018; pp. 685–689. [CrossRef]

14. Ahmed Abdulkadir, A.; Al-Turjman, F. Smart-grid and solar energy harvesting in the IoT era: An overview. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e4896. [CrossRef]
15. Rekeraho, A.; Cotfas, D.T.; Cotfas, P.A.; Bălan, T.C.; Tuyishime, E.; Acheampong, R. Cybersecurity challenges in IoT-based smart renewable energy. *Int. J. Inf. Secur.* **2023**, *23*, 101–117. [CrossRef]
16. Rekeraho, A.; Cotfas, D.T.; Cotfas, P.A.; Tuyishime, E.; Balan, T.C.; Acheampong, R. Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems. *Electronics* **2024**, *13*, 756. [CrossRef]
17. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.-S.; et al. A Review of Cyber–Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 4879–4901. [CrossRef]
18. Tatipatri, N.; Arun, S.L. A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. *IEEE Access* **2024**, *12*, 18147–18167. [CrossRef]
19. Abdelkader, S.; Amissah, J.; Kinga, S.; Mugerwa, G.; Emmanuel, E.; Mansour, D.-E.A.; Bajaj, M.; Blazek, V.; Prokop, L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results Eng.* **2024**, *23*, 102647. [CrossRef]
20. Van Landuyt, D.; Joosen, W. A descriptive study of assumptions in STRIDE security threat modeling. *Softw. Syst. Model* **2022**, *21*, 2311–2328. [CrossRef]
21. Saßnick, O.; Rosenstatter, T.; Schäfer, C.; Huber, S. STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review. In Proceedings of the 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS), St. Louis, MO, USA, 12–15 May 2024; pp. 1–8. [CrossRef]
22. STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. Available online: https://www.mdpi.com/2624-8921/6/3/54 (accessed on 19 November 2024).
23. Omotosho, A.; Ayemlo Haruna, B.; Mikail Olaniyi, O. Threat Modeling of Internet of Things Health Devices. *J. Appl. Secur. Res.* **2019**, *14*, 106–121. [CrossRef]
24. A Novel Approach for Fully Intuitionistic Fuzzy Multi-Objective Fractional Transportation Problem—ScienceDirect. Available online: https://www.sciencedirect.com/science/article/pii/S1110016820305810 (accessed on 20 February 2025).
25. El Sayed, M.A.; Baky, I.A. Multi-choice fractional stochastic multi-objective transportation problem. *Soft Comput.* **2023**, *27*, 11551–11567. [CrossRef]
26. Zhai, X.; Li, Z.; Li, Z.; Xue, Y.; Chang, X.; Su, J.; Jin, X.; Wang, P.; Sun, H. Risk-averse energy management for integrated electricity and heat systems considering building heating vertical imbalance: An asynchronous decentralized approach. *Appl. Energy* **2025**, *383*, 125271. [CrossRef]
27. El-Sofany, H.; El-Seoud, S.A.; Karam, O.H.; Bouallegue, B. Using machine learning algorithms to enhance IoT system security. *Sci. Rep.* **2024**, *14*, 12077. [CrossRef]
28. Khan, M.M.; Alkhathami, M. Anomaly detection in IoT-based healthcare: Machine learning for enhanced security. *Sci. Rep.* **2024**, *14*, 5872. [CrossRef] [PubMed]
29. Ju, Y.; Cao, Z.; Chen, Y.; Liu, L.; Pei, Q.; Mumtaz, S.; Dong, M.; Guizani, M. NOMA-Assisted Secure Offloading for Vehicular Edge Computing Networks With Asynchronous Deep Reinforcement Learning. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 2627–2640. [CrossRef]
30. Kareem, Y.; Djenouri, D.; Ghadafi, E. A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things. *Future Internet* **2024**, *16*, 285. [CrossRef]
31. Jain, A.K.; Shukla, H.; Goel, D. A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks. *Clust. Comput.* **2024**, *27*, 13129–13164. [CrossRef]
32. Rupanetti, D.; Kaabouch, N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Appl. Sci.* **2024**, *14*, 7104. [CrossRef]
33. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Barnawi, A.; Alzahrani, B.A. Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. *J. Netw. Comput. Appl.* **2020**, *157*, 102537. [CrossRef]
34. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
35. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 26–29 September 2017; pp. 1–6. [CrossRef]
36. Karim, Y.; Hasan, R. Towards a Threat Model for Fog Computing. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 1110–1116. [CrossRef]

37. Anwar, M.N.; Nazir, M.; Ansari, A.M. Modeling Security Threats for Smart Cities: A STRIDE-Based Approach. In Proceedings of the Smart Cities—Opportunities and Challenges; Ahmed, S., Abbas, S.M., Zia, H., Eds.; Springer: Singapore, 2020; pp. 387–396. [CrossRef]
38. Simonjan, J.; Taurer, S.; Dieber, B. A Generalized Threat Model for Visual Sensor Networks. *Sensors* **2020**, *20*, 3629. [CrossRef]
39. Al-Sada, B.; Sadighian, A.; Oligeri, G. MITRE ATT&CK: State of the Art and Way Forward. *ACM Comput. Surv.* **2024**, *57*, 12:1–12:37. [CrossRef]
40. Wolf, A.; Simopoulos, D.; D'Avino, L.; Schwaiger, P. The PASTA Threat Model Implementation in the IoT Development Life Cycle. Available online: https://dl.gi.de/items/7c61da62-26fc-4c51-9bd1-dade421e7921 (accessed on 16 November 2024).
41. Chen, X.; Wen, N. Information Security Risk Assessment Model Based on OCTAVE for E-Government. In Proceedings of the 2010 International Conference on Internet Technology and Applications, Wuhan, China, 21–23 August 2010; pp. 1–5. [CrossRef]
42. Abdullah, M.I.; Abas, A.I.; Hajamydeen, A.I. Effective SOC Response Strategies Using MITRE ATT & CK. *J. Emerg. Technol. Ind. Appl.* **2024**, *3*, 1–7. Available online: http://jetia.mbot.org.my/index.php/jetia/article/view/34 (accessed on 16 November 2024).
43. Naik, N.; Jenkins, P.; Grace, P.; Naik, D.; Prajapat, S.; Song, J. A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Available online: https://www.authorea.com/doi/full/10.36227/techrxiv.173014171.11449253?commit=09dec9318db01f4d93ebe23399f59c971e1681c9 (accessed on 16 November 2024).
44. Biswas, B.; Sharmin, S.; Hossain, M.A.; Alam, M.Z.; Sarkar, M.I. Risk Analysis-based Decision Support System for Designing Cybersecurity of Information Technology. *J. Bus. Manag. Stud.* **2024**, *6*, 13–22. [CrossRef]
45. Saurabh, K.; Gajjala, D.; Kaipa, K.; Vyas, R.; Vyas, O.P.; Khondoker, R. TMAP: A Threat Modeling and Attack Path Analysis Framework for Industrial IoT Systems (A Case Study of IoM and IoP). *Arab. J. Sci. Eng.* **2024**, *49*, 13163–13183. [CrossRef]
46. Asif, M.R.A.; Hasan, K.F.; Islam, M.Z.; Khondoker, R. STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems. In Proceedings of the 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 18–19 December 2021; pp. 1–6. [CrossRef]
47. Rizvi, S.; Pipetti, R.; McIntyre, N.; Todd, J.; Williams, I. Threat model for securing internet of things (IoT) network at device-level. *Internet Things* **2020**, *11*, 100240. [CrossRef]
48. Ben-Nakhi, A.A.; El-Barr, M.A.; Qureshi, K. Threat Modeling of IoT-based Smart Home Systems. *Int. J. Comput. Their Appl.* **2023**, *30*, 377–385. Available online: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=10765204&AN=174858370&h=b5qMVBDvvk5dGcI8kD+dl017lgjlFe5mh7X3FQsitAw81sV5wIRcfjftCv3ayCtF9wqekIjAIIoUlNdCaC2+EQ==&crl=c (accessed on 19 December 2024).
49. Sion, L.; Yskout, K.; Van Landuyt, D.; Joosen, W. Solution-aware data flow diagrams for security threat modeling. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, 9–13 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1425–1432. [CrossRef]
50. Kgremban. Tutorial—IoT Data Visualization with Power BI—Azure IoT Hub. Available online: https://learn.microsoft.com/en-us/azure/iot-hub/iot-hub-live-data-visualization-in-power-bi (accessed on 7 December 2024).
51. Tedvilutis. How to Add an IoT Hub Event Source—Azure Time Series Insights. Available online: https://learn.microsoft.com/en-us/azure/time-series-insights/how-to-ingest-data-iot-hub (accessed on 7 December 2024).
52. Zhang, L.; Taal, A.; Cushing, R.; de Laat, C.; Grosso, P. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *Int. J. Inf. Secur.* **2022**, *21*, 509–525. [CrossRef]
53. Rekeraho, A.; Balan, T.; Cotfas, D.T.; Cotfas, P.A.; Acheampong, R.; Musuroi, C. Sandbox Integrated Gateway for the Discovery of Cybersecurity Vulnerabilities. In Proceedings of the 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 10–11 November 2022; pp. 1–4. [CrossRef]
54. Santos, L.; Rabadao, C.; Gonçalves, R. Intrusion detection systems in Internet of Things: A literature review. In Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; pp. 1–7. [CrossRef]
55. Kumar, A.; Abhishek, K.; Ghalib, M.R.; Shankar, A.; Cheng, X. Intrusion detection and prevention system for an IoT environment. *Digit. Commun. Netw.* **2022**, *8*, 540–551. [CrossRef]
56. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors* **2024**, *24*, 713. [CrossRef]
57. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A Signature-based Intrusion Detection System for the Internet of Things. In *Proceedings of the Information and Communication Technology Form*; AUT: York, UK, 2018; Available online: https://eprints.whiterose.ac.uk/133312/ (accessed on 20 June 2024).
58. Tiwari, A.; Saraswat, S.; Dixit, U.; Pandey, S. Refinements In Zeek Intrusion Detection System. In Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 25–26 March 2022; Volume 1, pp. 974–979. [CrossRef]

59. Gupta, A.; Sharma, L.S. Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server. In Proceedings of the ICRIC 2019; Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 811–821. [CrossRef]
60. Jain, G.; Anubha. Application of SNORT and Wireshark in Network Traffic Analysis. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1119*, 012007. [CrossRef]
61. Mahboub, S.A.; Ahmed, E.S.A.; Saeed, R.A. Smart IDS and IPS for Cyber-Physical Systems. In *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*; IGI Global: Hershey, PA, USA, 2021; pp. 109–136. ISBN 978-1-79985-101-1. [CrossRef]
62. Chavez, A.; Lai, C.; Jacobs, N.; Hossain-McKenzie, S.; Jones, C.B.; Johnson, J.; Summers, A. Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; pp. 1–6. [CrossRef]
63. Deng, M.; Lyu, Y.; Yang, C.; Xu, F.; Ahmed, M.; Yang, N.; Xu, Z.; Ke, C. Lightweight Trust Management Scheme Based on Blockchain in Resource-Constrained Intelligent IoT Systems. *IEEE Internet Things J.* **2024**, *11*, 25706–25719. [CrossRef]
64. Suleski, T.; Ahmed, M.; Yang, W.; Wang, E. A Review of Multi-Factor Authentication in the Internet of Healthcare Things. 2023. Available online: https://journals.sagepub.com/doi/full/10.1177/20552076231177144 (accessed on 3 October 2024).
65. Lekidis, A.; Mavroeidis, V.; Fysarakis, K. Towards Incident Response Orchestration and Automation for the Advanced Metering Infrastructure. In Proceedings of the 2024 IEEE 20th International Conference on Factory Communication Systems (WFCS), Toulouse, France, 17–19 April 2024; pp. 1–8. [CrossRef]
66. Naseer, H.; Desouza, K.; Maynard, S.B.; Ahmad, A. Enabling cybersecurity incident response agility through dynamic capabilities: The role of real-time analytics. *Eur. J. Inf. Syst.* **2024**, *33*, 200–220. [CrossRef]
67. Singh, S.; Sharma, P.K.; Moon, S.Y.; Park, J.H. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *J Ambient Intell Hum. Comput* **2024**, *15*, 1625–1642. [CrossRef]
68. Chawla, D.; Mehra, P.S. A Survey on Quantum Computing for Internet of Things Security. *Procedia Comput. Sci.* **2023**, *218*, 2191–2200. [CrossRef]
69. Al-Mohammed, H.A.; Yaacoub, E. On The Use of Quantum Communications for Securing IoT Devices in the 6G Era. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. [CrossRef]
70. Babu, P.R.; Kumar, S.A.P.; Reddy, A.G.; Das, A.K. Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. *Comput. Sci. Rev.* **2024**, *54*, 100676. [CrossRef]
71. Zhou, L.; Lin, J.; Xie, Y.-M.; Lu, Y.-S.; Jing, Y.; Yin, H.-L.; Yuan, Z. Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking. *Phys. Rev. Lett.* **2023**, *130*, 250801. [CrossRef]
72. Experimental Quantum Byzantine Agreement on a Three-User Quantum Network with Integrated Photonics | Science Advances. Available online: https://www.science.org/doi/full/10.1126/sciadv.adp2877 (accessed on 13 December 2024).
73. Wijesundara, W.M.A.B.; Lee, J.-S.; Tith, D.; Aloupogianni, E.; Suzuki, H.; Obi, T. Security-enhanced firmware management scheme for smart home IoT devices using distributed ledger technologies. *Int. J. Inf. Secur.* **2024**, *23*, 1927–1937. [CrossRef]
74. Malatji, M. Management of enterprise cyber security: A review of ISO/IEC 27001:2022. In Proceedings of the 2023 International Conference on Cyber Management and Engineering (CyMaEn), Bangkok, Thailand, 26–27 January 2023; pp. 117–122. [CrossRef]
75. Kim, K.H.; Kim, K.; Kim, H.K. STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI J.* **2022**, *44*, 991–1003. [CrossRef]
76. Zhang, H.; Li, Z.; Xue, Y.; Chang, X.; Su, J.; Wang, P.; Guo, Q.; Sun, H. A Stochastic Bi-Level Optimal Allocation Approach of Intelligent Buildings Considering Energy Storage Sharing Services. *IEEE Trans. Consum. Electron.* **2024**, *70*, 5142–5153. [CrossRef]