electronics

Article

Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems

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

Faculty of Electrical Engineering and Computer Science, Transilvania University of Brasov, 500036 Brasov, Romania
* Correspondence: alexandre.rekeraho@unitbv.ro

Abstract: Renewable energy is an essential solution for addressing climate change, providing sustainable options that are vital for a more environmentally friendly future. Integrating information technology (IT) into renewable energy systems has driven remarkable progress, enhanced efficiency, and enabled remote monitoring. Nevertheless, integrating IT into these systems dramatically increases their vulnerability to cyber threats and potential attacks. This study thoroughly investigates the enhancement of security measures in an IoT-based solar energy remote monitoring system. The research integrates advanced technologies, including Advanced Encryption Standard (AES), myRIO board, and NI's SystemLink Cloud platform, to enhance data security in smart solar energy monitoring systems. Emphasizing AES encryption ensures secure information exchange between the myRIO board and the computer. NI's SystemLink Cloud offers a user-friendly interface for real-time monitoring of critical solar system parameters, supported by robust security measures such as HTTPS encryption and access control. This study sets higher data protection standards in smart energy systems by promoting advanced encryption and secure cloud infrastructures. The approach involves seamlessly integrating renewable energy sources with IT innovations while prioritizing proactive measures to strengthen solar energy system security.

Keywords: cybersecurity; solar energy; renewable energy; Internet of Things; myRIO; cloud security; Advanced Encryption Standard; LabVIEW; SystemLink Cloud

Citation: 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. https://doi.org/10.3390/electronics13040756

Academic Editors: Alessandra De Benedictis and Salvatore Barone

Received: 15 January 2024
Revised: 5 February 2024
Accepted: 9 February 2024
Published: 13 February 2024

1. Introduction

Renewable energy sources are necessary due to rising global demand and the adverse environmental effects of burning fossil fuels. Renewable energy is produced from naturally replenishable sources such as solar radiation, wind, water flow, geothermal heat, and biomass. Recognition that renewable energy systems provide cleaner, more sustainable alternatives to conventional energy sources while simultaneously addressing climate change mitigation, energy security, and socioeconomic development is driving the move to these systems [1]. Among the many types of renewable energy, solar energy stands out as the undisputed leader in rapid growth and extensive advancement. Solar power is widely recognized in the scientific community as the foremost contributor among renewable energy sources [2–4]. This recognition is based on many key factors, including the plentiful availability of solar resources, the environmental sustainability of solar power, and the significant technological advances achieved in this field [5]. According to projections, solar array installations may provide around 45% of the global energy demand by the middle of the 21st century [6].

The incorporation of Internet of Things (IoT) technology into solar photovoltaic (PV) systems signifies a noteworthy advancement in the field of sustainable energy [7]. The IoT is a conceptual framework that comprises a network of networked devices equipped with sensors, software, and communication capabilities [8]. This framework enables the smooth

exchange of data and remote-control functionalities. The use of this technology in solar PV systems enhances these installations, making them smart by facilitating adaptation, connection, and improved operating efficiency. The importance of IoT in solar energy systems is summarized in [9–12] as follows:

- Comprehensive Monitoring and Control: The use of IoT technology brings about a significant transformation in the operation of solar PV systems, enabling continuous and detailed monitoring of these systems in real time [9]. The system incorporates strategically positioned sensors to monitor and measure several performance indicators, such as voltage, current, and temperature, at numerous locations. The meticulous data collection at a granular level enables exact analysis, hence facilitating optimization of energy output and system performance;
- Remote Management Capabilities [10]: IoT technology enables remote access and control, crucial components in contemporary PV systems. Remote diagnostics have made it possible to detect and promptly address inefficiencies or anomalies inside a system. Moreover, remote configuration enables users to modify system parameters, such as the orientation of panels, in a responsive manner to external factors, maximizing energy capture efficiency;
- Predictive Maintenance Strategies: IoT sensors consistently collect data, facilitating the development of predictive maintenance models [10]. The proactive method entails identifying prospective flaws or abnormalities in the system's operation. Through the use of historical data and the application of predictive analytics, maintenance personnel can anticipate and effectively manage maintenance needs. This proactive approach serves to minimize system downtime and guarantee ongoing energy production;
- Optimization of Energy Management: Integrating IoT technology is crucial in optimizing energy management processes [11]. By allowing smooth interaction with smart grids, IoT integration enhances the effectiveness of energy management systems. The integration of this system enables the effective allocation of loads, optimizing the distribution and consumption of energy resources. Furthermore, the IoT technology facilitates the efficient exploitation of energy storage systems, enabling the collection and optimum utilization of excess energy;
- User Interface and Data Visualization [12]: The user interfaces of IoT-enabled PV systems provide a user-friendly experience, allowing users to access detailed information on energy production and consumption trends. Using user-friendly dashboards and mobile apps allows individuals to obtain a comprehensive understanding of system performance, enabling them to make well-informed decisions about energy consumption and optimization methods.

In addition to energy management, IoT-enabled PV systems possess the capacity to interact effortlessly with smart home or building systems. The integration described promotes a comprehensive approach to optimize energy use, enabling automated energy usage and supporting improved overall efficiency. Integrating IoT technology into solar PV systems surpasses traditional capabilities, converting these configurations into intelligent, adaptive, and exceptionally efficient components in sustainable energy solutions.

Nevertheless, despite the diverse functionalities introduced by the integration of IoT technology into smart PV systems, this concurrently exposes these systems to a spectrum of vulnerabilities and potential security risks [13]. The presence of these aspects in IoT-enabled PV systems requires an in-depth investigation of the inherent threats associated with their expanded functionality. The expanded attack surface is a noteworthy risk arising from the networked nature of IoT devices inside smart PV systems. The connectivity facilitated by various communication protocols and associated devices unintentionally introduces possible weaknesses in the system's infrastructure, which malevolent actors may exploit. Furthermore, the intrinsic characteristics of IoT devices, which include collecting, transmitting, and storing data inside these systems, give rise to concerns about potential cybersecurity breaches. The presence of vulnerabilities in encryption methods or insufficient security measures might lead to unauthorized individuals gaining access to

sensitive data, such as crucial energy production metrics or user information. Consequently, this exposes the system to potential exploitation.

Furthermore, the injection of false data into the monitoring systems of intelligent solar energy infrastructures presents a substantial threat to their integrity and reliability [14]. These systems depend on precise data from IoT devices to provide informed decision-making and operational control. Nevertheless, vulnerabilities in these devices or the communication channels they use create opportunities for adversaries to introduce modified or fabricated data into the system. Infiltration undermines the integrity of energy production measurements and other vital data, resulting in flawed decision-making procedures. Ensuring confidentiality inside IoT-enabled smart solar energy systems is equally important. The violation of confidentiality not only infringes upon users' privacy but also presents avenues for adversaries to exploit weaknesses inside the system, possibly leading to interruptions or manipulation of critical energy production metrics. Ensuring the preservation of the secrecy of this data is essential in maintaining credibility and safeguarding the integrity of intelligent solar energy systems.

Moreover, it is essential to maintain user privacy while employing IoT-based solar energy [15,16]. The collection of solar data, while providing useful insights into energy usage and system efficiency, raises a range of privacy problems that need thoughtful examination. Solar panels, in their effort to capture intricate energy patterns, unintentionally gather sensitive data on daily routines, energy use, and even the presence of individuals inside residences. The unlawful disclosure of these data presents a substantial risk, which could compromise the privacy and security of people and their homes. Ensuring protection against unwanted access to this vast amount of information becomes essential. In addition, the solar panels' geographical data pose a possible threat to location monitoring. Examining this data might enable the monitoring of an individual's whereabouts, raising worries about privacy infringement. Safeguarding the geographical data linked to solar energy installations is crucial in deterring unauthorized intrusions into people' personal privacy. In addition, a significant number of solar energy systems use cloud-based platforms and third-party service providers for the storage and processing of data. Although this strategy improves its usefulness, it also presents a vulnerability, namely, the potential for unauthorized access to personal information held on these sites.

This research thoroughly investigates the enhancement of security measures in an IoT-based solar energy remote monitoring system. The Advanced Encryption Standard (AES) [17], LabVIEW [18], myRIO board [19], SystemLink Cloud technology [20], Wi-Fi communication, and additional multidimensional approaches are integrated into the proposed approach to ensure the security of smart solar energy system monitoring. One of the most popular and extensively used symmetric block encryption algorithms worldwide is the Advanced Encryption Standard (AES) algorithm [21]. This method has a unique structure when it comes to encrypting and decrypting sensitive data. Using the AES technique to encrypt data makes it difficult for threat actors to decipher. To date, there has been no proof that anyone can break this algorithm. AES supports three distinct key sizes—128 bits, 192 bits, and 256 bits—with a block size of 128 for each of these ciphers. This integration of technologies aims to mitigate the vulnerabilities found in IoT-enabled solar systems by providing strong security measures and improved monitoring capabilities. A robust local monitoring system is built by using myRIO board and LabVIEW. The smart solar energy infrastructure utilizes the Advanced Encryption Standard (AES), a widely acknowledged encryption standard, to enhance the security and privacy of the data transmitted in the system. AES encryption is a cryptographic technique that protects sensitive data, such as energy production measurements and system settings, by preventing unauthorized access or security breaches. Moreover, using LabVIEW software enhances the ability to gather data with precision, allowing real-time monitoring and analysis of solar energy indicators. Implementing this localized monitoring system improves the accuracy and reliability of data while reducing the potential for introducing erroneous data. As a result, this system plays a significant role in facilitating well-informed decision-making procedures.

Furthermore, integrating SystemLink Cloud technology expands the monitoring capabilities beyond local networks, facilitating remote access and monitoring of the smart solar energy system. Using the SystemLink Cloud, authorized stakeholders can access real-time data and monitor system performance from any place and at any moment. The use of a cloud-based method improves the accessibility of the system while simultaneously maintaining strong security measures. The proposed complete method not only tackles the issues of data confidentiality and false data injection, but also promotes the development of a flexible and secure monitoring framework for intelligent solar energy systems.

The following are the main contributions of the article:

- Thoroughly examining the implementation and assessment of AES-256 encryption in the smart solar energy monitoring system. Highlighting the crucial significance of encryption emphasizes the utmost need to secure data and guarantee the confidentiality and integrity of sensitive information within renewable energy systems;
- The integration of NI's SystemLink Cloud platform, a significant advancement in improving remote access functionality. This integration greatly enhances the accessibility and usage of critical solar system parameters by providing secure access from multiple locations. As a result, this improves the efficiency and operational capabilities of the system;
- In addition, the research advocates using strong security measures, namely, HTTPS encryption, role-based access restrictions, and encryption protocols in renewable energy systems. This mechanism not only strengthens individual components but also enhances the overall security posture of smart energy systems, ensuring resistance against cyber-attacks;
- Finally, the research illuminates the benefits of integrating IT into renewable energy systems and discusses proactive measures to mitigate vulnerabilities from implementing information technology in renewable energy systems. It emphasizes the need to avoid security gaps, defend against new cyber threats, and guarantee the system's reliability by carrying out and supporting proactive methods.

2. Related Work

In recent years, the literature has strongly stressed the crucial significance of data encryption as a fundamental element in ensuring the security of data transmission inside energy monitoring systems [22–26]. Research has emphasized the vulnerability of unencrypted data as they are being sent, highlighting their susceptibility to being intercepted and tampered with by unauthorized individuals. Researchers [27–29] have extensively studied several encryption approaches, strongly pushing for the use of solid encryption protocols such as Advanced Encryption Standards. Comparative evaluations have examined the effectiveness and appropriateness of encryption algorithms in terms of characteristics such as computing efficiency, scalability, and resistance to possible cyber-attacks [30]. Furthermore, studies have investigated incorporating encryption techniques into current data-gathering systems, illustrating how encryption may enhance data integrity while maintaining system performance. These studies highlight the importance of encryption in safeguarding the confidentiality and integrity of data transmitted between monitoring devices. Encryption is a critical defense against possible cyber-attacks in power monitoring [31]. In parallel, cloud integration is a revolutionary method that substantially impacts data storage, accessibility, and the general operation of solar energy systems [32]. Cloud solutions are essential for facilitating remote access to critical solar parameters, providing scalability, flexibility, and redundancy in data storage. Research highlights the importance of robust authentication systems and data encryption while they are in the cloud [33]. In addition, cloud-based analytics are essential for analyzing large amounts of data from solar systems, offering optimization insights, and enabling predictive maintenance. The research in [34] clearly states how the interest in cybersecurity research in renewable energy has dramatically increased over the years.

One research paper [35] presents an innovative advancement in monitoring solar PV systems by introducing a novel data-collecting system based on the IoT. The proposed system provides a remedy for the inherent constraints of wired and wireless monitoring systems, which often encounter exorbitant expenses, limited availability, and labor-intensive operating requirements. Moreover, the suggested solution utilizes open-source software and cloud services, which offer cost-efficiency and readily available options. The proposed innovative method allows for real-time monitoring and thorough data collection from the PV system, making assessment and optimization of performance easier. Although the study properly presents a monitoring system that is both affordable and easily accessible, it fails to address the crucial issue of cybersecurity in IoT-based renewable energy systems. The absence of any focus on evaluating and reducing possible security and privacy weaknesses in these systems highlights a significant problem that requires attention. To fill this gap, our study prioritized strengthening security measures in renewable energy remote monitoring systems. This significant addition addressed the need for more solid security measures in connected renewable energy monitoring systems.

In article [36], the authors presented a wireless IoT network system that connects with a smart grid system. Its objective was to monitor the state of an unstable microgrid. The researchers suggested using a delay-universal coding system and a step-by-step estimate technique to address problems in the wireless connection and optimize the use of a specific coding method. By performing numerical testing, they demonstrate that this communication approach, in combination with the estimate strategy, successfully monitors the condition of any uncertain microgrid. The article also investigates the impact of various wireless network configurations on tracking capabilities. In addition, it compares the suggested technique and a regular block coding method, showing that the new approach surpasses the old one in terms of monitoring performance. Nevertheless, a significant drawback in the article is the need for more analysis or acknowledgment of possible cyber vulnerabilities in the communication infrastructure. The likelihood of malicious interception by hackers constitutes a significant concern. Although the architecture effectively reduces communication failures, a security compromise might still result in disruptive behaviors that could destabilize the grid system.

Another research paper [37] explores the cybersecurity aspects of exchanging renewable energy certificates (RECs) using distributed ledger technology (DLT) and blockchain. The statement emphasizes the crucial need for secure techniques to track and verify the source of energy resources while assuring the security of transactional operations related to renewable energy certificates (RECs). The article provides a thorough overview of the essential cybersecurity requirements that are necessary to protect REC-related data and applications. This entails using the NIST Smart Grid Cybersecurity Controls as a point of reference and suggesting a cybersecurity maturity model derived from the NIST Cybersecurity Frameworks. The research underscores the need to align and adapt the system when implementing a fully functioning DLT-based REC trading platform in current electricity markets and systems. It also highlights the compatibility of DLT technology with existing cybersecurity standards. Furthermore, it strongly emphasizes the need for a comprehensive evaluation of power system, communication, and cybersecurity standardized frameworks before commencing operational trials of the suggested use case.

Article [38] examines the preservation of end-user privacy in the smart grid by explicitly studying the usage of homomorphic encryption. The primary aim of the research was to protect consumers' personal information using homomorphic encryption methods. This encryption technique allows energy providers to interact with encrypted data without decryption, preserving sensitive information's security. The paper emphasizes the continuous testing and application of these methods, using Raspberry Pi devices as a crucial component of the experimental configuration. This study represents a significant advancement in safeguarding privacy in smart grid systems while allowing for necessary operations on encrypted data. It can promote greater security and privacy protection in the energy industry. In contrast, our research focuses on ensuring data security from solar

monitoring systems. This is achieved using the Advanced Encryption Standard (AES) with a myRIO board and a secure cloud infrastructure. Although both study fields focus on data security in the energy sector, there are substantial differences in the method and technology used. We prioritized securing the solar monitoring system by using AES encryption and a customized hardware configuration to improve security and integrity within the system.

Therefore, our research developed a new method to enhance the security of remote monitoring systems for solar energy. The research integrated advanced technologies, including Advanced Encryption Standard (AES), myRIO board, and NI's SystemLink Cloud platform, to enhance data security in smart solar energy monitoring systems. The study leverages the combination of LabVIEW programming with G Web Development tools to provide efficient data acquisition and communication with cloud services. Subsequently, we carefully implemented AES (Advanced Encryption Standard) encryption to guarantee secure data transmission inside solar systems. The study progressed beyond solely implementing AES and included preventative measures such as modeling possible attack scenarios on the system. Furthermore, we thoroughly investigated the integration of SystemLink Cloud, guaranteeing the ability to securely access critical solar parameters from a remote location.

3. Materials and Methods

3.1. System Architecture

Figure 1 depicts the overall design of the system. The architecture of this remote monitoring system is specifically intended to efficiently and securely monitor the characteristics of solar energy, including voltage and temperature, in a solar system. In the implementation of the security aspect of the study, two PV parameters, namely, voltage and temperature, were employed. It is worth noting that other PV parameters, such as current, light intensity, etc., can also be incorporated using the same methodology. The sensors are connected to a myRIO board, the central processing unit. The myRIO board is vital in collecting sensor data and using Advanced Encryption Standards (AES) to encrypt them in our system. The myRIO board and the PC are linked wirelessly using Wi-Fi, allowing communication between these components. The use of Wi-Fi for transmitting data from sensors in solar energy systems offers several benefits, including widespread accessibility, affordability, and the capacity to monitor and analyze data in real time [39]. Although we used Wi-Fi in our architecture to transmit data, other wireless communication technologies, such as cellular networks or specialized communication protocols, may also be used, depending on particular needs and limitations. The experiment is implemented for short distances, and, therefore, Wi-Fi is suitable. The wireless connection enables encrypted data transmission from the myRIO board to the PC. Upon reaching the computer, the encrypted data are decrypted using LabVIEW software. The encrypted data are shown on the local computer and transferred to a cloud application called SystemLink Cloud for remote monitoring.

The web application hosted on the SystemLink Cloud is designed using G Web Programming tools. This program facilitates the development of a user-friendly interface that can be accessed by web browsers, allowing users to conveniently monitor the solar system from any location with internet connectivity. Deploying this web application in the cloud using SystemLink Cloud significantly improves its accessibility. Cloud hosting guarantees the online availability of the program, enabling users to access it remotely without any limitations based on location. Users may conveniently access the monitoring dashboard or interface of the SystemLink Cloud platform by logging in using their web browsers. The SystemLink Cloud application acts as a platform for users to monitor the solar system from a distant location. The technology offers a user-friendly interface or dashboard that allows anyone to obtain real-time data on the voltage and temperature of the solar system. The ability to monitor remotely is essential for effective maintenance and prompt detection of any anomalies in the system.

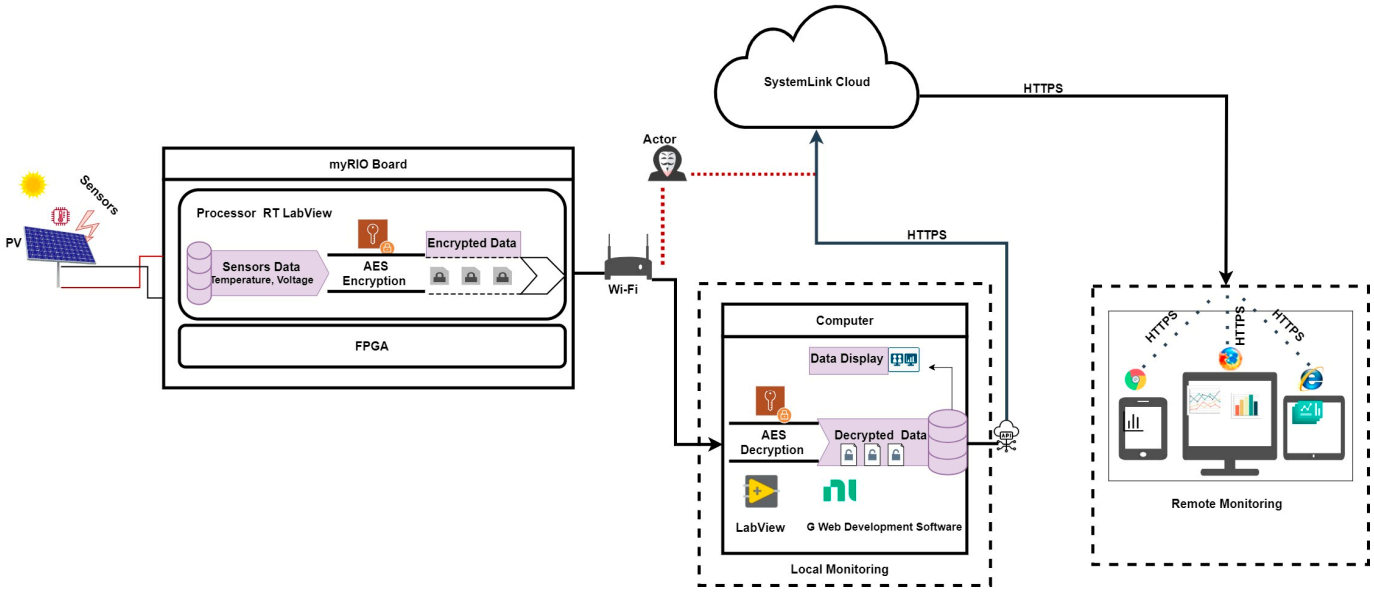

Figure 1. Overall system architecture.

3.2. NI myRIO-1950 Board

The myRIO board-1950 [40], created by National Instruments, is a crucial tool in embedded system development, demonstrating a powerful blend of features and capabilities. The myRIO board incorporates an FPGA fabric and a dual-core ARM Cortex-A9 CPU in a Xilinx Zynq system-on-chip (SoC). This integration provides the board with a powerful combination of processing power and versatility essential for various applications. The myRIO board excels in its flexible input/output interfaces, which include digital I/O, analog inputs, PWM outputs, and a wide array of communication interfaces (SPI, I2C, UART, USB). The myRIO board is essential in educational environments, as it is a crucial platform for students and engineers to delve into embedded systems, control theory, signal processing, and data collection. Figure 2 illustrates the arrangement and functionalities of the NI myRIO-1950 components. The graphic depicts two parts: (a) illustrates the Real-Time (RT) process of myRIO, while (b) showcases the Field-Programmable Gate Array (FPGA) of myRIO. In the RT processor, we have implemented the standard (AES) algorithm. Hence, the project's selection of the myRIO board was based on its adaptable integration capabilities, a wide range of input/output interfaces, wireless connectivity for remote monitoring, compatibility with LabVIEW for efficient development, educational significance, and suitability for small-scale embedded systems projects.

3.3. SystemLink Cloud

SystemLink [41] is a resilient cloud-based platform developed by National Instruments. It is a centralized hub for gathering, storing, and analyzing data from several interconnected devices and systems. SystemLink is essential for optimizing remote monitoring and management procedures, providing a comprehensive set of tools and services designed to improve data collection, processing, and visualization. The platform functions as a centralized storage system, gathering data from many sources, including IoT devices, sensors, and instruments, to provide a holistic perspective on the operation and behavior of the system. The platform's main feature is its remote monitoring and visualization ability. Users are enabled to receive real-time data from linked devices using configurable dashboards and graphical representations. The ability to monitor in real time provides instant visibility into the system's functioning, enabling quick decision-making. In addition, SystemLink offers advanced analytics tools specifically built to handle and analyze the gathered data. These technologies facilitate extracting valuable insights, trends, and patterns, empowering users to make well-informed choices and effectively execute diagnostics. The critical advantage

of SystemLink is its ability to effortlessly integrate with a diverse range of hardware and software platforms, enabling smooth connection. The support for APIs and developer tools enables the development of customized integrations and applications specifically designed to meet project needs. The project heavily relied on SystemLink since it could gather data from different devices, allowing remote monitoring, and due to its security features.

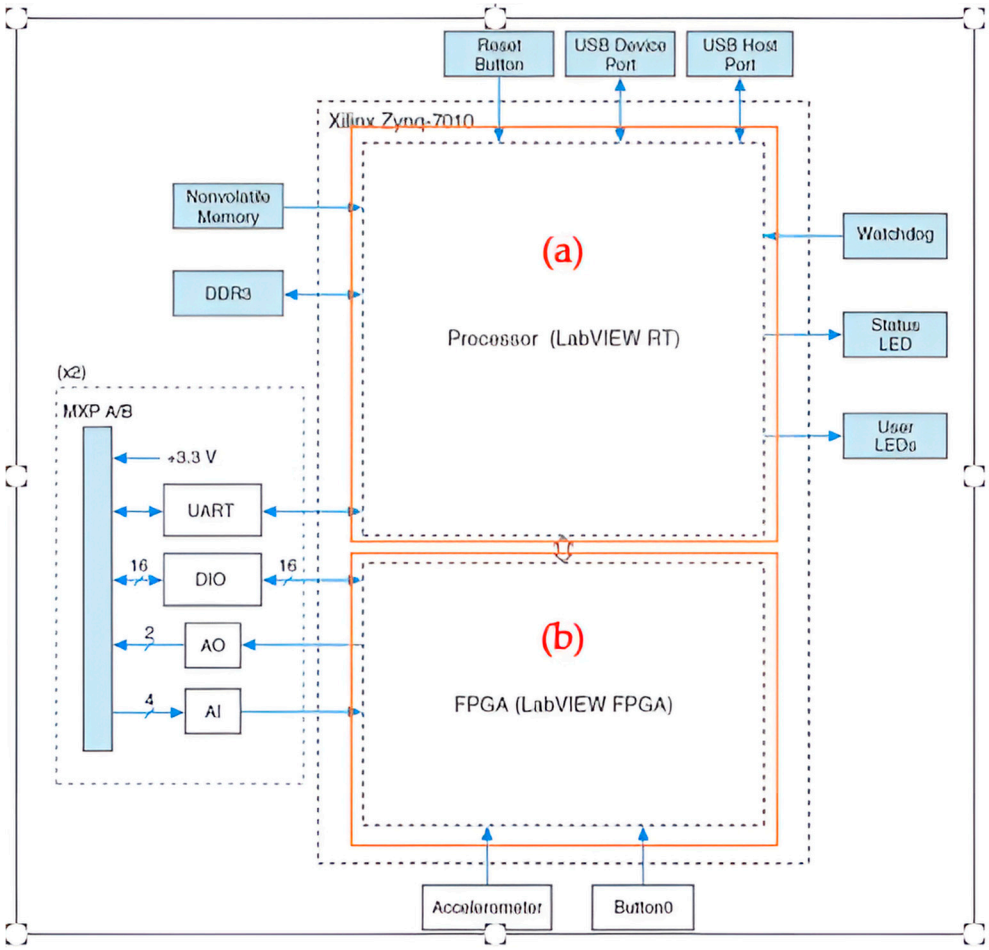

Figure 2. NI myRIO-1950 hardware block diagram [40].

3.4. Web Application for Web User Interface

A web user interface (UI) enables remote monitoring and control of the system, irrespective of the geographical location. This access might originate from a device inside the same network or any location. Employing web technology for these remote interfaces obviates the need to install specific apps on client devices such as desktops or mobile phones. The G Web Development Software 2021 [42] developed by National Instruments (NI) has a dual function. It offers an editor that generates the web application's user interface and client-side code. Furthermore, it provides hosting and data services, facilitating the sharing of web applications either inside the local network or across the internet. Depending on personal needs, there is the option to either use these technologies together or include individual components with external tools. Our approach utilizes remote monitoring to provide universal internet access.

The G Web editor simplifies the creation of WebVIs (Web Virtual Instruments). Although it may have a distinct appearance compared to LabVIEW, it utilizes a version of the G language that operates via a web browser. Modifying the panel of a WebVI is similar to LabVIEW, with a selection of controls and indicators designed explicitly for engineering purposes. Significantly, G Web enables the development of flexible designs that automatically adapt to different screen sizes. This feature allows for a unified WebVI

that appears ideal across browsers and mobile devices. The editor creates applications using HTML, JavaScript, and CSS, which are fundamental components of web applications. Hosting services acquire these application files and store them at a specific URL, similar to how accessing a URL such as ni.com retrieves a web application's HTML, JavaScript, and CSS files.

After the web application is launched in a browser, such as on a mobile device, data services facilitate communication between the web application and the system. The G Web Development Software encompasses hosting and data services, providing all the essential elements for constructing a complete online application. The methodology used is developing a web application that can be accessed over the internet using the hosting services provided by systemlinkcloud.com. This approach guarantees safe user access without the need to maintain a server that is publicly accessible. NI provides industry-standard HTTPS security for hosting apps and enables access and permissions via users' ni.com accounts (accessed on 5 December 2023).

At first, we modified our LabVIEW system to use data services to publish data to SystemLink. Although the main emphasis is on using LabVIEW in this situation, it is essential to mention that NI has data service APIs for other programming languages like Python and C# if the system includes components developed in those languages. In the future, we will create a web application and upload it to SystemLink's Hosting service, providing a URL for accessing the program on devices like smartphones. Since the web application runs on our device, we will employ data services to establish communication with SystemLink and obtain the data from our system.

3.5. SystemLink Cloud API Connection

Figure 3 shows the connection between SystemLink and our system. The workflow includes initial authentication through the creation of an API key in SystemLink, the establishment of connections through the functionalities of LabVIEW, the transmission of voltage and temperature data to SystemLink tags, the verification of data reception in the Data section of SystemLink, and the replication of the same functionality in a web application project through the use of G Web Development Software. The following steps are taken for the connectivity:

Authentication and establishing a Connection to the SystemLink Cloud: First, log in to SystemLink using the credentials associated with an NI account to generate an API key. Through the Security section, an API key is generated, which is a unique identification used for authentication. It is copied to a local document to refer to the API key value in the future. The naming must be proper so that its application may be identified;

1. Using the API Key in LabVIEW: In LabVIEW, the Open Connection function is used to establish a connection to SystemLink using the API key and server URL (api.systemlinkcloud.com). Once the API key has been pasted into the constant provided to Open Configuration, authentication for data transfer is established;
2. Transmission of data to the SystemLink: Opening a tag and giving it a name is the first step in creating a tag. If the tag does not exist, this operation will create it first;
3. Writing voltage and temperature data: Send the voltage and temperature data that have been acquired to the write tag that has been defined in SystemLink;
4. Verification of tag creation: Upon executing LabVIEW VI, examine the Data section of SystemLink to validate the establishment of the tag and the successful receipt of data. At this step, we ensure that the communicated voltage and temperature values are accurately shown in the tag on SystemLink;
5. G Web Development Software: Using G Web Development Software, we develop a web application project and use the same code that we used in LabVIEW throughout the development process. First, using our API key, we establish a connection to SystemLink. Next, open the tag by its name. Finally, read it. The value is wired to both our indicator and our charts simultaneously.

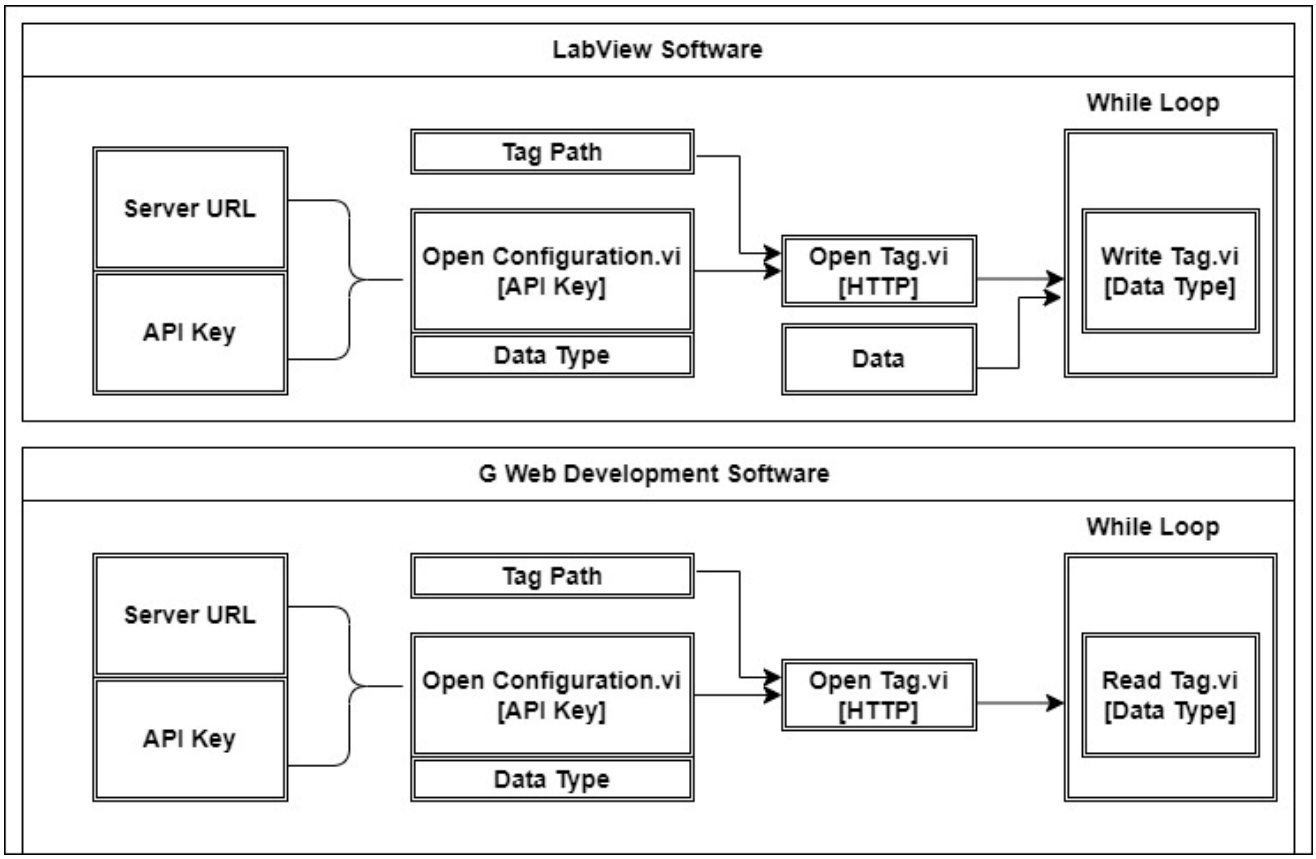

Figure 3. SystemLink Cloud connectivity.

3.6. Advanced Encryption Standard (AES)

The Advanced Encryption Standard, or AES [43], is a popular symmetric encryption algorithm for protecting private information. It works with keys that are 128 bits, 192 bits, or 256 bits in size and with fixed block sizes that are 128 bits. In order to convert plaintext into ciphertext, AES uses a series of mathematical operations such as XOR, substitution, shifting, and permutation. It has become the de facto standard for data security in communications, software, and hardware because of its reputation for resilience, speed, and resistance to different cryptographic attacks. Figure 4 illustrates the summary of how AES works, and the process is explained below:

1. Key Expansion: The procedure starts with key expansion. The initial key undergoes a sequence of modifications to generate a collection of round keys. The keys are generated by a key schedule method, which produces subkeys for each cycle of the encryption process;
2. Initial round key addition: The process of first-round key addition involves dividing the 128-bit plaintext block into a 4×4 matrix, which is referred to as the State. The first step entails performing an XOR operation (AddRoundKey) between the State and the first-round key.
    - Rounds: AES works by executing a sequence of rounds, with the specific number defined by the size of the key—10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key, as shown in Table 1 for AES parameters. Every round has four primary transformation steps: SubBytes: This stage entails substituting each byte individually using a predetermined lookup table known as an S-box. The S-box is used to substitute each byte in the State matrix with another byte;
    - ShiftRows: During this stage, the bytes inside the State matrix are cyclically moved across the rows. The first row stays unaltered, the second-row changes

one position to the left, the third row shifts two places to the left, and the fourth row shifts three positions to the left;

- MixColumns: This stage applies a mathematical operation to each column in the State matrix, considering the column as a polynomial and multiplying it by a predetermined polynomial. This mixing step enhances the dispersion and obfuscation of the data;
- AddRoundKey: The State matrix is XORed with a round key that is derived from the key schedule. The encryption procedure becomes much more challenging after completing this phase;

3. Last Round: The MixColumns step is omitted in the last round to streamline the decryption procedure. The components include SubBytes, ShiftRows, and AddRoundKey;
4. Output: The ciphertext is represented by the State matrix that is produced when the last round is finished;
5. Decryption: Decryption in AES entails a similar but reversed procedure. The ciphertext is subjected to a reverse transformation, employing the round keys in the opposite order. To obtain the original plaintext, the inverse procedures (InvSubBytes, InvShiftRows, InvMixColumns) are used in addition to the AddRoundKey step.

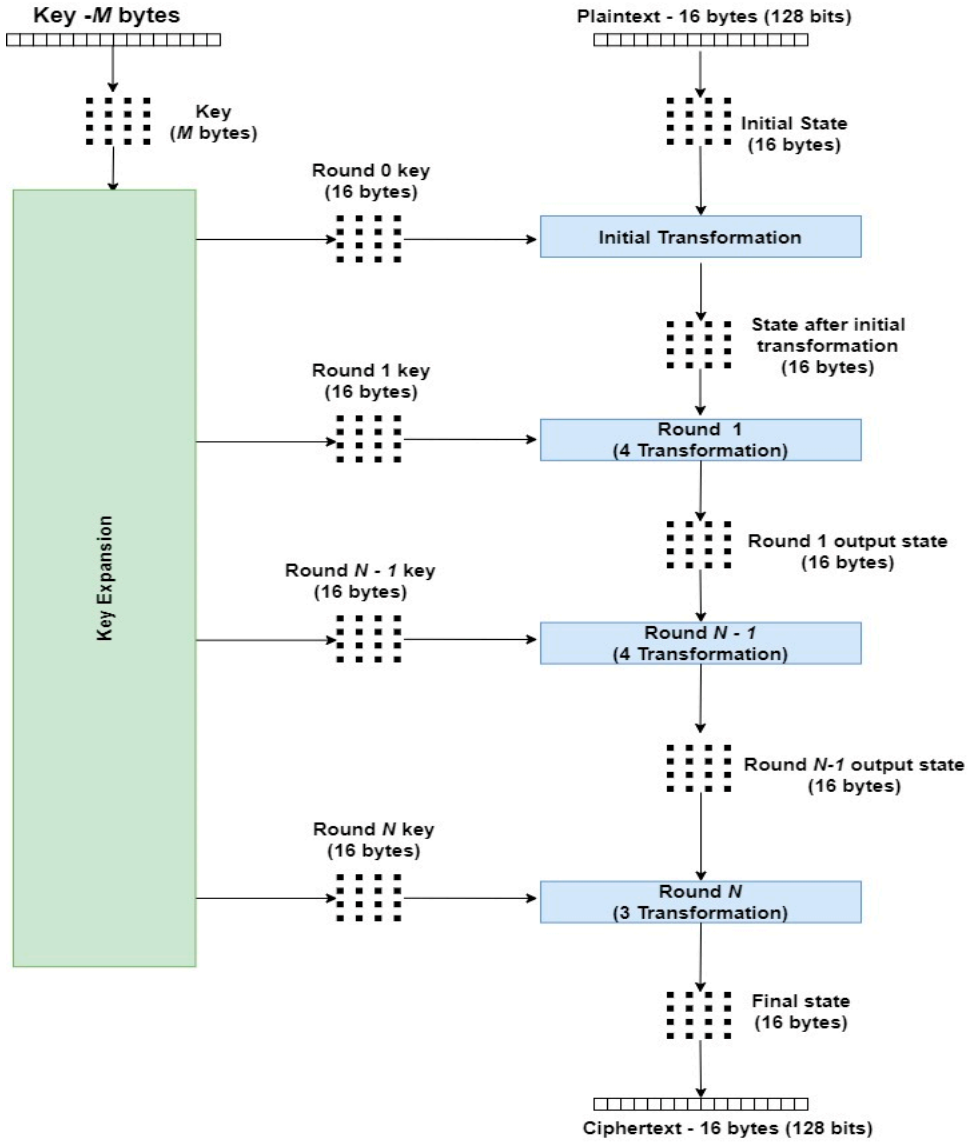

Figure 4. Advanced Encryption Standard architecture [31].

Table 1. Advanced Encryption Standard parameters.

AES Parameters	AES-128	AES-192	AES-256
Key size	128	192	256
Plaintext block size	128	128	128
Number of rounds	10	12	14
Round key size	128	128	128

The LabVIEW Cryptography Toolkit [44] was used to carry out the AES encryption and decryption procedures in this study. The encryption was implemented to protect the data, voltage, and temperature measurements transmitted from the solar energy system's sensors to a computer over Wi-Fi. The toolkit enables the implementation of symmetric encryption and decryption, and it includes all block cypher modes [45] of operation with various key lengths, such as 128, 192, and 256 bits. However, in the context of IoT, where nodes often have limited resources, using classical cryptographic algorithms is costly and inefficient [46]. In light of this issue, our work implemented Electronic Codebook Mode (ECB) with a key of 256 bits in our system. This mode of operation is suitable for IoT applications with small payload lengths, usually less than 16 bytes [47]. This strategic decision aligns with the need to maximize security measures in the limited-resource environment of IoT nodes while maintaining a careful balance between strong cryptography and operational efficiency. Figure 6 shows the AES encryption method inside LabVIEW's graphical programming environment. It demonstrates the methodical process of encrypting data acquired from sensors. The illustration consists of linked blocks or components representing the various steps of the LabVIEW Cryptography Toolkit's AES encryption process. These blocks represent the process of converting raw sensor data into encrypted ciphertext, which guarantees the confidentiality of the data while they are being transmitted. On the other hand, the decryption process that is implemented inside LabVIEW is shown in Figure 7. This schematic shows how the LabVIEW Cryptography Toolkit's AES decryption decodes the encrypted data that the myRIO board sends to the computer via Wi-Fi. This shows the process of receiving encrypted data, decrypting them, and then obtaining the original plaintext. The pseudo-code procedure of the AES architecture is illustrated in Figure 5.

3.7. PV Module and Sensors

For PV data acquisition in this project, two essential components are employed: a compact monocrystalline PV module for measuring voltage and a TMP116 Sensor [48] for recording temperature. The TMP116 Sensor, manufactured by Texas Instruments, provides very accurate temperature measurement with a precision of ± 0.1 °C. It can measure temperatures within a broad range from -55 °C to 125 °C. The device's minimal energy use, data transmission via the I2C (Inter-Integrated Circuit) protocol, and ability to provide alerts boost its adaptability for many uses. Additionally, its small size allows for easy incorporation into systems with limited space. The sensor's outstanding reliability and adaptability make it an excellent option for accurate temperature monitoring. Integrating these components with the myRIO-1950 board entails refined connections and communication protocols. The compact monocrystalline PV module, which produces a voltage when lighted, is directly connected to the myRIO-1950 board. This connection is used to measure the voltage output of the PV module. The myRIO board successfully monitors and collects the voltage readings from the PV module by using its analog input channels. This integration is essential for acquiring accurate voltage data from the PV module for analysis and monitoring.

The TMP116 Sensor utilizes the I2C [49] protocol as a digital temperature sensor. The protocol, known for its simple nature and effectiveness, offers a standardized means of communication to establish a connection between digital sensors like the TMP116 and microcontrollers like the myRIO-1950 board. The TMP116 Sensor utilizes the I2C protocol to enable connection with the myRIO board. To successfully integrate the TMP116 Sensor with the myRIO-1950 board, we established physical connections between the sensor

and the I2C ports or pins. Connecting the TMP116 Sensor through the I2C protocol is detailed in the sensor datasheet [48]. LabVIEW's I2C driver libraries form a connection between the myRIO board and the TMP116 Sensor. LabVIEW programming is essential for coordinating the transmission and the collection of temperature data from the TMP116 Sensor over the established I2C connection. Therefore, this establishes the foundation for detailed analysis, monitoring, and control of the monitored systems. Integrating devices, supported by LabVIEW programming and adherence to the I2C communication protocol standards, guarantees a robust and reliable data collection procedure, which is crucial for exact measurements and subsequent analysis within the project's scope.

```
function AES_Encrypt(plaintext, key):
    round_keys = KeyExpansion(key)
    state = AddRoundKey(plaintext, round_keys[0])

    for round in 1 to Nr-1:
        state = SubBytes(state)
        state = ShiftRows(state)
        state = MixColumns(state)
        state = AddRoundKey(state, round_keys[round])

    state = SubBytes(state)
    state = ShiftRows(state)
    state = AddRoundKey(state, round_keys[Nr])

    return state

function AES_Decrypt(ciphertext, key):
    round_keys = KeyExpansion(key)
    state = AddRoundKey(ciphertext, round_keys[Nr])

    for round in (Nr-1) down to 1:
        state = InvShiftRows(state)
        state = InvSubBytes(state)
        state = AddRoundKey(state, round_keys[round])
        state = InvMixColumns(state)

    state = InvShiftRows(state)
    state = InvSubBytes(state)
    state = AddRoundKey(state, round_keys[0])

    return state
```

Figure 5. AES pseudo-code.

3.8. LabVIEW Program

LabVIEW plays a significant role in our process, serving as a robust tool that enhances the efficiency and security of our solar system monitoring setup. LabVIEW is well-recognized for its advanced graphical programming features, allowing us to manage intricate operations, including data collecting and processing, effortlessly. Figure 6 is a visual depiction that clarifies the stages in our LabVIEW software. This diagram illustrates the flow of data from sensor inputs to encryption procedures, offering a concise representation of how LabVIEW oversees the many elements in our monitoring system. LabView efficiently handles both digital and analog inputs from sensors inside this framework. The device utilizes the I2C protocol to collect data from the digital temperature sensor, demonstrating its versatility in connecting with many sensors. LabVIEW concurrently and effectively acquires voltage data from the solar system using analog inputs, a crucial element in our monitoring procedure. LabVIEW enhanced the security of our transmitted data by using AES encryption, which utilized a robust 256-bit key. LabVIEW's implementation highlights its proficiency in managing complex encryption methods, guaranteeing the secrecy and reliability of our sensitive data. Furthermore, Global Variables in the LabVIEW program enabled smooth encrypted data transfer.

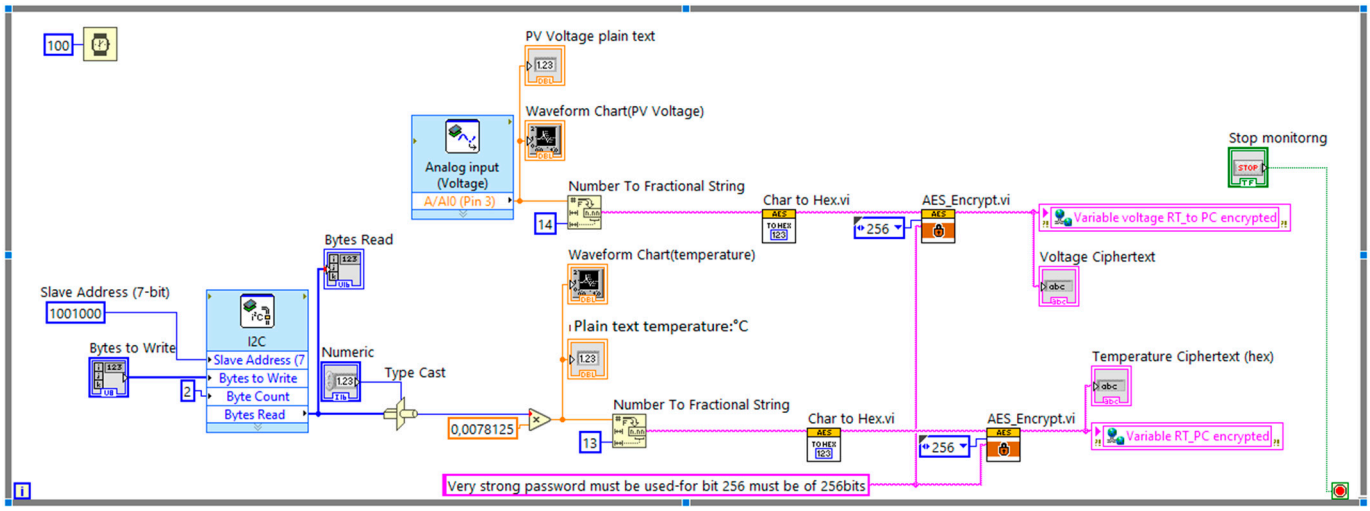

Figure 6. LabVIEW data acquisition and encryption.

Keeping with our approach, Figure 7 shows the LabVIEW program where the encrypted data received from the myRIO board are decrypted using the same encryption key by using the AES decryption procedure. The constancy of this encryption key guarantees a smooth decryption procedure, facilitating the conversion of the encrypted data back to their original state. After the data have been successfully decrypted, they may be used inside our monitoring system for various reasons. Initially, the deciphered data might be shown locally on the computer. The local display allows immediate and on-site monitoring of critical parameters such as voltage and temperature, offering real-time monitoring of the solar system's efficiency. In addition, the decrypted data are transmitted to the SystemLink Cloud platform, as explained before. By establishing a link to SystemLink Cloud, users may remotely monitor and view the solar system's data from any place with an internet connection. The cloud-based platform provides a user-friendly interface or dashboard, allowing users to monitor and analyze the decrypted data remotely in a comfortable and easily accessible way. As previously elucidated, the incorporation of SystemLink Cloud into our monitoring system showcases the harmonious interaction between our on-site monitoring configuration and the ability to access it remotely using cloud-based services. This link enables users to effortlessly monitor and comprehensively assess the solar system's performance, whether nearby or at a distance. Table 2 lists the materials used in this study.

Table 2. List of materials used in the study.

No	Tool	Software	Hardware	Ref.
1	LabVIEW 2019	✓		[50]
2	SystemLink Cloud	✓		[41]
3	NI myRIO-1950 board		✓	[40]
4	PV module		✓	[51]
5	TMP116 sensor		✓	[48]
6	Wireshark 4.0.5	✓		[52]
7	G Web development Software 2021	✓		[42]
8	Advance Encryption Standard	✓		[44]
9	Wi-Fi technology	-	-	[53]
10	Windows 10 PC		✓	

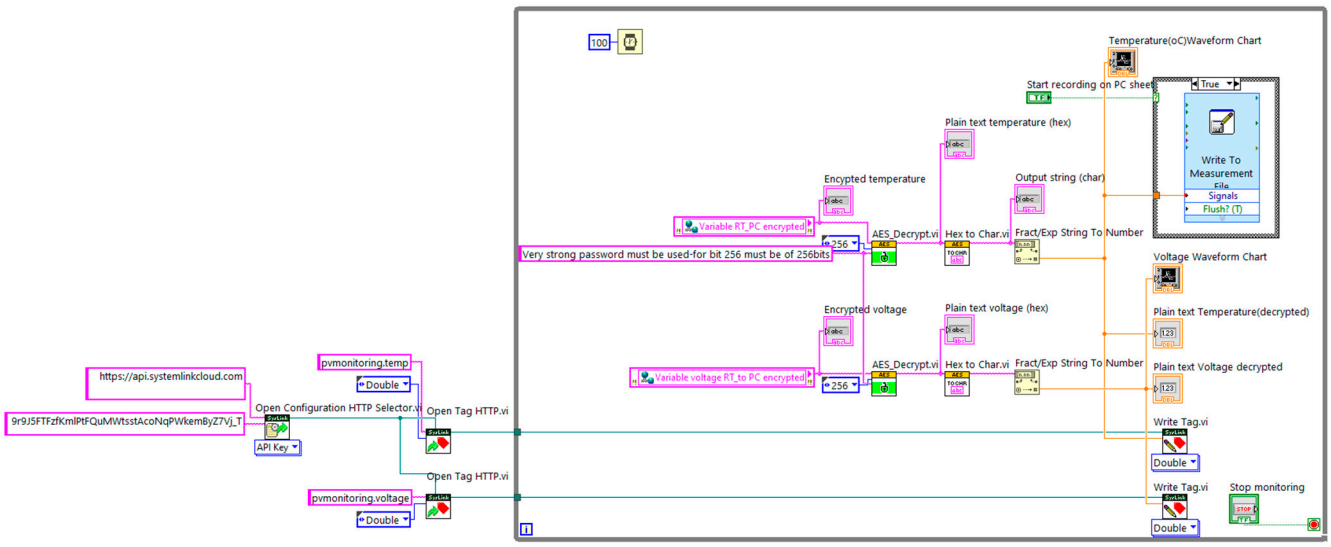

Figure 7. LabVIEW AES decryption and connection with the cloud platform.

4. Results and Discussion

Analyzing the system's vulnerability before applying AES encryption was a critical test in our system security analysis. Before encrypting, we conducted a simulated breach by playing the role of a malicious actor in the communication channel between the myRIO board and the computer via Wi-Fi. Figure 8 illustrates this situation, depicting data transfer in plain text without encryption. Transferring data in their original, unencrypted form introduces substantial security vulnerabilities into the system. An unencrypted data transmission may be used by a malicious party, such as a cybercriminal, to pose significant risks to the system's integrity and confidentiality, such as the following:

- Data Interception and Collection: Intercepting unencrypted data allows hackers to gain unauthorized access to critical information about the solar system's characteristics, including voltage and temperature measurements. The captured data might be gathered and kept for analysis or immediate exploitation;
- Tampering and Manipulation: The hacker can alter the delivered information with access to unencrypted data. This manipulation may include modifying voltage measurements or inserting fabricated data, resulting in inaccurate interpretations, system faults, or complete shutdowns;
- Security Breach and Network Vulnerability: The transfer of unencrypted data has consequences that extend beyond the local system. This may compromise other networked devices or systems, increasing the number of security threats;
- Privacy Violation: Apart from manipulating the system, the intercepted data may include sensitive or personally identifiable information, which might violate user privacy or expose crucial operational facts about the solar system configuration;
- Strategic Reconnaissance: The act of intercepting unencrypted data, which enables the threat actor to analyze patterns of communication. This analysis may serve as a foundation for more advanced targeted attacks or for gaining deeper access to the system;
- Exploitation of Vulnerabilities: Malicious individuals may take advantage of any weaknesses found in the unencrypted data transfer to gain extended access to the system or carry out further attacks, increasing the overall risk.

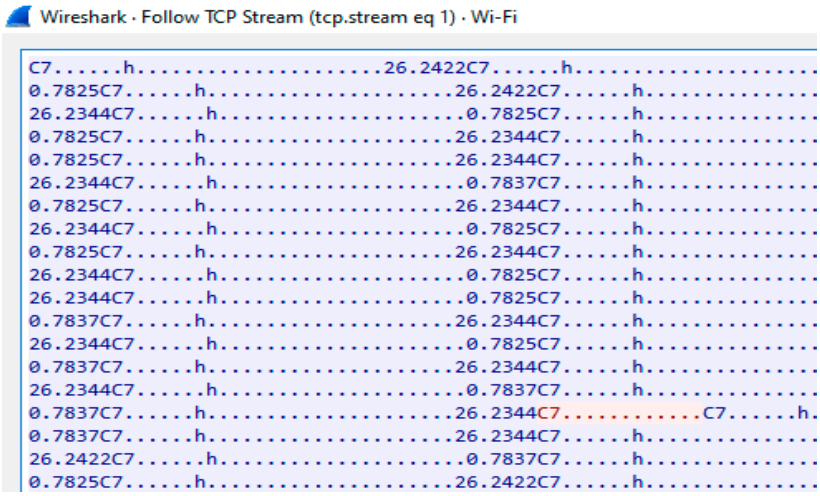

Figure 8. Plain-text data captured by Wireshark before encryption.

Therefore, the scenario highlights the essential need to use robust encryption algorithms, like AES, to strengthen the security of the data being transferred. The successful deployment of the AES-256 encryption protocol represents significant progress in enhancing the security of data transmission from the myRIO board to the PC over Wi-Fi. Figure 9 provides a visual representation of the LabVIEW front panel, demonstrating the encryption procedure that guarantees the confidentiality and integrity of the sent data. The AES-256 encryption technique, which is generally acknowledged as strong, ensures a high degree of cryptographic security using a 256-bit key. The LabVIEW front panel visualization demonstrates the systematic transformation of raw data into their encrypted form using AES-256 encryption. This portrayal highlights the elaborate but organized procedures required to ensure the security of the sent data. Within this panel, the encryption algorithm converts essential data, such as voltage and temperature measurements from the solar system sensors, into a cipher text format that is difficult to decode without the corresponding decryption key. Implementing AES-256 encryption in the LabVIEW framework demonstrates a proactive stance in safeguarding data security.

The decryption step is crucial in regaining the original information for local and remote monitoring after transmitting AES-256-encrypted data from the myRIO board to the PC using Wi-Fi. Figure 10 demonstrates the LabVIEW front panel and provides a visual illustration of the decryption process, demonstrating the conversion of encrypted data back to their original, readable form. The decryption process described utilizes the same AES-256 encryption key used during the encryption phase. The symmetrical nature of the key used for encryption and decryption is crucial, as it guarantees a smooth and accurate reversal of the encryption process. The encrypted data gained via this method are crucial in several ways. Firstly, they enable quick local monitoring on the computer, allowing real-time evaluation of essential metrics for prompt system interventions or modifications. Furthermore, as previously mentioned, the decrypted data may be securely communicated to the SystemLink Cloud, allowing for remote monitoring and analysis. Therefore, the solar system's performance can be monitored and accessed easily, assuring both accessibility and continuity.

The system's security was assessed after implementing AES encryption, which required modelling possible breaches by acting as a threat actor. We used the Wireshark program to intercept the Wi-Fi traffic between the myRIO board and the computer. Figure 11 graphically represents the data captured by Wireshark, illustrating the effective encryption of sent information. The data recorded in Wireshark demonstrate the encrypted structure of the transferred information. This encryption guarantees that any data collected will be transformed into an unintelligible form, known as ciphertext, making it impossible for unauthorized hackers seeking to eavesdrop on the communication channel to understand

or decode them. Hence, this encryption's effectiveness confirms the system's capacity to preserve sensitive data, emphasizing AES-256 encryption as a reliable defense against security risks and illegal access while transmitting data.

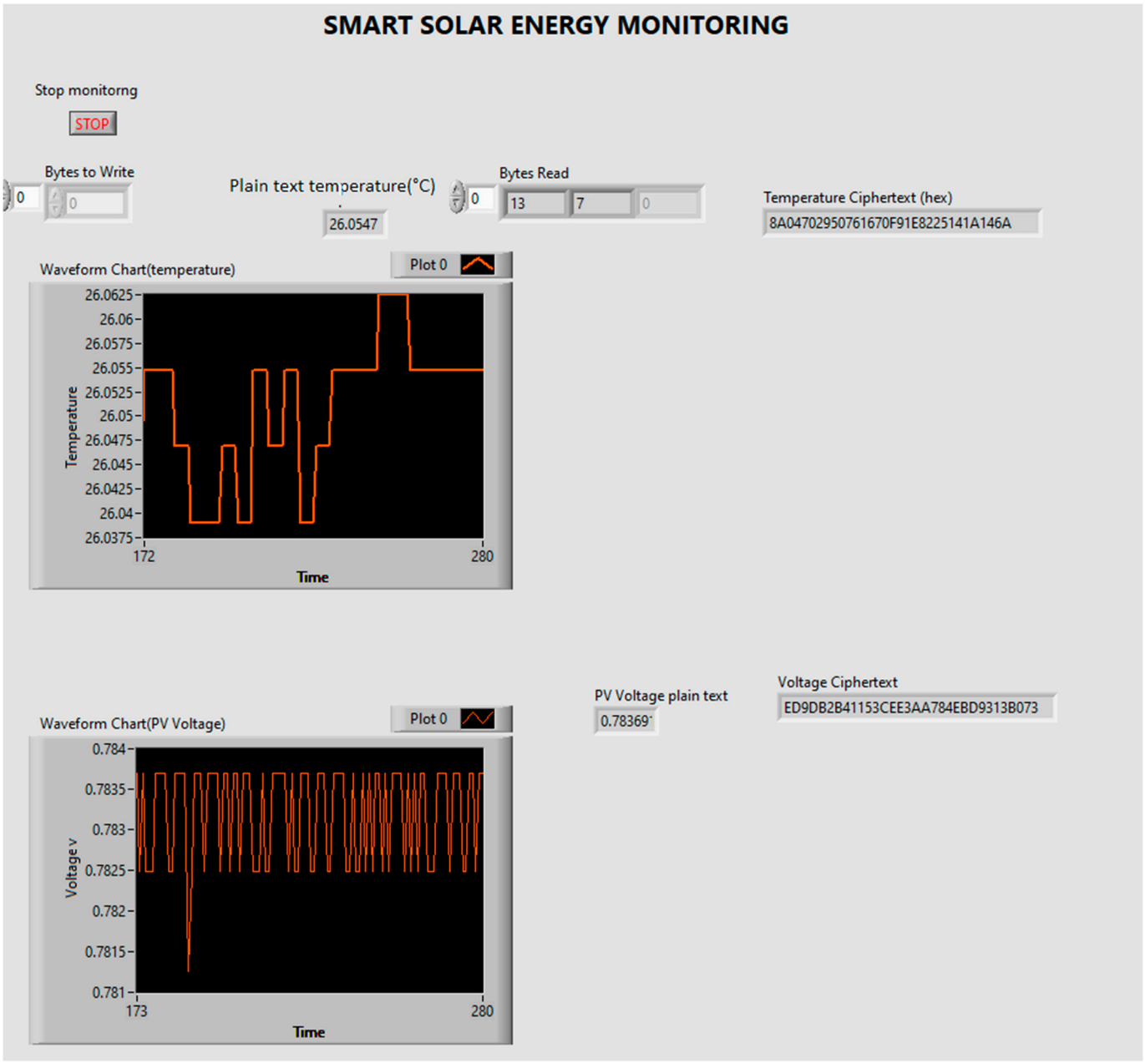

Figure 9. Encrypted data in the LabView front panel.

In addition, we evaluated the security of remote monitoring throughout the SystemLink Cloud platform. We focused on intercepting traffic from SystemLink Cloud to individuals accessing it using the Chrome browser from a computer. The security testing was to ensure the privacy and confidentiality of data transfer during remote monitoring sessions. Our Wireshark inspection, shown in Figure 12, revealed a comforting finding: the transmission was encrypted using TLS 1.2. Transport-Layer Security (TLS) is a cryptographic protocol that provides safe communication over a computer network; version 1.2 is notable for its strong encryption capabilities and defends against intruders attempting to exploit communication channel vulnerabilities.

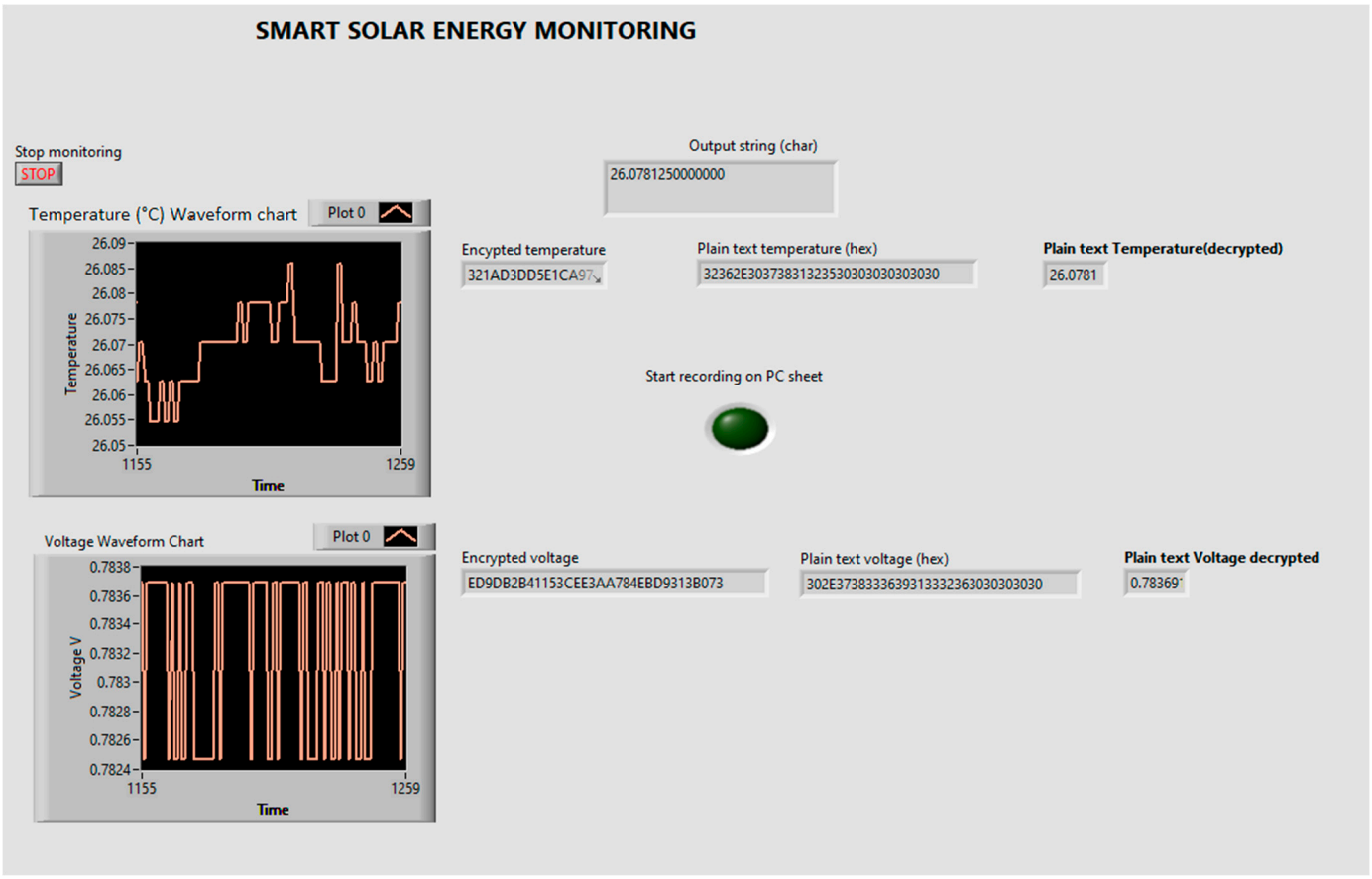

Figure 10. Decrypted data on PC-LabVIEW front panel.

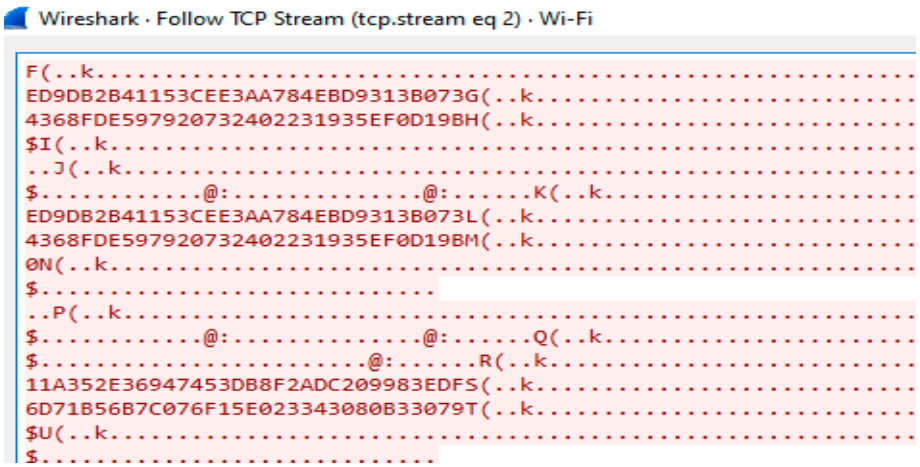

Figure 11. Encrypted data captured within Wireshark.

Integrating remote monitoring via the SystemLink Cloud is a notable advancement in our system, facilitating the retrieval of essential solar system data from any geographical location. Figure 13 visually represents a solar system dashboard on the SystemLink Cloud platform. It presents voltage and temperature measurements for monitoring and analysis. The visualization in SystemLink Cloud displays a user-friendly dashboard that provides essential solar system metrics, including voltage and temperature, for immediate monitoring and analysis. Users may safely access the dashboard from any location, allowing them to gain detailed insights into the solar system's performance. HTTPS is employed to guarantee secure data transmission to SystemLink Cloud, ensuring information confiden-

tiality and integrity. The intuitive dashboard design equips users with the necessary tools to monitor trends, set alerts, and make informed decisions for optimized management of solar systems.

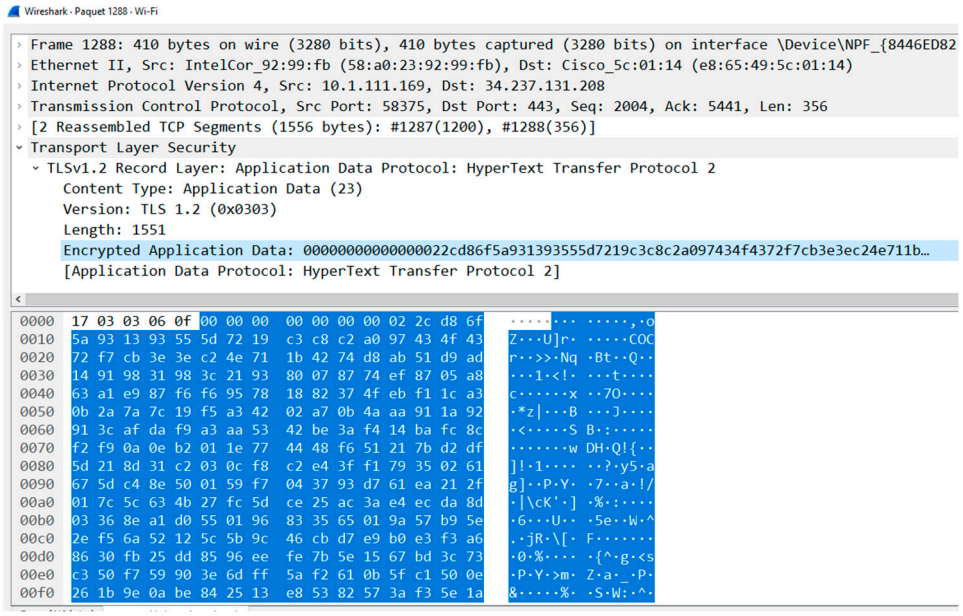

Figure 12. Encrypted communication for remote monitoring.

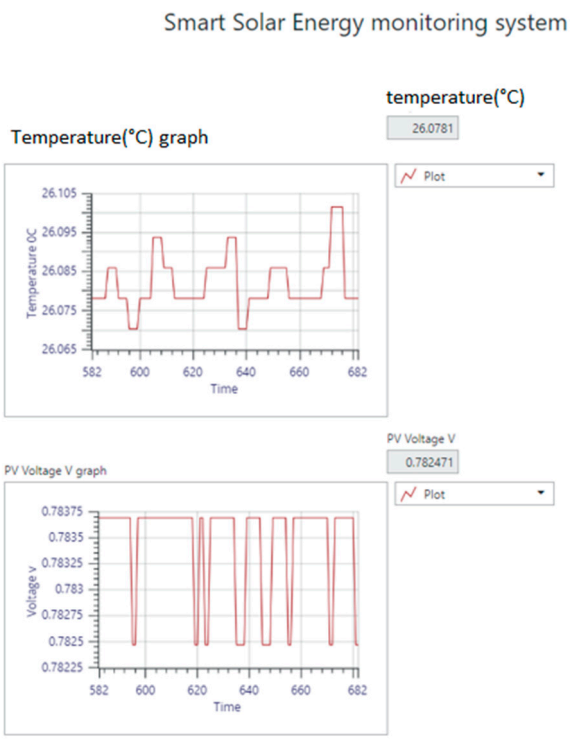

Figure 13. Solar system monitoring dashboard in the cloud.

Furthermore, NI (National Instruments) has integrated HTTPS security, which securely allows the system to be accessed from any computer browser or phone. This implementation reduces the cost for us to install it on our server. This solution enables effortless and protected entry to the dashboard, guaranteeing that users may safely monitor the solar system's performance on different devices. The SystemLink Cloud platform offers significant

benefits in terms of accessibility and flexibility. Users may view the dashboard securely at any time and from any location with internet availability. This accessibility allows for ongoing monitoring and analysis, enabling prompt interventions or modifications based on real-time data, regardless of geographical limitations.

NI's SystemLink Cloud offers many additional security benefits that enhance the integrity and safeguarding of data within the platform, extending beyond the implementation of HTTPS [54]. SystemLink Cloud has access control measures, leading to a secure and highly controlled authentication procedure. Administrators are permitted access using National Instruments (NI) credentials obtained from ni.com. This authentication mechanism allows administrators to set user permissions and access levels inside the system. Using delicate controls ensures that unauthorized access to critical data is successfully controlled. SystemLink Cloud allows for establishing URLs with more flexibility to ensure safe user access. Administrators may create a private, shared URL to provide safe login access to the online application. Alternatively, a publicly accessible URL may be made, allowing everyone to access the content. The flexibility in URL generation accommodates a wide range of user circumstances, enabling administrators to customize access methods depending on unique security and use needs. SystemLink Cloud emphasizes data security, both during transmission and at rest. Robust encryption mechanisms protect stored data, which remain protected even on cloud servers. This dual-layered data encryption technique improves security by protecting against possible breaches or unauthorized access to stored data. The dedication to encrypting data at rest demonstrates SystemLink Cloud's security approach, which protects data at all stages of their lifetime.

NI continually monitors SystemLink Cloud for malicious attacks, which has been shown to be resistant in many circumstances. SystemLink Cloud includes built-in protection [54] against cross-site scripting attacks, Denial of Service, and any request on the site that is not verified with the correct API key and formatting is instantly rejected. The following are a few examples of how NI defends against common online security risks. Cross-site scripting (XSS) is the most prevalent sort of attack. XSS happens when an attacker injects malicious code or scripts into a website without modifying or sanitizing the attacker's input. For example, if a forum website does not sanitize user-submitted posts, an attacker may upload malicious code, which executes on all users' browsers when the post is loaded. NI's web technology uses escape strings to sanitize all inputs and displayed data, as is conventional best practice. SQL injection is an attack that occurs when one of a website's inputs is sent straight to a database without first being sanitized. For example, an attacker might add code to the input data to destroy, edit, or access a database without the user's consent. Because NI's web technology employs MongoDB instead of SQL, it is not always susceptible to SQL injection. However, NI continues to sanitize inputs to MongoDB.

Therefore, NI's SystemLink Cloud provides a wide range of security features that extend beyond encryption. These measures include access restrictions, encryption protocols, frequent updates, and strict physical and compliance-based security measures. This collaborative approach guarantees a strong and secure setting for hosting crucial data and applications, instilling users with confidence about safeguarding their information.

5. Conclusions

This study developed a new method to enhance the security of remote monitoring systems for solar energy. The research integrated advanced technologies, including Advanced Encryption Standard (AES), myRIO board, and NI's SystemLink Cloud platform, to enhance data security in smart solar energy monitoring systems. The study leverages LabVIEW programming combined with G Web Development tools to provide efficient data acquisition and communication with cloud services. Subsequently, we carefully implement AES (Advanced Encryption Standard) encryption to guarantee secure data transmission inside solar systems. The study goes beyond solely implementing AES and includes preventative measures such as modeling attack scenarios on the system. In addition, the incorporation of NI's SystemLink Cloud played a crucial role in facilitating remote access.

It provided a user-friendly dashboard, allowing real-time monitoring of essential solar system data. The platform's robust security measures, such as deploying HTTPS and access restrictions, establish it as a reliable and fortified environment for monitoring data remotely. The work is essential because it highlights the collaboration between modern encryption technologies and cloud-based monitoring platforms. It demonstrates a comprehensive method to strengthen security for smart solar energy systems in remote monitoring situations. This study establishes a precedent for implementing sophisticated security measures in IoT-based solar energy systems and remote monitoring, hence raising the requirements for data protection in comparable fields. In the future, we will implement AES encryption on the myRIO FPGA directly. We will prioritize improving security and assessing the encryption performance, timing efficiency, and overall efficacy compared to the current implementation. Moreover, other PV parameters will be integrated into the study.

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

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: We would like to sincerely thank National Instruments for allowing us to use their LabVIEW and SystemLink systems, which have made our experiments possible.

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

References

1. Cotfas, D.T.; Cotfas, P.A. Education for Sustainability through Renewable Energy. In Proceedings of the 17th International Technology, Education and Development Conference, Valencia, Spain, 6–8 March 2023; pp. 7639–7648. [CrossRef]
2. Kumar, C.M.S.; Singh, S.; Gupta, M.K.; Nimdeo, Y.M.; Raushan, R.; Deorankar, A.V.; Kumar, T.M.A.; Rout, P.K.; Chanotiya, C.S.; Pakhale, V.D.; et al. Solar energy: A promising renewable source for meeting energy demand in Indian agriculture applications. *Sustain. Energy Technol. Assess.* **2023**, *55*, 102905. [CrossRef]
3. Pourasl, H.H.; Barenji, R.V.; Khojastehnezhad, V.M. Solar energy status in the world: A comprehensive review. *Energy Rep.* **2023**, *10*, 3474–3493. [CrossRef]
4. Mohammad, A.; Mahjabeen, F. Revolutionizing Solar Energy with AI-Driven Enhancements in Photovoltaic Technology. *BULLET J. Multidisiplin Ilmu.* **2023**, *2*, 1174–1187.
5. Zhong, J.; Zhang, W.; Xie, L.; Zhao, O.; Wu, X.; Zeng, X.; Guo, J. Development and challenges of bifacial photovoltaic technology and application in buildings: A review. *Renew. Sustain. Energy Rev.* **2023**, *187*, 113706. [CrossRef]
6. Deshmukh, M.K.G.; Sameeroddin, M.; Abdul, D.; Abdul Sattar, M. Renewable energy in the 21st century: A review. *Mater. Today Proc.* **2023**, *80*, 1756–1759. [CrossRef]
7. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the Energy Sector. *Energies* **2020**, *13*, 494. [CrossRef]
8. Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. *Mob. Netw. Appl.* **2023**, *28*, 296–312. [CrossRef]
9. Mostofa, K.Z.; Islam, M.A. Creation of an Internet of Things (IoT) system for the live and remote monitoring of solar photovoltaic facilities. *Energy Rep.* **2023**, *9*, 422–427. [CrossRef]
10. Hema, N.; Krishnamoorthy, N.; Chavan, S.M.; Kumar, N.M.G.; Sabarimuthu, M.; Boopathi, S. A Study on an Internet of Things (IoT)-Enabled Smart Solar Grid System. In *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT*; IGI Global: Hershey, PN, USA, 2023; pp. 290–308. [CrossRef]
11. 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]
12. Nasserddine, G.; Nassereddine, M.; Arid, A.A.E. Internet of Things Integration in Renewable Energy Systems. In *Handbook of Research on Applications of AI, Digital Twin, and Internet of Things for Sustainable Development*; IGI Global: Hershey, PN, USA, 2023; pp. 159–185. [CrossRef]
13. Hadi, A.A.; Sinha, U.; Faika, T.; Kim, T.; Zeng, J.; Ryu, M.-H. Internet of Things (IoT)-Enabled Solar Micro Inverter Using Blockchain Technology. In Proceedings of the 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 29 September–3 October 2019; pp. 1–5. [CrossRef]

14. 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]
15. An, L.; Yang, G.-H. Enhancement of opacity for distributed state estimation in cyber–physical systems. *Automatica* **2022**, *136*, 110087. [CrossRef]
16. Muhammad Salman Bukhari, S.; Kumayl Raza Moosavi, S.; Hamza Zafar, M.; Mansoor, M.; Mohyuddin, H.; Sajid Ullah, S.; Alroobaea, R.; Sanfilippo, F. Federated transfer learning with orchard-optimized Conv-SGRU: A novel approach to secure and accurate photovoltaic power forecasting. *Renew. Energy Focus* **2024**, *48*, 100520. [CrossRef]
17. Selent, D. *Advanced Encryption Standard*; U.S. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001.
18. Zhao, X.; Gray, J. Towards a metrics suite for the complexity analysis of LabVIEW systems models. *Sci. Comput. Program.* **2023**, *227*, 102931. [CrossRef]
19. *National Instruments NI myRIO-1900 User Guide and Specifications*; Michigan State University: East Lansing, MI, USA, 2013. Available online: https://www.egr.msu.edu/classes/me451/me451_labs/robot/myRIO/NI%20myRIO-1900%20User%20Guide%20and%20Specifications.pdf (accessed on 4 January 2024).
20. Connecting to SystemLink Cloud—NI. Available online: https://www.ni.com/docs (accessed on 11 January 2024).
21. Münch, J.-P.; Schneider, T.; Yalame, H. VASA: Vector AES Instructions for Security Applications. In Proceedings of the ACSAC '21: Proceedings of the 37th Annual Computer Security Applications Conference, Virtual Event, 6–10 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 131–145. [CrossRef]
22. Zografopoulos, I.; Hatziargyriou, N.D.; Konstantinou, C. Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations. *IEEE Syst. J.* **2023**, *17*, 6695–6709. [CrossRef]
23. Aghmadi, A.; Hussein, H.; Polara, K.H.; Mohammed, O. A Comprehensive Review of Architecture, Communication, and Cybersecurity in Networked Microgrid Systems. *Inventions* **2023**, *8*, 84. [CrossRef]
24. Jamil, N.; Qassim, Q.S.; Bohani, F.A.; Mansor, M.; Ramachandaramurthy, V.K. Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. *Appl. Sci.* **2021**, *11*, 9812. [CrossRef]
25. Ma, Y.; Qiu, J.; Sun, X.; Tao, Y. A Novel Cryptography-based Architecture to Achieve Secure Energy Trading in Microgrid. *IEEE Trans. Smart Grid* **2023**, 1. [CrossRef]
26. An, Q.; Dong, C.; Li, J.; Jiang, F. A Secure and Efficient Renewable Energy Sharing Framework for Distributed Prosumers. In Proceedings of the 2023 IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT), Male, Maldives, 11–12 March 2023; pp. 1–5. [CrossRef]
27. Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. *J. Appl. Eng. Technol. Sci. (JAETS)* **2020**, *1*, 113–123. Available online: https://journal.yrpipku.com/index.php/jaets/article/view/78 (accessed on 11 January 2024).
28. Prasanna Rani, D.D.; Suresh, D.; Rao Kapula, P.; Mohammad Akram, C.H.; Hemalatha, N.; Kumar Soni, P. IoT based smart solar energy monitoring systems. *Mater. Today Proc.* **2023**, *80*, 3540–3545. [CrossRef]
29. Sanap, S.; More, V. An Ultra-High Throughput and Efficient Implementation of Advanced Encryption Standard. *Int. J. Electr. Electron. Eng. Telecommun.* **2023**, *12*, 46–52. [CrossRef]
30. Alemami, Y.; Mohamed, M.A.; Atiewi, S. Advanced approach for encryption using advanced encryption standard with chaotic map. *Int. J. Electr. Comput. Eng. IJECE* **2023**, *13*, 1708–1723. [CrossRef]
31. Abdullah, A. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. *Cryptogr. Netw. Secur.* **2017**, *16*, 11.
32. Niraj, K.; Mohan, V.; Adesh, K. Smart Grid Security by Embedding S-Box Advanced Encryption Standard. *Intell. Autom. Soft Comput.* **2022**, *34*, 623–638.
33. Yang, P.; Xiong, N.; Ren, J. Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
34. 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]
35. Gupta, V.; Sharma, M.; Pachauri, R.K.; Babu, K.N.D. A Low-Cost Real-Time IOT Enabled Data Acquisition System for Monitoring of PV System. *Energy Sources Part Recovery Util. Environ. Eff.* **2021**, *43*, 2529–2543. [CrossRef]
36. Noor-A-Rahim, M.; Khyam, M.O.; Mahmud, M.A.; Huque, M.T.I.u.; Li, X.; Pesch, D.; Oo, A.M.T. Robust and Real-Time State Estimation of Unstable Microgrids Over IoT Networks. *IEEE Syst. J.* **2021**, *15*, 2176–2185. [CrossRef]
37. Cali, U.; Kuzlu, M.; Pipattanasomporn, M.; Elma, O.; Reddi, R. Cybersecurity of Renewable Energy Data and Applications Using Distributed Ledger Technology. *arXiv* **2021**, arXiv:2110.11354.
38. Hussain, I.; Samara, G.; Ullah, I.; Khan, N. Encryption for End-User Privacy: A Cyber-Secure Smart Energy Management System. In Proceedings of the 2021 22nd International Arab Conference on Information Technology (ACIT), Muscat, Oman, 21–23 December 2021; pp. 1–6. [CrossRef]
39. IoT-Enabled Smart Solar Energy Management System for Enhancing Smart Grid Power Quality and Reliability | SN Computer Science. Available online: https://link.springer.com/article/10.1007/s42979-023-02298-8 (accessed on 3 February 2024).
40. myRIO-1950 Getting Started Guide and Specifications—NI. Available online: https://www.ni.com/docs/en-US/bundle/myrio-1950-getting-started/resource/376099b.pdf (accessed on 11 January 2024).
41. SystemLink Cloud | Getting Started. Available online: https://www.systemlinkcloud.com/gettingstarted (accessed on 11 January 2024).

42. What Is G Web Development Software? Available online: https://www.ni.com/en/shop/electronic-test-instrumentation/programming-environments-for-electronic-test-and-instrumentation/what-is-g-web-development-software.html (accessed on 11 January 2024).
43. Kaur, J.; Lamba, S.; Saini, P. Advanced Encryption Standard: Attacks and Current Research Trends. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022; pp. 112–116. [CrossRef]
44. Advanced Encryption Standard Crypto Toolkit Download. Available online: https://www.ni.com/en/support/downloads/tools-network/download.advanced-encryption-standard-crypto-toolkit.html (accessed on 11 January 2024).
45. Kim, K.; Choi, S.; Kwon, H.; Liu, Z.; Seo, H. FACE–LIGHT: Fast AES–CTR Mode Encryption for Low-End Microcontrollers. In Proceedings of the Information Security and Cryptology—ICISC 2019, Seoul, Republic of Korea, 4–6 December 2019; Seo, J.H., Ed.; Lecture Notes in Computer Science. Springer International Publishing: Cham, Switzerland, 2020; pp. 102–114. [CrossRef]
46. Panahi, P.; Bayılmış, C.; Çavuşoğlu, U.; Kaçar, S. Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications. *Arab. J. Sci. Eng.* **2021**, *46*, 4015–4037. [CrossRef]
47. Hung, C.-W.; Hsu, W.-T. Power Consumption and Calculation Requirement Analysis of AES for WSN IoT. *Sensors* **2018**, *18*, 1675. [CrossRef] [PubMed]
48. TMP116 Data Sheet, Product Information and Support. Available online: https://www.ti.com/product/TMP116 (accessed on 11 January 2024).
49. Dawoud, D.S.; Dawoud, P. 1 Inter-integrated Circuits (IIC/I2C). In *Microcontroller and Smart Home Networks*; River Publishers: Ljubljana, Slovenia, 2020; pp. 1–54. Available online: https://ieeexplore.ieee.org/abstract/document/9227675 (accessed on 11 January 2024).
50. LabVIEW Download. Available online: https://www.ni.com/en/support/downloads/software-products/download.labview.html (accessed on 11 January 2024).
51. Kumar, N.M.; Chopra, S.S.; de Oliveira, A.K.V.; Ahmed, H.; Vaezi, S.; Madukanya, U.E.; Castañón, J.M. Chapter 3—Solar PV module technologies. In *Photovoltaic Solar Energy Conversion*; Gorjian, S., Shukla, A., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 51–78. [CrossRef]
52. "The World's Most Popular Network Protocol Analyzer," Wireshark. Available online: https://www.wireshark.org/ (accessed on 12 January 2024).
53. Molisch, A.F. *Wireless Communications*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
54. Security in NI Web Technology. Available online: https://www.ni.com/en/support/security/security-in-ni-web-technology.html (accessed on 15 January 2024).