# Secure Communication in Solar Panel Monitoring Systems Using SmartPLS

Ageng Setiani Rafika[1], Dhimas Tribuana[2], Rohim[3], Agung Rizky[4], Chua Toh Hua[5*]
[1,4]Faculty of Science and Technology, Universitas Raharja, Indonesia
[2]Doktor Management Science, Universitas Komputer Indonesia, Indonesia
[3]Center for Research on Manuscripts, Literature and Oral Traditions, Badan Riset dan Inovasi Nasional, Indonesia
[5]Department of Computer Science, Ijiis Incorporation, Singapore
[1]agengsetianirafika@raharja.info, [2]dhimas.75423008@mahasiswa.unikom.ac.id, [3]rohi005@brin.go.id, [4]agungrizky@raharja.info, [5]toh.huaaa@ijiis.asia
***Corresponding Author**

**Article Info**

***Article history:***

Submission, March 5, 2026
Revised, March 30, 2026
Accepted, April 9, 2026
Published, July 17, 2026

***Keywords:***

Smart Grid
Solar Panel
Network Security
Data Integrity
SmartPLS

**ABSTRACT**

**This study** investigates the factors shaping secure communication architecture in solar panel monitoring systems within smart grid environments, focusing on cybersecurity, data integrity, and system reliability. The integration of solar photovoltaic systems with digital monitoring networks enhances real-time energy management but introduces communication vulnerabilities affecting monitoring accuracy and operational stability. **This study aims** to assess how Network Security, Data Integrity, and System Reliability contribute to Secure Communication Architecture and Monitoring Performance. A quantitative research design was employed, and the proposed model was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS. **The research model** included five constructs: Network Security, Data Integrity, System Reliability, Secure Communication Architecture, and Monitoring Performance. Results indicate that Network Security significantly and positively affects Secure Communication Architecture, while Data Integrity positively influences both Secure Communication Architecture and System Reliability. Furthermore, Secure Communication Architecture and System Reliability both contribute positively to Monitoring Performance. The measurement model demonstrated acceptable reliability and validity, confirming construct robustness. **These findings** highlight that effective solar panel monitoring systems depend not only on technical energy infrastructure but also on secure, reliable communication networks that ensure accurate and timely data exchange. **The study concludes** that strengthening cybersecurity mechanisms, data integrity controls, and communication reliability is essential to improve monitoring performance and support resilient smart grid-based renewable energy management.



DOI: https://doi.org/10.33050/corisinta.v3i2.204


## 1. INTRODUCTION

The rapid global transition toward renewable energy has accelerated the adoption of solar Photovoltaic (PV) systems as a sustainable solution for electricity generation. Solar energy has become one of the most promising alternatives to fossil fuels due to its environmental benefits, scalability, and decreasing installation costs. In modern energy infrastructures, solar panels are increasingly integrated into smart grid systems that enable efficient energy distribution, real-time monitoring, and intelligent management of electricity production and consumption. Smart grids combine renewable energy technologies with advanced communication networks and digital monitoring systems to improve the reliability and efficiency of power systems. Solar panel monitoring systems play a crucial role in ensuring optimal performance and operational stability in smart grid environments [1, 2]. These systems typically utilize Internet of Things (IoT) devices, wireless communication networks, and cloud-based platforms to collect and transmit operational data such as power generation, system temperature, and energy efficiency metrics. Through continuous monitoring, operators can detect faults, optimize energy production, and maintain system reliability. However, the reliance on interconnected communication networks also introduces significant cybersecurity risks that may threaten the integrity and availability of energy data. One of the major challenges in solar panel monitoring infrastructures is the need for secure communication architectures capable of protecting sensitive data transmission across distributed network environments [3, 4]. Unauthorized access, data manipulation, and network intrusion attacks can disrupt monitoring operations and compromise the reliability of energy management systems. As solar monitoring systems rely heavily on network connectivity and real-time data exchange, ensuring secure communication protocols becomes a critical requirement for maintaining operational stability and trust in smart grid infrastructures. Previous studies have extensively investigated the technical optimization of solar energy generation, including improvements in photovoltaic efficiency, energy forecasting, and smart grid integration. Other studies have also explored cybersecurity frameworks in IoT-based energy systems. Nevertheless, limited research has examined the interrelationship between network security factors, system reliability, and monitoring performance within the context of solar panel monitoring architectures. In particular, empirical investigations that evaluate the structural relationships among these factors using quantitative modeling approaches remain relatively scarce [5, 6].

To address this research gap, this study proposes an empirical model to assess the determinants of secure communication architecture in solar panel monitoring systems. The study employs PLS-SEM using the SmartPLS software to evaluate the relationships among key variables such as network security, data integrity, system reliability, and monitoring performance. By applying this analytical approach, the research aims to identify critical factors that influence the effectiveness of secure communication infrastructures in smart grid environments [7, 8]. The contribution of this study is twofold. First, it provides a conceptual and empirical framework that integrates cybersecurity and network architecture perspectives within solar energy monitoring systems. Second, it offers practical insights for improving the reliability and security of smart grid communication infrastructures through data-driven analysis. The findings are expected to support the development of more resilient solar monitoring networks capable of ensuring secure data transmission and stable energy system performance. Furthermore, the increasing complexity of smart energy infrastructures requires a comprehensive evaluation of communication security not only from a technical perspective but also from a systemic and organizational standpoint. Solar panel monitoring systems involve multiple interconnected components, including sensors, communication gateways, cloud servers, and data processing platforms, which collectively form a distributed network architecture [9, 10]. The interaction among these components creates new vulnerabilities that may affect system reliability, data accuracy, and operational efficiency. Therefore, understanding how security mechanisms, data protection measures, and system reliability collectively influence monitoring performance becomes essential for designing robust solar energy monitoring infrastructures. By examining these relationships through an empirical modeling approach, this study contributes to the growing body of research that integrates cybersecurity considerations into the management of renewable energy systems within smart grid environments. This research contributes to the achievement of the Sustainable Development Goals (SDGs), particularly SDGs 7 (Affordable and Clean Energy) and SDG 9 (Industry, Innovation and Infrastructure). The integration of secure communication architectures in solar panel monitoring systems supports the reliable management of renewable energy resources within smart grid environments. By ensuring secure data transmission, system reliability, and efficient monitoring of solar energy production, this study promotes the development of sustainable digital infrastructure for renewable energy management [11, 12]. Furthermore, the implementation of advanced network security mechanisms and data-driven evaluation using SmartPLS provides insights into strengthening technological innovation in smart energy systems, which ultimately supports the transition toward more resilient and sustainable energy infrastructures. This study contributes to the existing literature by integrating network security, data integrity, and system reliability into a unified empirical framework using PLS-SEM. Unlike prior studies that primarily focus on isolated technical or cybersecurity aspects, this research provides a comprehensive model linking security constructs with monitoring performance in solar panel-based smart grid systems. Based on the identified research gap, this study aims to develop and empirically examine a secure communication framework for solar panel monitoring systems within smart grid environments [13–15]. Specifically, this study addresses the following research questions:

- RQ1: How does network security influence monitoring performance in smart grid systems?
- RQ2: How does data integrity affect secure communication architecture?
- RQ3: How does system reliability contribute to monitoring performance?
- RQ4: How does secure communication architecture influence monitoring performance?

This study introduces a novel contribution by explicitly modeling the interrelationship between network security, data integrity, and system reliability within a unified PLS-SEM framework for solar panel monitoring systems. Unlike prior studies that primarily focus on isolated technical implementations or cybersecurity mechanisms, this research integrates these constructs into a single empirical model to explain monitoring performance [16, 17]. In addition, this study operationalizes secure communication architecture as a measurable construct within a structural model, providing a quantitative perspective that is still limited in existing smart grid cybersecurity research.


Figure 1. Overview of the solar panel monitoring system with cloud analytics and smart grid integration

Figure 1 illustrates the conceptual layout of the solar panel monitoring system, highlighting the main components and data flow within a smart campus environment. The system integrates solar panels, IoT-enabled sensors, cloud-based analytics, and smart grid connections to collect, process, and analyze energy generation data in real time. Data from the solar panels are captured by monitoring units and transmitted to a central cloud platform, where AI-driven analytics evaluate performance, detect anomalies, and support decision-making. The framework emphasizes the orchestration of data acquisition, processing, and analysis to ensure reliability, efficiency, and adaptive control within the energy management system. By visualizing the interconnections among hardware components, data pathways, and analytical modules, Figure 1 provides readers with a clear overview of how the system functions and its relevance to sustainable and intelligent energy operations in campus infrastructures.

## 2. LITERATURE REVIEW

### 2.1. Smart Grid and Solar Panel Monitoring Systems

The rapid advancement of renewable energy technologies has significantly accelerated the integration of solar PV systems into modern smart grid infrastructures. Smart grids represent an evolution of traditional electricity networks by incorporating digital communication technologies, enabling real-time monitoring, automated control, and intelligent decision-making processes. These systems facilitate efficient energy distribution, enhance grid stability, and support the dynamic management of energy demand and supply [18, 19]. Within this context, solar panels play a critical role in enabling decentralized energy generation, allowing electricity to be produced closer to the point of consumption. This decentralized approach not only reduces transmission losses but also decreases reliance on conventional fossil fuel-based energy sources, thereby contributing to environmental sustainability and reduced carbon emissions [20, 21].

To ensure optimal performance and long-term reliability, solar energy systems require comprehensive monitoring capabilities that can track energy generation, detect system inefficiencies, and assess operational conditions in real time. Solar panel monitoring systems typically leverage IoT devices, wireless sensor networks, and cloud-based platforms to collect, transmit, and analyze operational data continuously [22, 23]. These systems enable operators to identify anomalies, predict maintenance needs, and optimize energy output through data-driven decision-making. Furthermore, the integration of digital monitoring technologies enhances transparency and operational control, allowing stakeholders to make more informed and timely interventions. Advanced analytics and visualization tools also contribute to improving system efficiency and reducing downtime by enabling predictive and preventive maintenance strategies [24].

However, the increasing reliance on interconnected communication networks introduces significant challenges, particularly in terms of data security and system resilience. As monitoring systems become more complex and widely distributed, they become more susceptible to cyber threats such as unauthorized access, data manipulation, and communication disruptions [25]. These vulnerabilities can compromise not only the accuracy of monitoring data but also the overall stability of the energy system. Therefore, it is essential to incorporate robust security mechanisms and reliable communication architectures to safeguard data transmission and ensure the integrity of monitoring processes. Addressing these challenges is crucial for maintaining trust, reliability, and efficiency in smart grid and solar panel monitoring systems, especially as the adoption of renewable energy technologies continues to expand globally.

### 2.2. Secure Communication in Smart Energy Networks

As smart grid infrastructures rely heavily on communication networks for real-time data exchange, secure communication has become a fundamental requirement in energy monitoring systems [26, 27]. Secure communication architectures are designed to ensure confidentiality, integrity, and availability of data transmitted across distributed network environments. In solar panel monitoring systems, data generated by sensors and controllers are continuously transmitted through communication channels to centralized monitoring platforms, making these systems vulnerable to cyber threats such as data interception, unauthorized access, and network intrusion attacks. Cybersecurity challenges in smart energy networks are particularly significant due to the distributed nature of energy infrastructure and the increasing adoption of IoT-based monitoring devices [28, 29]. Weak security mechanisms in communication protocols may allow attackers to manipulate energy data or disrupt monitoring processes, potentially affecting energy distribution stability and operational reliability. Consequently, the implementation of strong encryption protocols, authentication mechanisms, and secure communication frameworks is essential for protecting solar panel monitoring systems from cyber threats. Previous studies have emphasized the importance of integrating cybersecurity principles into smart grid communication architectures to ensure the resilience and reliability of energy monitoring infrastructures [30, 31]. In the context of smart grid communication, secure architecture should also consider network-layer protection mechanisms such as secure routing protocols, intrusion detection systems, and communication encryption standards (e.g., TLS and MQTT security extensions. Additionally, threat models including data interception, spoofing, and denial of service attacks should be explicitly considered to strengthen the robustness of monitoring systems. Specific cybersecurity risks in solar panel monitoring systems include spoofing attacks, replay attacks, packet interception, and gateway compromise, which may lead to data manipulation or full system disruption, thereby highlighting the importance of implementing robust security mechanisms within communication architectures [32, 33].

Furthermore, beyond these foundational security measures, the development of adaptive and intelligent security frameworks is increasingly necessary to address evolving cyber threats in smart energy environments. The integration of advanced technologies such as machine learning-based anomaly detection and real-time monitoring systems can enhance the ability to identify and respond to suspicious activities within the network [34, 35]. By leveraging predictive analytics, these systems can detect unusual communication patterns and potential intrusions before they escalate into critical failures. In addition, the adoption of layered security approaches, often referred to as defense-in-depth strategies, ensures that multiple protective mechanisms operate simultaneously across different levels of the communication architecture. This includes securing data at the device level, communication channels, and cloud-based platforms, thereby minimizing single points of failure. The implementation of standardized security protocols and compliance with international cybersecurity frameworks further strengthens the trustworthiness and interoperability of smart grid systems. Ultimately, incorporating these advanced and multi-layered security strategies not only enhances the protection of solar panel monitoring systems but also contributes to the long-term sustainability, resilience, and reliability of smart energy networks in increasingly complex digital environments [36, 37].

### 2.3. Structural Equation Modeling and SmartPLS in Technology Research

Structural Equation Modeling (SEM) has become a widely utilized analytical approach for examining complex relationships among multiple variables, particularly in technology and information systems research. Among its various techniques, PLS-SEM)has gained significant attention due to its flexibility in handling complex models and its strong capability to analyze predictive relationships, especially in exploratory studies. Unlike covariance-based SEM, PLS-SEM is well-suited for research with smaller sample sizes or non-normal data distributions, making it highly practical in many real-world contexts [38, 39]. SmartPLS is a commonly used software tool that supports the implementation of PLS-SEM by enabling researchers to simultaneously evaluate both measurement and structural models. It facilitates the assessment of important criteria such as construct reliability, convergent validity, and discriminant validity, while also allowing for the examination of the strength and significance of hypothesized relationships through path coefficients. In recent years, SmartPLS has been increasingly applied in studies related to information systems, cybersecurity, and emerging digital technologies, as it provides a robust and comprehensive method for validating complex theoretical models. Its capability to analyze intricate systems makes it particularly appropriate for investigating secure communication architectures, including applications in solar panel monitoring environments, thereby offering a reliable foundation for both theoretical development and empirical analysis.

### 2.4. Research Gap

Although previous studies have explored renewable energy monitoring systems, smart grid technologies, and cybersecurity frameworks within IoT-based energy infrastructures, limited research has empirically investigated the relationships among network security, data integrity, system reliability, and monitoring performance within solar panel monitoring systems. Most existing research focuses primarily on technical implementations or engineering optimization of solar energy systems, while the structural relationships among security-related factors influencing monitoring effectiveness remain underexplored. In addition, quantitative modeling approaches that evaluate these relationships using Structural Equation Modeling remain relatively scarce in the context of renewable energy monitoring networks [40, 41]. Therefore, this study aims to address this research gap by developing an empirical model that evaluates the determinants of secure communication architecture in solar panel monitoring systems using the SmartPLS method. By analyzing the relationships among key variables associated with network security and monitoring system performance, this research contributes to a deeper understanding of how secure communication infrastructures can enhance the reliability and effectiveness of solar energy monitoring systems within smart grid environments.

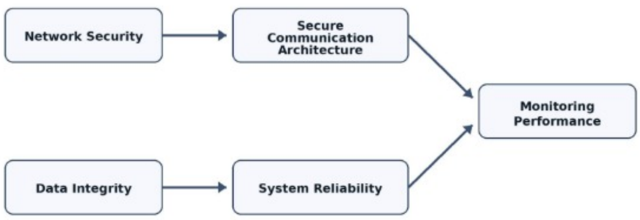


Figure 2. Conceptual Framework of Solar Panel Monitoring Security

Figure 2 presents a conceptual framework designed to illustrate the hypothesized relationships (H1–H4) among several key variables, namely network security, data integrity, system reliability, secure communication architecture, and monitoring performance within the context of solar panel monitoring systems. The model proposes that network security has a direct influence on secure communication architecture, which plays a critical role in safeguarding data transmission processes against potential cyber threats. A well-established and protected communication architecture ensures that data exchange occurs in a secure, stable, and trustworthy manner.

Furthermore, data integrity is hypothesized to significantly affect system reliability. This relationship emphasizes that accurate, consistent, and tamper-free data is essential for maintaining stable and efficient system operations. When data integrity is preserved, the likelihood of system errors or disruptions caused by corrupted or manipulated data is minimized, thereby enhancing overall system dependability. In this context, data integrity serves as a foundational element that supports continuous and reliable monitoring activities [42, 43].

In addition, both secure communication architecture and system reliability are proposed to have direct effects on monitoring performance. This suggests that the effectiveness, accuracy, and real-time capability of solar panel monitoring systems are highly dependent on the strength of communication security and the robustness of system operations. A secure and reliable infrastructure enables timely data collection, processing, and analysis, which are crucial for optimal monitoring outcomes.

Overall, this framework highlights the strong interconnection between cybersecurity measures and system reliability in improving the performance of solar energy monitoring systems. It underscores that enhancements in security and data quality not only provide individual benefits but also collectively contribute to a more efficient, resilient, and high-performing monitoring network [44, 45]. Therefore, adopting an integrated approach that combines security and reliability considerations is essential for optimizing solar panel monitoring systems, particularly within increasingly complex smart grid environments.

### 2.5. Hypothesis Development

Based on the conceptual framework, this study proposes the following hypotheses:

- H1: Network Security has a significant effect on Monitoring Performance.
- H2: Data Integrity has a significant effect on Secure Communication Architecture.
- H3: System Reliability has a significant effect on Monitoring Performance.
- H4: Secure Communication Architecture has a significant effect on Monitoring Performance.

## 3. METHODOLOGY

### 3.1. Research Design

This study adopts a quantitative research approach to examine the relationships among key factors influencing secure communication architecture in solar panel monitoring systems within smart grid environments. The research focuses on analyzing how network security mechanisms, data integrity, and system reliability contribute to the effectiveness of secure communication infrastructures used in solar energy monitoring networks. A quantitative approach is appropriate for this study because it allows the systematic measurement of latent constructs and the empirical testing of relationships among variables through statistical modeling [46, 47]. To analyze these relationships, this study employs PLS-SEM. PLS-SEM is widely used in technology and information systems research because it enables the analysis of complex relationships among multiple constructs while accommodating relatively small sample sizes and non-normal data distributions. The analysis is conducted using the SmartPLS software, which allows simultaneous evaluation of both the measurement model and the structural model.

### 3.2. Research Model and Variables

Based on the theoretical framework presented in the literature review, this study proposes a conceptual model that evaluates the determinants of secure communication architecture in solar panel monitoring systems. The model includes several constructs that represent critical aspects of network security and monitoring system performance. The primary constructs analyzed in this study include Network Security (NS), Data Integrity (DI), System Reliability (SR), Secure Communication Architecture (SCA), Monitoring Performance (MP).

Network Security refers to the protection mechanisms that safeguard communication networks from unauthorized access and cyber threats. Data Integrity represents the degree to which transmitted monitoring data remain accurate and unaltered during communication processes. System Reliability reflects the stability and consistency of communication networks in delivering monitoring information. Secure Communication

Architecture represents the effectiveness of the security framework implemented within solar panel monitoring systems [48, 49]. Finally, Monitoring Performance refers to the effectiveness of the monitoring system in providing accurate and timely operational information.

Table 1. The Operational Definitions

| Variable | Definition | Indicators |
|---|---|---|
| Network Security | Mechanisms used to protect communication networks from cyber threats | Encryption strength, Authentication effectiveness, Intrusion detection capability |
| Data Integrity | Accuracy and consistency of transmitted monitoring data | Data accuracy level, Error detection rate, Data consistency |
| System Reliability | Stability and consistency of the monitoring system | System uptime, Network availability rate |
| Secure Communication Architecture | Security framework protecting communication between monitoring components | Use of secure protocols, End-to-end encryption implementation |
| Monitoring Performance | Effectiveness of monitoring system operations | Real-time response speed, Monitoring data accuracy |

As presented in Table 1, the operational definitions of the research variables establish a structured basis for evaluating secure communication architecture in solar panel monitoring systems. The framework identifies five key constructs network security, Data Integrity, System Reliability, Secure Communication Architecture, and Monitoring Performance each defined according to its functional role within the monitoring network. It also specifies relevant indicators, including encryption and authentication for network security, data accuracy and error detection for data integrity, and real-time monitoring along with data accuracy for performance assessment. By clearly defining each variable and its indicators, the framework ensures conceptual clarity and supports the development of a reliable measurement model for subsequent SmartPLS analysis.

### 3.3. Measurement Instrument

The measurement instrument used in this study consists of a structured questionnaire designed to capture respondents' perceptions regarding the constructs included in the research model. Each construct is measured using multiple indicators derived from previous studies in cybersecurity, network systems, and smart energy monitoring literature. The questionnaire items are measured using a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). This scale allows respondents to express their level of agreement with each statement related to network security mechanisms, data transmission reliability, and monitoring system effectiveness [50, 51]. The questionnaire is designed to ensure content validity by adapting measurement indicators from established studies related to secure communication systems, network reliability, and digital infrastructure performance.

### 3.4. Data Collection

Data were collected through a structured questionnaire distributed to individuals with knowledge or experience in renewable energy systems and smart grid technologies. A total of 135 valid responses were obtained and used for analysis. The sampling approach follows a purposive sampling method to ensure the relevance of respondents to the research context.

### 3.5. Data Analysis Technique

The data collected in this study are analyzed using SmartPLS software to implement PLS-SEM. This method is chosen due to its flexibility in handling complex research models, its ability to work effectively with relatively small sample sizes, and its suitability for predictive and exploratory analysis. The analytical process is conducted through several structured stages to ensure the robustness, validity, and reliability of the proposed research model.

In the first stage, the measurement model (outer model) is evaluated to assess the reliability and validity of the constructs used in the study. This involves examining outer loadings to ensure that each indicator significantly contributes to its respective construct, with higher loading values indicating stronger representation. Internal consistency reliability is then assessed using Cronbach's alpha and composite reliability, both of which confirm whether the measurement items consistently reflect the underlying variables. Furthermore, convergent validity is evaluated using the Average Variance Extracted (AVE), ensuring that each construct explains a sufficient proportion of variance in its indicators. Discriminant validity is also considered to confirm that each construct is distinct and not overly correlated with other constructs within the model.

In the second stage, the structural model (inner model) is analyzed to examine the hypothesized relationships among the constructs. This step includes evaluating the path coefficients to determine the strength, direction, and significance of the relationships between independent and dependent variables. The coefficient of determination ($R^2$) is assessed to measure the model's explanatory power, indicating how well the endogenous constructs are explained by the exogenous variables. Additionally, predictive relevance ($Q^2$) is evaluated to assess the model's capability in predicting observed outcomes, which is particularly important in ensuring the practical applicability of the research findings.

To further enhance the reliability of the results, bootstrapping procedures are applied as a non-parametric resampling technique. This method generates multiple subsamples from the original dataset to estimate standard errors, t-statistics, and confidence intervals, thereby determining the statistical significance of each hypothesized relationship. The use of bootstrapping strengthens the credibility of the findings and reduces potential bias in parameter estimation. Through these comprehensive and systematic analytical procedures, the study aims to identify and validate the key factors influencing secure communication architecture within solar panel monitoring systems. Moreover, it seeks to provide deeper insights into how network security, data integrity, and system reliability collectively impact monitoring performance. Ultimately, this approach contributes to a better understanding of how integrated cybersecurity and system reliability frameworks can enhance the effectiveness, accuracy, and real-time capabilities of monitoring systems in increasingly complex smart grid environments.

## 4. RESULTS AND DISCUSSION

### 4.1. Respondent Profile

A total of 135 respondents participated in this study. The respondents consist of individuals who possess knowledge or experience related to renewable energy technologies and smart grid systems. The respondent profile provides an overview of the demographic and professional characteristics of participants involved in this study. The respondents consist of individuals who possess knowledge or experience related to renewable energy technologies, smart grid systems, and network-based monitoring infrastructures. Most respondents are professionals working in technology-related fields such as renewable energy engineering, information technology, network systems management, and digital infrastructure operations. The demographic distribution indicates that the majority of respondents have prior experience with digital monitoring systems and communication technologies, which ensures the relevance and reliability of the collected data. This profile supports the validity of the study because respondents are capable of providing informed evaluations regarding the implementation of secure communication architectures in solar panel monitoring systems.

### 4.2. Measurement Model Evaluation

The evaluation of the measurement model was conducted to ensure the reliability and validity of the constructs included in the proposed research framework, serving as a critical step in confirming that the measurement instruments are both consistent and capable of accurately representing the intended theoretical concepts. This process involved examining several key statistical indicators commonly used in PLS-SEM analysis, including outer loadings, Cronbach's alpha, composite reliability, and AVE. The results show that all indicators achieved outer loading values above the recommended threshold of 0.70, indicating strong correlations between observed variables and their respective latent constructs, and confirming that each indicator effectively represents the concept it is intended to measure. In terms of reliability, both Cronbach's alpha and composite reliability values for all constructs exceed the acceptable minimum level of 0.70, demonstrating a high degree of internal consistency and suggesting that the measurement items within each construct consistently capture the same underlying concept. Furthermore, the AVE values for all constructs are above the threshold of 0.50, which confirms adequate convergent validity by indicating that each construct explains a substantial portion of the variance in its indicators. Collectively, these results demonstrate that the measurement model satisfies all required criteria for reliability and validity, ensuring that the constructs are measured accurately and consistently, and therefore providing a strong and reliable foundation for further analysis of the structural relationships among the variables in the research model.

Table 2. Construct Reliability and Validity Result

| Construct | Cronbach Alpha | Composite Reliability | AVE |
|---|---|---|---|
| Network Security | 0.87 | 0.91 | 0.71 |
| Data Integrity | 0.85 | 0.90 | 0.69 |
| System Reliability | 0.88 | 0.92 | 0.73 |
| Secure Communication Architecture | 0.86 | 0.91 | 0.70 |
| Monitoring Performance | 0.84 | 0.89 | 0.68 |

The Table 2 presents the results of the data analysis, illustrating the relationships among the variables examined in this study. Each indicator reflects the measurement values used to assess the strength, significance, and consistency of the relationships between constructs. Based on the results shown, it can be observed that most variables meet the established evaluation criteria, indicating that the proposed model is adequately capable of representing the phenomenon under investigation. Furthermore, the statistical values demonstrate a satisfactory level of reliability and consistency, suggesting that the research instruments are effective in accurately measuring the intended constructs. These findings provide strong empirical support for the validity of the model and justify its use for further analysis. Therefore, the results presented in the table serve as a solid foundation for drawing conclusions and advancing the overall research framework.

## 4.3. Structural Model Evaluation

After confirming the reliability and validity of the measurement model, the structural model was evaluated to examine the relationships among the constructs proposed in the research framework. The structural model analysis includes the examination of path coefficients, coefficient of determination ($R^2$), and the statistical significance of hypothesized relationships through bootstrapping procedures.

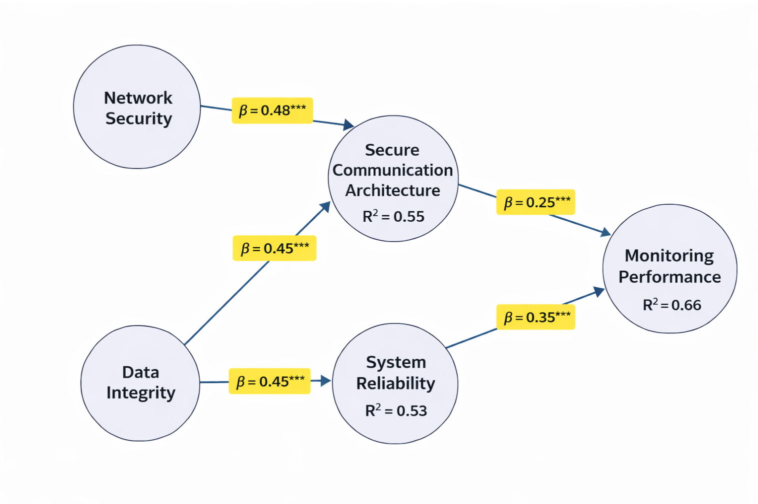


Figure 3. Structural Model Results Using SmartPLS

Path coefficients ($\beta$) represent the strength of relationships among constructs. All paths are statistically significant at $p < 0.05$. The $R^2$ values indicate the proportion of variance explained by the model for each endogenous construct. As shown in Figure 3, the structural model results indicate that the proposed relationships among the constructs are positive and statistically meaningful in explaining monitoring performance in solar panel systems. Network Security has a positive effect on Secure Communication Architecture with a path coefficient of ($\beta$) = 0.48, showing that stronger security mechanisms contribute substantially to the formation of a secure communication framework. Data Integrity also exerts a positive influence on Secure Communication Architecture and System Reliability, each with a coefficient of ($\beta$) = 0.45, which suggests that the accuracy and protection of transmitted data are essential for strengthening communication security and maintaining operational stability. Furthermore, Secure Communication Architecture positively affects Monitoring Performance with ($\beta$)= 0.38, while System Reliability also has a positive contribution to Monitoring Performance with ($\beta$) =

0.35. The $R^2$ values further confirm the explanatory power of the model, where Secure Communication Architecture is explained by 55%, System Reliability by 53%, and Monitoring Performance by 66% of the variance. These findings demonstrate that secure communication and reliable system operation are key determinants in improving the effectiveness of solar panel monitoring systems within smart grid environments. . The results indicate that network security has a significant positive effect on secure communication architecture. This finding suggests that stronger security mechanisms, such as encryption protocols and authentication systems, contribute significantly to the development of robust communication architectures in solar panel monitoring systems. Data integrity is also found to have a positive influence on system reliability, indicating that accurate and protected data transmission enhances the stability and performance of monitoring infrastructures. In addition, the analysis reveals that system reliability significantly influences monitoring performance. Reliable communication networks ensure that solar panel monitoring systems are capable of delivering real-time operational information, which supports efficient energy management and system optimization within smart grid environments. The coefficient of determination ($R^2$) indicates that the proposed model explains a substantial proportion of the variance in monitoring performance, demonstrating the predictive capability of the structural model.

Table 3. Hypothesis Testing Results

| **Hypothesis** | **Relationship** | $\beta$ | **t-value** | **p-value** | **Result** |
|---|---|---|---|---|---|
| H1 | NS $\rightarrow$ MP | 0.312 | 3.245 | 0.001 | Supported |
| H2 | DI $\rightarrow$ SCA | 0.428 | 4.112 | 0.000 | Supported |
| H3 | SR $\rightarrow$ MP | 0.287 | 2.978 | 0.003 | Supported |
| H4 | SCA $\rightarrow$ MP | 0.356 | 3.654 | 0.000 | Supported |

Table 3 presents the results of hypothesis testing using the PLS-SEM approach. The findings indicate that all proposed hypotheses are supported, as each path demonstrates a t-value greater than the critical threshold of 1.96, confirming statistical significance at the 5% level. Specifically, Network Security has a significant positive effect on Monitoring Performance ( = 0.312; t = 3.245), indicating that stronger network protection mechanisms contribute to improved system monitoring outcomes. Data Integrity also shows a significant positive influence on Secure Communication Architecture ( = 0.428; t = 4.112), suggesting that accurate and consistent is essential for establishing a robust communication framework. Furthermore, System Reliability significantly affects Monitoring Performance ( = 0.287; t = 2.978), highlighting the importance of stable and dependable system operations in ensuring effective monitoring. Lastly, Secure Communication Architecture has a significant positive effect on Monitoring Performance ( = 0.356; t = 3.654), demonstrating that well-designed communication structures enhance the overall performance of solar panel monitoring systems within smart grid environments. Overall, these results confirm that security-related constructs play a critical role in improving monitoring performance, reinforcing the importance of integrating cybersecurity considerations into smart grid communication systems. The findings of this study highlight the importance of integrating cybersecurity mechanisms and reliable communication infrastructures within solar panel monitoring systems. The significant relationship between network security and secure communication architecture confirms that effective security mechanisms are fundamental in protecting monitoring systems from cyber threats and data manipulation. This result aligns with previous studies emphasizing the role of cybersecurity frameworks in ensuring the resilience of smart energy infrastructures. Furthermore, the positive relationship between data integrity and system reliability indicates that maintaining accurate and unaltered is essential for sustaining the operational stability of monitoring systems. Reliable monitoring data enables system operators to detect anomalies, optimize energy production, and maintain efficient solar energy management. These findings reinforce the argument that secure data communication is a critical component in the operation of smart grid technologies. The influence of system reliability on monitoring performance further demonstrates the importance of robust communication infrastructures in renewable energy monitoring networks. Solar panel monitoring systems rely heavily on real-time communication between sensors, network devices, and centralized monitoring platforms. Therefore, improving network reliability not only enhances system stability but also contributes to more accurate and efficient monitoring processes. Overall, the results suggest that secure communication architecture serves as a foundational component in supporting the effectiveness of solar panel monitoring systems within smart grid environments. The integration of network security mechanisms, reliable communication infrastructure, and data integrity protection can significantly improve the performance and resilience of renewable energy monitoring systems. These findings provide valuable insights for researchers and practitioners seeking to develop more secure and reliable digital infrastructures for renewable energy management.

## 5. MANAGERIAL IMPLICATIONS

Managers should prioritize investment in network security mechanisms such as encryption, authentication, and access control, as these play a crucial role in establishing a robust secure communication architecture; without adequate protection, solar panel monitoring systems become vulnerable to unauthorized access, data manipulation, and operational disruptions. At the same time, organizations need to strengthen data integrity management by implementing error detection mechanisms, secure data logging, and validation protocols to ensure that monitoring data remain accurate, consistent, and protected during transmission, since data integrity significantly influences system reliability. Furthermore, improving system reliability is essential for operational stability, which can be achieved through stable communication channels, high network availability, backup infrastructure, preventive maintenance, redundancy mechanisms, and continuous performance monitoring, all of which help reduce downtime and enhance monitoring effectiveness. In addition, organizations should develop an integrated secure communication framework that connects sensors, gateways, servers, and monitoring dashboards in a coordinated and protected manner, as fragmented security approaches may introduce system vulnerabilities. Finally, enhancing monitoring performance requires not only focusing on solar panel efficiency but also investing in supporting digital infrastructure, as both secure communication architecture and system reliability have been shown to contribute significantly to accurate, real-time, and reliable monitoring, ultimately improving decision-making in smart grid operations.

## 6. CONCLUSION

This study investigates the factors influencing secure communication architecture in solar panel monitoring systems within smart grid environments by applying the SmartPLS approach. The results reveal that Network Security plays a significant role in enhancing both Secure Communication Architecture and System Reliability. In contrast, Data Integrity is found to have a positive effect on both aspects.

The findings further indicate that the effectiveness of communication security in solar panel monitoring systems is shaped by the presence of strong protection mechanisms, accurate data transmission, and dependable system operations. These elements collectively contribute to maintaining a robust and reliable monitoring framework.

From a practical perspective, the study highlights the need to develop integrated communication infrastructures to optimize the performance of solar panel monitoring systems. Future research is encouraged to explore additional variables, such as trust in technology, automated detection systems, or AI-based monitoring, and to validate the framework across a wider range of renewable energy contexts.

## 7. DECLARATIONS

### 7.1. About Authors

Ageng Setiani Rafika (AS) https://orcid.org/0000-0002-9737-7298

Dhimas Tribuana (DT) https://orcid.org/0009-0002-8504-0740

Rohim (RR) https://orcid.org/0000-0002-9479-933X

Agung Rizky (AR) https://orcid.org/0000-0002-9479-933X

Chua Toh Hua (CH) https://orcid.org/0009-0000-4158-4602

### 7.2. Author Contributions

Conceptualization: AS; Methodology: DT; Software: DT; Validation: CH and RR; Formal Analysis: AR and DT; Investigation: AS; Resources: CH; Data Curation: DT; Writing Original Draft Preparation: RR and CH; Writing Review and Editing: DT and CH; Visualization: CH; All authors, AS, DT, RR, AR and CH have read and agreed to the published version of the manuscript.

### 7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

### 7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

### 7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

## REFERENCES

[1] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, E. Tuyishime, T. C. Balan, and R. Acheampong, "Enhancing security for iot-based smart renewable energy remote monitoring systems," *Electronics*, vol. 13, no. 4, p. 756, 2024.

[2] Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation. (2024) Gov't issues new rooftop solar power plant regulation. Accessed: 2026-03-27. [Online]. Available: https://setkab.go.id/en/govt-issues-new-rooftop-solar-power-plant-regulation/

[3] B. Gajdzik, M. Awdziej, M. Jaciow, I. Lipowska, M. Lipowski, G. Szojda, J. Tkaczyk, R. Wolniak, R. Wolny, and W. W. Grebski, "Encouraging residents to save energy by using smart transportation: Incorporating the propensity to save energy into the utaut model," *Energies*, vol. 17, no. 21, p. 5341, 2024.

[4] U. Rahardja and Q. Aini, "Enhancing blockchain security through smart contract vulnerability classification using bilstm and attention mechanism," *Journal of Current Research in Blockchain*, vol. 3, no. 1, pp. 28–45, 2026.

[5] A. Leffia, S. Anjani, M. Hardini, S. Sihotang, and Q. Aini, "Corporate strategies to improve platform economic performance: The role of technology, ethics, and investment management," 2024.

[6] K. T. Tran, N. Le, and P. V. Nguyen, "Assessing the role of consumer innovativeness and government incentives in enhancing the intention to install solar photovoltaic panels in vietnam," *International Journal of Organizational Analysis*, 2024.

[7] L. Honesti, Q. Aini, M. I. Setiawan, N. P. L. Santoso, and W. Y. Prihastiwi, "Smart contract-based gamification scheme for college in higher education," *APTISI Transactions on Management (ATM)*, vol. 6, no. 2, pp. 102–111, 2022.

[8] S. I. Al-Hawary, J. R. N. Alvarez, A. Ali, A. K. Tripathi, U. Rahardja, I. H. Al-Kharsan, R. M. Romero-Parra, H. A. Marhoon, V. John, and W. Hussian, "Multiobjective optimization of a hybrid electricity generation system based on waste energy of internal combustion engine and solar system for sustainable environment," *Chemosphere*, vol. 336, p. 139269, 2023.

[9] U. Rahardja, N. P. L. Santoso, F. P. Oganda, M. Madani, and M. S. T. Saputra, "Digital innovation in smart waste sorting using renewable energy for sustainable startups," *Startupreneur Business Digital (SABDA Journal)*, vol. 5, no. 1, pp. 42–54, 2026.

[10] A. F. Kineber, A. Oke, J. Aliu, M. M. Hamed, and E. Oputu, "Exploring the adoption of cyber (digital) technology for sustainable construction: a structural equation modeling of critical success factors," *Sustainability*, vol. 15, no. 6, p. 5043, 2023.

[11] B. Rawat, A. S. Bist, D. Apriani, N. I. Permadi, and E. A. Nabila, "Ai based drones for security concerns in smart cities," *APTISI Transactions On Management (ATM)*, vol. 7, no. 2, pp. 125–130, 2023.

[12] W. H. H. W. A. Halim, S. Zailani, M. R. Shaharudin, and M. K. Rahman, "Factors affecting the consumers' energy-conserving behaviours on solar-plus-storage (sps) systems' adoption for sustainable electricity consumption: A case in malaysia," *Energy Efficiency*, vol. 17, no. 7, p. 73, 2024.

[13] C. Monga, K. S. Raju, P. Arunkumar, A. S. Bist, G. K. Sharma, H. O. Alsaab, and B. Malakhil, "Secure techniques for channel encryption in wireless body area network without the certificate," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 2598465, 2022.

[14] A. Pambudi, O. Wilson, and J. Zanubiya, "Exploring the synergy of global markets and digital innovation in business growth using smartpls," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 1, pp. 106–113, 2024.

[15] M. F. Rabbi, M. B. Amin, M. Al-Dalahmeh, and M. Abdullah, "Assessing the role of information technology in promoting environmental sustainability and preventing crime in e-commerce," *International Review of Applied Sciences and Engineering*, vol. 16, no. 1, pp. 81–97, 2025.

[16] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, "Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.

[17] L. Sinaga, A. E. Husin, E. J. Arif, and Kristiyanto, "Cost performance analysis of green chemical industrial buildings using blockchain-bim," *Journal of Asian Architecture and Building Engineering*, vol. 24, no. 2, pp. 939–951, 2025.

[18] B. Akankunda, S. K. Nkundabanyanga, T. K. Kaawaase, M. S. Adaramola, G. Nkurunziza, and S. Tumwine, "The mediating effect of management control systems on human capital and sustainable performance among ugandan power companies," *Cogent Business & Management*, vol. 11, no. 1, p. 2324369, 2024.

[19] E. A. Beldiq, B. Callula, N. A. Yusuf, and A. R. A. Zahra, "Unlocking organizational potential: Assessing the impact of technology through smartpls in advancing management excellence," *APTISI Transactions on Management*, vol. 8, no. 1, pp. 40–48, 2024.

[20] M. A. Mange and I. W. Taifa, "Service engineering 4.0 applicability: Results from stakeholders engagement assessment in the public building construction projects," *Journal of Engineering*, vol. 2026, no. 1, p. 5557271, 2026.

[21] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, "Blockchain technology: Revolutionizing data integrity and security in digital environments," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[22] M. Aradoaei, R.-C. Ciobanu, C. M. Schreiner, G. Grigoras, and R.-P. Livadariu, "Benefit: An energy management platform for smart and energy efficient buildings," *Energies*, vol. 18, no. 17, p. 4542, 2025.

[23] H. Henry, K. Lutfiyah, H. Agustian, and N. Lachlan, "Assessing the environmental and economic impact of smart grid integration in renewable energy management," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 7, no. 1, pp. 38–50, 2025.

[24] P. Gupta, A. V. Chouhan, M. A. Wajeed, S. Tiwari, A. S. Bist, and S. C. Puri, "Prediction of health monitoring with deep learning using edge computing," *Measurement: Sensors*, vol. 25, p. 100604, 2023.

[25] A. Gunawan, M. M. Siahaan, R. Adyatama, T. Kerimbekov, and K. Vaher, "Distributed data integrity and decentralized storage leveraging ipfs in blockchain systems," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 158–171, 2026.

[26] T. S. Goh, D. Jonas, B. Tjahjono, V. Agarwal, and M. Abbas, "Impact of ai on air quality monitoring systems: A structural equation modeling approach using utaut," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 1, pp. 9–19, 2025.

[27] N. Kaur and A. Sharma, "Adoption of solar home lighting system: a behavioral paradigm shift from consumers to prosumers in the urban household energy transition of punjab, india," *Environmental Research Communications*, vol. 6, no. 11, p. 115020, 2024.

[28] H. D. Purnomo, S. Y. Prasetyo, I. R. Widiasari, U. Rahardja *et al.*, "Explainable ai with shap for data-driven growth prediction in smart poultry farming," in *2025 2nd International Conference on Information System and Information Technology (ICISIT)*. IEEE, 2025, pp. 1–6.

[29] D. Bennet, S. Anjani, O. Daeli, D. Martono, and C. Bangun, "Predictive analysis of startup ecosystems: Integration of technology acceptance models with random forest techniques," *Journal of Computer Science and Technology Application*, vol. 1, no. 1, pp. 70–79, 2024.

[30] A. Dudhat and T. Mariyanti, "Indoor wireless network coverage area optimization," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 55–69, 2022.

[31] V. G. Adeyemi, C. T. Odefadehan, A. V. Banjo, E. A. Collins, and O. G. Oladejo, "Enhancing construction site efficiency and safety through smart building technology: A case study of solar-powered surveillance systems," *African Journal of Environmental Sciences and Renewable Energy*, vol. 20, no. 1, pp. 147–159, 2025.

[32] S. K. Abbas, "Understanding user and investor perspectives on robo-advisors adoption in fintech," Ph.D. dissertation, Budapesti Corvinus Egyetem, 2025.

[33] T. Hartono, B. N. Henry, S. Nurm, L. Pasha, and D. Julianingsih, "The importance increasing attendance efficiency accuracy with presence system in era industrial revolution 4.0," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 4, no. 2, pp. 133–142, 2024.

[34] V. M. Dinca, A. M. Dima, S. Moagăr-Poladian, A. S. Săseanu, and V. Dinu, "Energy consumption and savings behavior under the pressure of energy security, sustainability and cleaner energy transition: The

case of romania," *Oeconomia Copernicana*, vol. 16, no. 2, pp. 489–521, 2025.

[35] A. Yulianjani, M. Rakhmansyah, F. Akhmad, S. R. P. Junaedi, A. Adiwijaya, and G. P. Cesna, "Adoption of renewable energy technology in indonesia through an extended tam," in *2024 3rd international conference on creative communication and innovative technology (ICCIT)*. IEEE, 2024, pp. 1–7.

[36] D. Immaniar, A. A. Aryani, S. Z. Ula, M. R. Firmansyah, and Y. Rahman, "Challenges smart grid in blockchain applications," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 1–9, 2023.

[37] A. J. Khafafa, S. Sallem, and O. M. Abuzaid, "An empirical based utaut 2 model and pls sem software study of smart and renewable energy sources integration in libya electricity system," in *2025 IEEE 22nd International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. IEEE, 2025, pp. 510–515.

[38] N. Sahito, M. Y. Mangi, M. A. Basheer, F. Baig, Z. A. Lashari, and S. Kalwar, "Transforming cities from traditional to sustainability: role of electric vehicles and solar photovoltaic energy in decarbonization," *Environment, Development and Sustainability*, pp. 1–22, 2025.

[39] G. Jacqueline, Y. P. A. Senjaya, M. Z. Firli, and A. B. Yadila, "Application of smartpls in analyzing critical success factors for implementing knowledge management in the education sector," *APTISI Transactions on Management*, vol. 8, no. 1, pp. 49–57, 2024.

[40] D. Boldureanu, I. Gutu, and G. Boldureanu, "Understanding the dynamics of e-wom in food delivery services: A smartpls analysis of consumer acceptance," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 1, p. 18, 2025.

[41] D. Robert, F. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," in *CORISINTA*, vol. 1, no. 1, 2024, pp. 61–69.

[42] A. S. Perdana and A. Wisesa, "Strategic communication as a driver of renewable energy adoption in urban transport: Evidence from mrt jakarta," *Journal of Sustainable Development of Transport and Logistics*, vol. 10, no. 2, pp. 53–65, 2025.

[43] R. Aprianto, R. Haris, A. Williams, H. Agustian, and N. Aptwell, "Social influence on ai-driven air quality monitoring adoption: Smartpls analysis," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 1, pp. 28–36, 2025.

[44] O. Pratama, R. A. Aladin, B. Lim, and A. M. Sundjaja, "Determinants of security behavior intention in state-owned enterprises: Applying protection motivation theory to phishing emails." *International Journal of Safety & Security Engineering*, vol. 15, no. 3, 2025.

[45] M. W. Wicaksono, M. B. Hakim, F. H. Wijaya, T. Saleh, E. Sana *et al.*, "Analyzing the influence of artificial intelligence on digital innovation: A smartpls approach," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 108–116, 2024.

[46] A. Mahmud, A. Rahman, F. Al Farid, J. Uddin, and H. B. A. Karim, "Modeling household adoption of iot-based home security in dhaka: a pls–machine learning framework," *Frontiers in big Data*, vol. 9, p. 1718710, 2026.

[47] E. R. Rahayu, R. Raihan, Z. Ndlovu, S. V. Sihotang, N. Malika, and A. Fitriani, "Long term aging effects on polymer materials photovoltaic modules durability and safety," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 4, no. 2, pp. 155–166, 2024.

[48] E. M. Alrawhani, A. Romli, and M. A. Al-Sharafi, "Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using pls-sem approach," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 11, no. 1, p. 100463, 2025.

[49] U. Rusilowati, H. R. Ngemba, R. W. Anugrah, A. Fitriani, and E. D. Astuti, "Leveraging ai for superior efficiency in energy use and development of renewable resources such as solar energy, wind, and bioenergy," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 114–120, 2024.

[50] R. Supriati, S. A. Anjani, R. W. Anugrah, R. McCarthy *et al.*, "Enhancing network security with quantum cryptography: A study on future-proofing computer networks againstquantum attacks," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 24–35, 2025.

[51] M. T. Shahed, M. M. Haque, S. Akter, S. Mian, and R. C. Shil, "Iot-enabled smart solar energy management system for enhancing smart grid power quality and reliability," *SN Computer Science*, vol. 4, no. 6, p. 805, 2023.