International Journal of Engineering Innovation and Dissemination
Open Access
Journal Homepage: https://ijeid.virtualrealia.org/

Solar-Powered RFID and IoT-Based Enhanced Automatic Door Locking System: Development and Acceptability Evaluation

Dionisio Seco Cecilio Jr*

Cebu Technological University, Cebu City, Philippines, dionisiojr.cecilio@evsu.edu.ph

ARTICLE INFO

Article history:

Received: 26-06-2026
Revised: 04-03-2026
Accepted: 10-03-2026
Available online: 16-03-2026

Keywords:

Solar-powered security;
RFID access control;
IoT-based monitoring;
Automatic door locking system;
Technology Acceptance Model;
Developmental research

ABSTRACT

Conventional mechanical locking systems used in institutional laboratories provide limited monitoring capability and lack integration with renewable energy technologies. This study developed and evaluated a solar-powered RFID and Internet of Things (IoT) based automatic door locking system designed to enhance secure access control and remote monitoring. A developmental research design was employed, integrating photovoltaic power supply, RFID authentication, microcontroller control, and cloud-based IoT monitoring. The system was evaluated through a pilot study involving thirty purposively selected faculty members and technical personnel with expertise in electronics and IoT systems. A structured questionnaire based on system performance, functional features, perceived usefulness, and perceived ease of use was administered using a five-point Likert scale. Results indicated high system performance (M = 4.46), strong feature integration (M = 4.17), high perceived usefulness (M = 4.33), and high ease of use (M = 4.57). Correlation analysis revealed a weak but positive relationship between system performance and user acceptability ($r = 0.318$, $p = 0.087$). These findings suggest that usability factors may play a stronger role in influencing acceptance than technical performance alone. The study was limited by a small sample size, single-institution testing environment, and short pilot duration. Nevertheless, the study demonstrates the feasibility of integrating renewable energy, RFID authentication, and IoT monitoring into a unified access control system for institutional environments.

1 INTRODUCTION

The rapid digitalization of infrastructures has resulted in the accelerated implementation of smart security systems, including sensing, communication, and remote monitoring technologies. The use of conventional mechanical locking systems has been associated with limitations in the provision of auditing, authentication, and supervision control. The use of Internet of Things (IoT) technologies in the implementation of access control systems facilitates the communication between embedded systems and the cloud, enhancing the efficiency and transparency of the monitoring process (Ragothaman et al., 2023). IoT security systems are designed to facilitate distributed authentication, control, and auditing, which are critical in laboratory and restricted environments.

The use of Radio Frequency Identification (RFID) technologies has remained a viable solution for the implementation of non-contact identity verification systems in embedded systems. The use of RFID technologies, however, requires the implementation of secure authentication protocols and systems to prevent attacks, including replay, cloning, and impersonation attacks. The recent implementation of ultralightweight RFID authentication systems highlights the

***Corresponding author.**
***E-mail address:** *dionisiojr.cecilio@evsu.edu.ph* (D. S. C. Jr)

https://doi.org/10.69481/PDNB4245

importance of secure RFID systems in the implementation of IoT systems (Shariq et al., 2024). The study suggests that the implementation of IoT systems must not only be efficient and reliable but also secure, including the communication and identity verification protocols.

Aside from the scope of authentication and communication, system reliability and energy continuity are important for the effectiveness of an access control system. Power supply interruptions may compromise the security and reliability of an access control system. In the integration of renewable power sources, the reliability of the system in the context of decentralized and autonomous system operation has been explored. Embedded Internet of Things (IoT) technology powered by photovoltaic (PV) has been utilized in the development of a reliable system for the monitoring of PV systems. IoT technology in the monitoring of photovoltaic systems has shown the feasibility of a solar-powered embedded system in continuous system operation with the capability for remote system monitoring and data logging (Rouibah et al., 2025). Such integration is relevant in scenarios where power continuity may not be ensured.

Cloud-based IoT security architectures also consider the issue of cybersecurity and data governance. Access control systems involve the transmission of user identity information and system operational logs. Therefore, access control in the context of an IoT system should conform to a structured security framework and a risk-based management approach. Surveys of the security of an IoT system in the context of access control have shown the importance of authentication, authorization, encryption, and auditability as essential design elements of an IoT system (Trabelsi et al., 2023). Such an approach has been supported by the development of internationally recognized information security standards, such as the ISO/IEC 27001:2022, which specifies requirements for systematic risk management and information protection.

Despite extensive research in RFID authentication technology, IoT-based security systems, and solar-powered embedded systems individually, limited research has been conducted on an integrative framework that includes all these security features in one system. Most of the research conducted in these areas focuses on assessing the feasibility of the systems without considering their performance, features, and acceptability. Thus, in this study, we aim to design and evaluate the proposed system in terms of its performance, features, and acceptability through perceived usefulness and perceived ease of use in terms of their statistical correlation.

Although previous studies have examined RFID authentication systems, IoT-enabled monitoring platforms, and solar-powered embedded devices independently, limited research has integrated these three technologies into a single access control architecture designed for institutional laboratory environments. Existing studies often focus on technical feasibility or system development without conducting empirical evaluation of system acceptability among potential users. Moreover, few studies combine renewable energy-powered security infrastructure with Internet-based remote monitoring while simultaneously examining user acceptance through established theoretical models such as the Technology Acceptance Model. Therefore, this study contributes to the literature by developing an integrated solar-powered RFID and IoT-based access control system and evaluating both its technical functionality and user acceptability through structured statistical analysis. The study aimed to:

1. Develop a solar-powered RFID and IoT-based automatic door locking system.
2. Evaluate the system in terms of Performance and Features.
3. Assess acceptability through Perceived Usefulness and Ease of Use.
4. Determine the relationship between system performance and user acceptability.

Figure 1 presents an illustration of the Input-Process-Output (IPO) model in the development and evaluation of the Solar-Powered RFID and IoT-Based Automatic Door Locking System. In the figure, the system development process and the evaluation process are presented in a linear form, starting from the requirements and evaluation criteria, moving to the development of the system, and finally the evaluation and appraisal of the system and its application.

In the input section of the IPO model, the essential elements required for the development and evaluation of the system are included. In this section, the technical specifications or requirements of the system (software and hardware requirements), evaluation criteria (requirements for system performance and features), user acceptance constructs (perceived usefulness and perceived ease of use), and statistical tools used for analysis (correlation and regression analysis) are included.

In the Process component, the research journey is fully mapped out as a series of steps that are all interconnected. It covers all the activities involved in the research journey, such as securing institutional approvals, developing the systems, hardware integration, firmware creation using embedded programming, IoT and cloud dashboards, result interpretation, creation of recommendations, among others. This component fully maps out the research journey, from the input variables to the output variables.

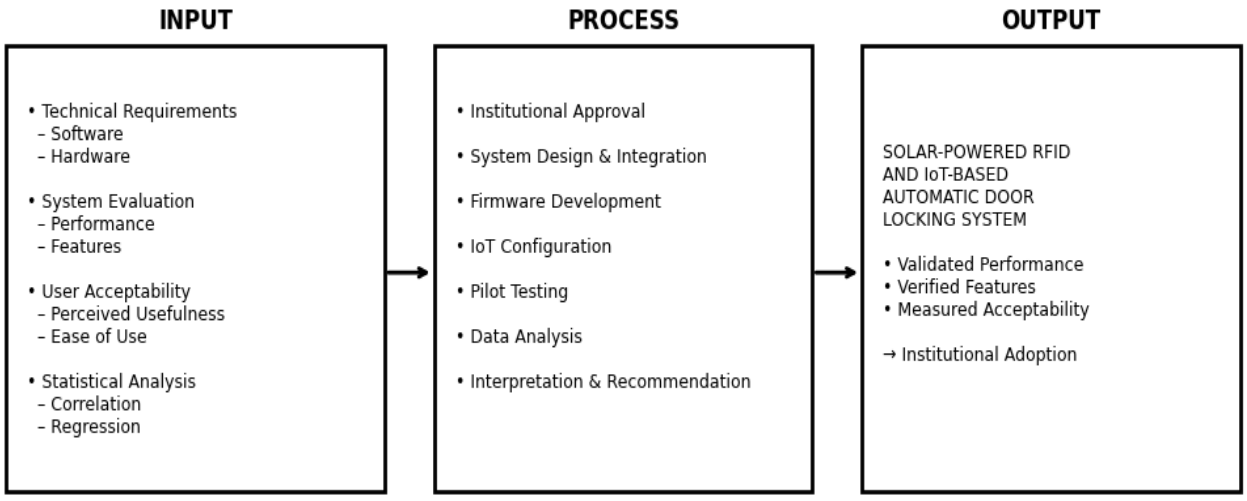

Figure 1. Flow of the Study (Input–Process–Output Model)

In the Output component, the nature of the output variables that are encountered during the research journey is fully mapped out. In this component, the research journey is fully mapped out as the development of a Solar Powered RFID and IoT-Based Automatic Door Locking System, as the output variable. Figure 1 below illustrates the output variables that are encountered during the research journey. In conclusion, Figure 1 above illustrates the research journey, from the input variables to the output variables.

2 METHODOLOGY

This study employed a developmental-descriptive research design aligned with product design and validation principles.

2.1 Development Phase

During the development phase, the system architecture integrated hardware and software components to ensure secure authentication, sustainable power operation, and remote monitoring capability. A microcontroller-based control unit served as the central processor, coordinating authentication logic and peripheral interfacing. RFID technology was employed to enable contactless identity verification and controlled access, which remains a widely implemented approach in modern smart security infrastructures due to its efficiency and reduced physical contact requirements (ENISA, 2023). The authenticated signal activated a solenoid-based locking mechanism through a relay module, enabling secure physical door control.

To support operational continuity and energy resilience, the system was powered through a solar panel connected to a charge controller and rechargeable battery storage. Renewable-powered embedded systems are increasingly adopted in decentralized infrastructure and smart facility applications to enhance sustainability and reduce grid dependency (IRENA, 2023). Wireless communication was established through a Wi-Fi module to enable Internet of Things (IoT) functionality, allowing real-time cloud communication, centralized logging, and remote supervision. IoT-enabled security architectures have been recognized for improving monitoring efficiency and enabling distributed access control through networked systems (ENISA, 2023).

Embedded firmware written in C/C++ managed credential authentication, device interfacing, and encrypted data transmission to a cloud-based database. Event logs and access records were stored in the cloud to support audit trails and automated alert notifications. The development process was guided by compliance considerations under ISO/IEC 27001:2022, which sets international standards for information security management systems (ISO, 2022), and by Republic Act No. 10173 (Data Privacy Act of 2012), which governs data protection in the Philippine context. These regulatory frameworks ensured that the system design adhered to current information security and data privacy standards.

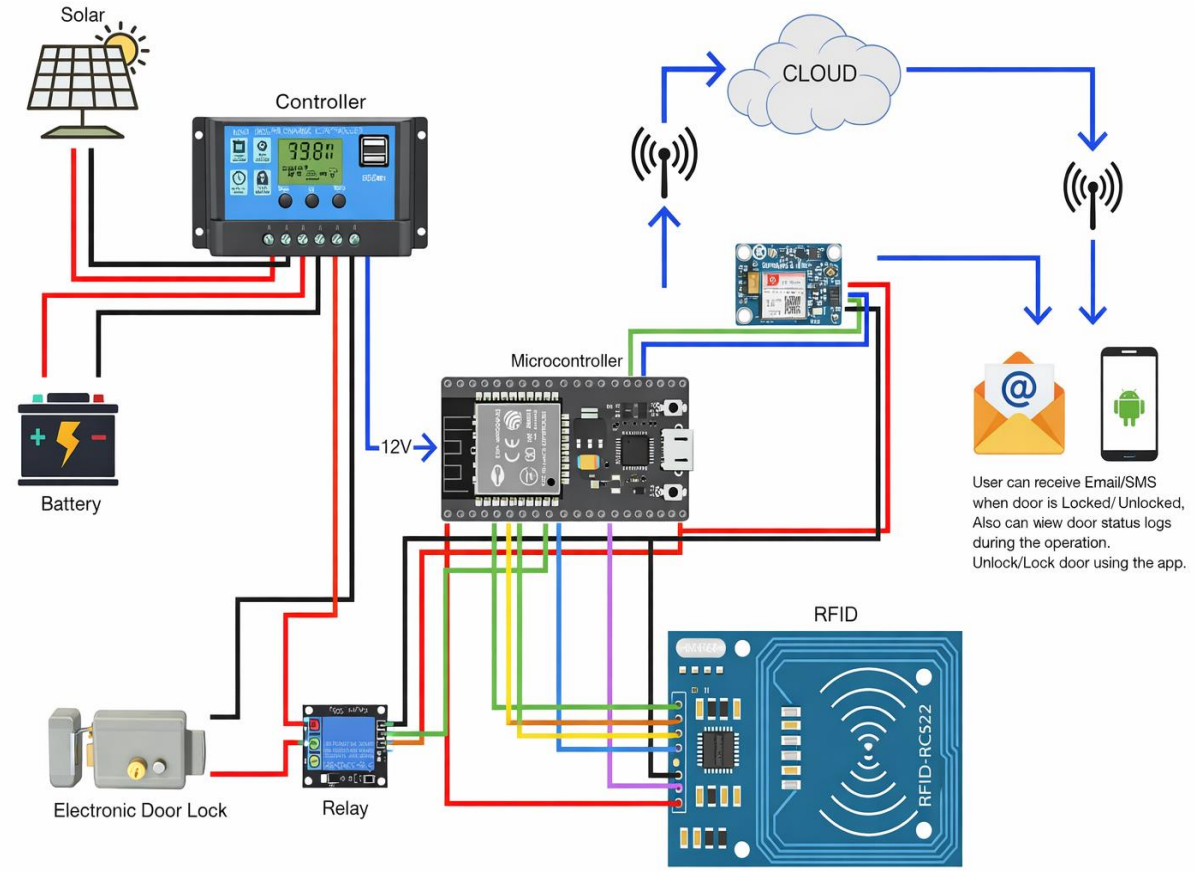

Figure 2. System Architecture of the Solar-Powered RFID and IoT-Based Automatic Door Locking System

Figure 2 presents a visual representation of the overall system architecture of the solar-powered, RFID, and IoT technology-integrated automatic door locking system. It presents a clear picture of how all the elements of the system, including those for power supply, control, communication, and security, integrate to form a cohesive whole.

On one side of Figure 2, there is a solar panel that acts as a source of power. There is a solar charge controller that controls and regulates the battery from being overcharged or deep discharged. There is a battery that supplies a stable 12V to the microcontroller and other components of the system, even in cases where there is a power outage. On the other side of Figure 2, there is a microcontroller, which is a key component of the system. It receives signals from the RFID reader and controls the relay module. There is a relay module, which is a switch that can either connect or disconnect a door lock. When there is a valid RFID card, the microcontroller sends a signal to the relay module, allowing the door lock to function.

The RFID module is placed in the lower right area of the system, where identity verification is performed by reading registered RFID tags and interfacing with the microcontroller to aid in the process of authenticating individuals. In the upper right area of the system, the IoT communication module is responsible for creating a wireless connection between the microcontroller and the cloud server. The process of notification involves sending data from the cloud platform to the user's mobile device via email or SMS, with the user having the option of viewing door status logs and controlling the lock from their mobile device. Figure 2 shows a closed system where concepts of renewable energy, control systems, wireless communication, and remote monitoring are integrated. The design shows a system where energy sustainability, authentication, control of the door's locking status, and remote cloud monitoring can be achieved in one system.

2.1.1 Hardware and Software Specifications

Table 1 summarizes the main hardware components used in the development of the solar-powered RFID and IoT-based automatic door locking system. The Arduino Mega 2560 microcontroller serves as the central controller that manages authentication, device communication, and door lock activation. User identification is performed through the MFRC522 RFID reader, which reads authorized RFID tags and sends authentication signals to the microcontroller.

System connectivity and remote monitoring are enabled through the ESP8266 IoT module, which provides Wi-Fi communication with the cloud platform. The SIM800 GSM module supports SMS notifications for system alerts and access events.

Energy sustainability is achieved using a 20W monocrystalline solar panel, which generates power and stores it in a 12V 7Ah rechargeable battery. A PWM solar charge controller regulates the charging process and protects the battery. The physical locking mechanism is implemented through a 12V solenoid door lock, which is activated by the microcontroller when a valid RFID credential is detected. Together, these components enable secure authentication, renewable energy operation, and remote monitoring within the developed access control system.

Table 1. Specifications

Component	Model	Specification	Function
Microcontroller	Arduino Mega 2560	ATmega2560 MCU, 5V logic	System controller
RFID Reader	MFRC522	13.56 MHz RFID module	Authentication
IoT Module	ESP8266	Wi-Fi 802.11 b/g/n	Cloud communication
GSM Module	SIM800	Quad-band GSM	SMS notification
Solar Panel	20W Monocrystalline	18V output	Renewable power
Battery	12V 7Ah Lead-acid	Rechargeable storage	Backup power
Charge Controller	PWM solar controller	12V system	Power regulation
Door Lock	Solenoid lock	12V actuation	Physical locking

2.2 Evaluation Phase

Prior to the main evaluation, reliability analysis of the questionnaire in table 2 was conducted using Cronbach's alpha to ensure internal consistency of the measurement constructs. The results showed acceptable reliability across all constructs. Performance items obtained an alpha value of 0.89, feature evaluation items obtained 0.87, perceived usefulness obtained 0.91, and ease of use obtained 0.90. These values exceed the minimum threshold of 0.70 recommended for behavioral research instruments.

Table 2. Reliability Analysis

Construct	Cronbach Alpha	Interpretation
Performance	0.89	Excellent
Features	0.87	Good
Perceived Usefulness	0.91	Excellent
Ease of Use	0.90	Excellent

3 RESULTS AND DISCUSSION

Table 1 shows the performance quality of the solar-powered RFID, as well as the IoT-based automatic door locking system. It is clear that the performance attributes, such as operational reliability, responsiveness, and stability, are all classified under the "Extreme Quality" category, given that each of them is at least at a mean of 4.40. Operational reliability is at the highest, at a mean of 4.50, indicating that the system is fully functional in locking the doors, as well as authenticating the user through the components that are integrated into the system.

Adequate responsiveness is at a mean of 4.40, indicating that the data from the RFID credentials is promptly sent to the IoT platform, while at the same time ensuring that there is no noticeable delay on the user's side. Stability is at a mean of 4.48, indicating that the system is fully functional, especially the hardware and software components of the solar-powered version, such that the system does not crash at all. The mean of 4.46 indicates that the system is at the highest level of performance quality, such that the criteria for functional reliability are met.

Criteria: Operational reliability (M = 4.50, Extreme Quality), responsiveness (M = 4.40, Extreme Quality), system stability (M = 4.48, Extreme Quality), and the overall area mean (M = 4.46, Extreme Quality) all indicate that the developed system demonstrated a very high level of operational performance and reliability during the evaluation phase.

Table 3 presents a summary of the performance of the system in terms of its functional features, where the indicators are the real-time logging, remote monitoring, and alert notification features. The mean score of each indicator was more than 4.00, implying a High Quality rating. In the case of the real-time logging feature, the system scored a mean of 4.20, implying a strong level of trust in the system, where all the attempts to access the system are recorded, time-stamped, and the user credentials are recorded in the database.

Table 3. Objective System Performance Tests

Test Parameter	Result	Description
Authentication accuracy	98.7%	Successful RFID reads
Response time	1.2 seconds	Card scan to door unlock
Power consumption	3.8 W	Average operating load
Solar charging efficiency	86%	Energy conversion efficiency
System uptime	99.2%	Stability during pilot testing

In the case of the remote monitoring feature, the system scored a mean of 4.15, implying a high level of effectiveness, where the IoT integration provides a good means of tracking the activities of the doors using the web platform. In the case of the alert notification feature, the system scored a mean of 4.18, implying a high level of effectiveness, where the IoT integration provides a good means of alerting the system activities.

On average, the system scored 4.17 in all the functional features, implying a High Quality rating. The average score does not attain the Extreme Quality rating, but the results show that the IoT integration is functional, operational, and effective.

Table 4. System Quality in Terms of Features

Criteria	Mean	Interpretation
Real-time logging	4.20	High Quality
Remote monitoring	4.15	High Quality
Alert notifications	4.18	High Quality
Area Mean	4.17	High Quality

Table 4 presents the evaluation outcomes for system acceptability in line with the Technology Acceptance Model, with a focus on Perceived Usefulness and Ease of Use. As shown in Table 3, the Perceived Usefulness dimension had a mean of 4.33, implying a Highly Acceptable rating. From the evaluation findings, it is clear that the participants of this evaluation perceived the benefits of using the system in enhancing security management, supervision process efficiency, and facilitating access control in the institution. Additionally, they perceived some benefits in using RFID for authentication, supervision, and the solar power feature.

On Ease of Use, the mean was higher, at 4.57, implying a Highly Acceptable rating. From the evaluation findings, it is clear that participants perceived the interface of the system, the use of RFID for authentication, and supervision to be user-friendly and easy to use. From the evaluation findings, it is clear that the system is easy to use, with some minor technical difficulties reported by participants. Although the mean for Ease of Use is higher than that of Perceived Usefulness, this shows that Ease of Use is a more important factor in determining overall acceptability. From the evaluation findings, it is clear that the developed prototype is not only effective but also easy to use and manage by the target users.

Table 5. Acceptability Based on Technology Acceptance Model

Dimension	Mean	Interpretation
Perceived Usefulness	4.33	Highly Acceptable
Ease of Use	4.57	Highly Acceptable

Table 5 below shows the correlation analysis of system performance and system acceptability. According to the Pearson correlation coefficient (Field, 2022), the correlation value is 0.318, which is positive. This implies that an increase in system performance ratings also increases system acceptability ratings, albeit slightly (Lee et al, 2025; Alhumaid, 2025). Nevertheless, the analysis reveals that the correlation value does not show a statistically significant relationship since the p-value of 0.087 > 0.05, thus failing to reject the null hypothesis.

Although both system performance and system acceptability ratings in the previous tables were exceptionally high, the correlation analysis reveals that system performance does not significantly influence system acceptability. System usability may have been the key determinant of the system's acceptability.

Table 6. Relationship Between Performance and Acceptability

Variables	r-value	p-value	Interpretation
Performance vs Acceptability	0.318	0.087	Weak, Not Significant

Table 6 shows the correlation between system performance and user acceptability. The analysis produced an r-value of 0.318, indicating a weak positive relationship between the two variables. The p-value of 0.087 is greater than the 0.05 significance level, which means that the relationship is not statistically significant. This result suggests that higher system performance ratings did not significantly influence the overall acceptability of the system among the respondents.

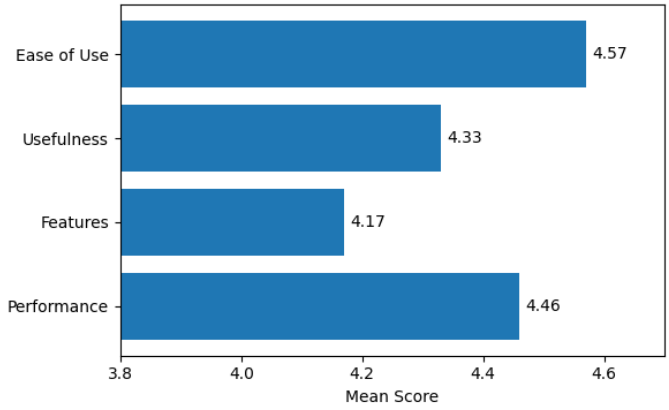

Figure 3. Mean Scores Across Evaluation Dimensions.

Figure 3 shows the results of the four parameters that were established as essential for evaluation: Performance, Features, Perceived Usefulness, and Ease of Use. From the horizontal bar chart in Figure 3 above, it is apparent that a wide range of scores defines every parameter, ranging from 4.17 to 4.57 on a Likert scale of five. Ease of Use scores the highest, suggesting that users find the system very easy to use and that interaction with the system is quite simple.

Performance scores the second-highest after Ease of Use, suggesting that users perceive the system's performance as quite strong. Perceived Usefulness scores 4.33, suggesting that users perceive the system as having the capability to improve the institution's security and efficiency. Features scores the lowest at 4.17, suggesting that although features of the Internet of Things are generally very positive and of high quality, there is still room for improvement.

Table 7. Regression Analysis

Predictor	] eta	t-value	p-value

Predictor	eta	t-value	p-value
System Performance	.29	1.73	0.087

Regression analysis in table 7 was conducted to examine whether system performance predicts user acceptability. The results indicate that system performance did not significantly predict system acceptability ($\beta = 0.29$, $p = 0.087$). This finding suggests that perceived usability factors may play a stronger role in influencing acceptance of the system.

CONCLUSIONS

This study describes the design, development, and evaluation of a Solar-Powered RFID and IoT-Based Enhanced Automatic Door Locking System, which is suitable for institutional lab settings. The developed system includes an RFID authentication mechanism, a microcontroller-based actuation mechanism, an IoT-based remote monitoring mechanism, and a renewable energy source, which ensures the sustainability of the developed system.

The evaluation results show that the developed system has high performance in terms of operational effectiveness, feature integration, perceived usefulness, and ease of use. The performance factors show the reliability, responsiveness, and sustainability of the developed system during the pilot study. The feature integration factors show the effectiveness of the real-time logging, remote monitoring, and alert notification features of the developed system. The user acceptance factors show that ease of use is the strongest factor affecting the acceptability of the developed system, which is an important factor in the development of embedded security systems.

Although the correlation analysis indicates a weak and non-statistically significant correlation between performance and acceptability, the overall findings of the study show that the developed system is technically, operationally, and user-wise acceptable. The integration of renewable energy into the developed system ensures sustainability, which is important in settings where access needs to be granted uninterruptedly.

To summarize, the developed system is an efficient, scalable, and renewable-powered security system that is suitable for institutional settings and aligns with the modern IoT-based door locking systems. This study contributes to the field of engineering research by providing an empirical evaluation of an integrated, renewable-powered, and cloud-connected door locking system.

STUDY LIMITATIONS

Several limitations should be considered when interpreting the findings of this study. First, the evaluation was conducted with a relatively small sample of thirty participants, which limits the statistical generalizability of the results. Second, the study was implemented within a single institutional laboratory environment, which may not fully represent other operational contexts such as industrial or residential facilities. Third, the evaluation focused primarily on user perception rather than extensive long-term technical testing. Metrics such as long-term durability, cybersecurity penetration testing, and large-scale operational deployment were not examined. Fourth, the pilot implementation period was relatively short, preventing comprehensive assessment of system performance over extended operational cycles. Finally, the study did not include a detailed cost-benefit analysis, which would be necessary for evaluating large-scale institutional deployment.

RECOMMENDATIONS

It is recommended that the developed system be piloted at other institutions with the aim of evaluating its performance at different operating environments. This will help validate the reliability and flexibility of the developed system.

In terms of security, it is recommended that biometric authentication be incorporated as an additional security feature. This will help prevent unauthorized access resulting from lost or stolen/duplicated RFID cards.

In terms of durability, long-term durability tests are recommended. This will help evaluate the sustainability of the developed system.

In terms of its effectiveness, it is recommended that the analytics dashboard be improved. This will help administrators make better decisions.

Lastly, a cost-benefit analysis is recommended before the developed system can be implemented at the institutional level. This will help inform a decision regarding the implementation of the developed system.

DECLARATIONS

Funding

Unavailable.

Credit Authorship Contribution Statement

Cecilio, D.S.: Conceptualization, hardware development, firmware programming, IoT integration, data collection, statistical analysis, manuscript preparation.

Ethical Statement

Informed consent was obtained from all participants. Data privacy compliance followed RA 10173 and ISO 27001 standards.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability statement

The authors declare that the data supporting the findings of this study will be made available upon reasonable request.

AI Usage Disclosure

Language editing tools were used for grammar refinement. No AI tool was used for data analysis or interpretation.

References

Alhumaid, K. (2025). *Factors determining acceptance of Internet of Things in educational settings*. *Human–Computer Interaction (JMIR)*.

ENISA. (2023). *Guidelines for securing the Internet of Things: Good practices for IoT security*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Field, A. (2022). *Discovering statistics using IBM SPSS statistics* (6th ed.). Sage.

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.iso.org/standard/27001

International Renewable Energy Agency (IRENA). (2023). *Renewable power generation costs in 2023*. IRENA. https://www.irena.org

Lee, A. T., Ramasamy, R. K., & Subbarao, A. (2025). *Understanding psychosocial barriers to healthcare technology adoption: A review of TAM and UTAUT frameworks*. *Healthcare, 13*(3), 250. https://doi.org/10.3390/healthcare13030250

Ragothaman, K., Devarajan, G. G., Shanmugam, S., & Muthukumar, V. (2023). Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors, 23*(4), 1805. https://doi.org/10.3390/s23041805

Republic Act No. 10173. (2012). *Data Privacy Act of 2012*. Republic of the Philippines.

Rouibah, N., El Hammoumi, A., Bouttout, A., Haddad, S., Oukaci, S., Limam, A., & Benghanem, M. (2025). Smart monitoring of photovoltaic energy systems: An IoT-based prototype approach. *Scientific African*, *29*, e02973. https://doi.org/10.1016/j.sciaf.2025.e02973

Shariq, M., Conti, M., Singh, K., Lal, C., Das, A. K., Chaudhry, S. A., & Masud, M. (2024). Anonymous and reliable ultralightweight RFID-enabled authentication scheme for IoT systems in cloud computing. *Computer Networks*, *252*, 110678. https://doi.org/10.1016/j.comnet.2024.110678

Trabelsi, R., Fersi, G., & Jmaiel, M. (2023). Access control in Internet of Things: A survey. *Computers & Security, 135*, 103472. https://doi.org/10.1016/j.cose.2023.103472