PWD CONNECT: A COMPREHENSIVE ONLINE HUB USING RFID WITH DATA ANALYTICS

Kenneth J. Ababa[1], Jayrold Dave J. Bebit[2], Enrique L. Gonzales[3], Freslee P. Salazar[4], Billy Joe C. Lupera[5]

School of Information and Communication Technology, West Visayas State University-Lambunao Campus, Ladrido Street, Poblacion Ilawod, Lambunao, Iloilo, Philippines

[1]kennethj.ababa@wvsu.edu.ph

[2]jayrolddavej.bebit@wvsu.edu.ph

[3]enriquel.gonzales@wvsu.edu.ph

[2]fresleep.salazar@wvsu.edu.ph

[2]billyjoe.lupera@wvsu.edu.ph

***Abstract*— This study developed PWD Connect: A Comprehensive Online Hub Using RFID with Data Analytics, an integrated digital platform designed to modernize, secure, and streamline services for Persons with Disabilities (PWDs). The system automates the registration and renewal of PWD identification cards, centralizes beneficiary records, and integrates RFID technology for fast, contactless, and reliable identity verification during service transactions. To strengthen fraud prevention, the platform incorporates multi-layered authentication, unique QR–RFID tagging, and an activity log capable of detecting suspicious or duplicate claims. It also features built-in data analytics tools that generate real-time insights on service utilization trends, demographic distributions, and assistance claim patterns to support evidence-based decision-making and efficient resource allocation among partner agencies. Using a descriptive-developmental research design, the system was evaluated by PDAO personnel, store owners, and registered PWD users based on internationally recognized software quality criteria, including functionality, usability, reliability, security, and efficiency. Results indicated an "Excellent" level of acceptability across all criteria, confirming that the system is robust, secure, efficient, and capable of consistently meeting administrative and accessibility needs.**

***Keywords*— RFID Technology, Data Analytics, PWD Services, Identity Verification, Fraud Prevention**

I. INTRODUCTION

Persons with Disabilities (PWDs) continue to experience substantial barriers in accessing essential services and participating fully in society. These barriers arise not only from physical, mental, sensory, or psychosocial impairments but also from systemic and environmental limitations that restrict inclusion. In the Philippines, the Magna Carta for Disabled Persons establishes the legal rights and privileges of PWDs, including access to healthcare services, transportation discounts, education, employment opportunities, and other government-mandated benefits [1]. Despite these statutory protections, challenges remain in the effective delivery and administration of services at the local government level. Many PWDs encounter difficulties in obtaining and renewing their Persons with Disabilities Identification Card (PWD ID), which serves as the primary credential for availing entitled benefits.

The evolving understanding of disability further underscores the need for systemic reform. The World Health Organization introduced the International Classification of Functioning, Disability and Health (ICF), which conceptualizes disability as the interaction between health conditions and contextual factors, including environmental and institutional barriers [2]. This framework highlights that inefficient administrative systems and inaccessible technological infrastructures significantly contribute to participation restrictions. In many local Persons with Disability Affairs Offices (PDAOs), registration and verification processes remain manual and paper-based, requiring applicants to physically visit government offices, complete extensive documentation, and endure prolonged waiting times. These procedures disproportionately disadvantage individuals with mobility impairments, cognitive limitations, and mental health conditions.

Studies have demonstrated that accessibility challenges extend to digital government platforms as well. Abdul Aziz et al. reported that PWDs faced considerable barriers in accessing e-government services due to limited accessibility features and poor system design [3]. Similarly, Furnell, Heikola, and Libods emphasized that many authentication mechanisms lack inclusive design principles, thereby restricting usability for individuals with disabilities [4]. These findings indicate that both traditional and digital systems must incorporate accessibility, security, and user-centered design to ensure equitable access.

Beyond accessibility concerns, the absence of a centralized and secure identification mechanism creates operational inefficiencies. Manual verification processes increase the likelihood of data duplication, fraudulent claims, and misuse of privileges. Fragmented record management systems also hinder effective monitoring of service utilization and demographic trends. As noted by Davenport and Harris, data analytics enables organizations to transform raw data into actionable insights that support evidence-based decision-making [5]. However, limited

integration of analytics tools within local government units restricts their capacity to develop responsive and inclusive policies.

Technological advancements provide opportunities to address these systemic challenges. Radio Frequency Identification (RFID) technology enables secure, contactless, and real-time identification through embedded tags and readers, improving accuracy and efficiency in authentication processes [6]. When combined with multi-layered security mechanisms, RFID-based systems enhance identity verification and reduce vulnerabilities to fraud [7]. Integrating such technologies into a centralized digital platform can significantly modernize PWD registration and benefit management processes.

In response to these identified gaps, this study proposes PWD Connect: A Comprehensive Online Hub Using RFID with Data Analytics, a web-based system designed to streamline PWD registration, authentication, and service monitoring. The platform integrates RFID-enabled identification cards with a centralized database, enabling real-time verification of beneficiaries in partner establishments while minimizing manual paperwork and physical visits. Additionally, the system incorporates prescriptive data analytics to generate demographic summaries, monitor service utilization, and support informed decision-making at the administrative level. The developed system is evaluated using the ISO/IEC 25010:2011 framework, which assesses software quality characteristics such as functional suitability, reliability, usability, security, and maintainability [8].

By combining secure identification technologies, inclusive digital services, and analytics-driven governance, the proposed system aims to enhance accessibility, transparency, and operational efficiency in delivering services to the PWD community. Ultimately, this research contributes to advancing digital transformation in public administration and strengthening inclusive service delivery mechanisms for Persons with Disabilities.

II. Literature Review

A. Legal and Policy Framework for Persons with Disabilities

The protection and promotion of the rights of Persons with Disabilities (PWDs) are grounded in national and international legal frameworks. In the Philippines, the Magna Carta for Disabled Persons mandates equal access to education, employment, healthcare, transportation, and other social services for PWDs [1]. The law emphasizes non-discrimination and the provision of auxiliary services that enhance participation in society. However, while policy frameworks provide legal guarantees, several studies indicate that implementation challenges persist, particularly in local government units where administrative systems remain manual and fragmented.

On a global scale, the World Health Organization introduced the International Classification of Functioning, Disability and Health (ICF), which reframes disability as an interaction between individuals and environmental barriers rather than solely a medical condition [2]. This socio-environmental perspective underscores the importance of accessible systems, inclusive infrastructure, and adaptive technologies. Literature suggests that digital transformation in government services must align with inclusive design principles to address both functional limitations and systemic barriers affecting PWDs.

B. Accessibility in E-Government Systems

E-government initiatives aim to improve efficiency and accessibility of public services; however, accessibility gaps remain a major concern. Abdul Aziz et al. [3] found that many online government platforms lacked user-centered accessibility features, limiting usability for individuals with visual, cognitive, and motor impairments. Their findings highlight the need for compliance with accessibility standards and adaptive interface design.

Similarly, Furnell, Heikola, and Libods [4] emphasized that authentication systems often neglect accessibility considerations. Multi-factor authentication methods, while enhancing security, may unintentionally exclude users with disabilities if not properly designed. These studies demonstrate that digital platforms must balance security requirements with usability and accessibility to ensure equitable access. In the context of PWD service management, the integration of secure yet inclusive authentication mechanisms is therefore critical.

C. RFID Technology in Identification and Verification Systems

Radio Frequency Identification (RFID) technology has been widely utilized in identification, tracking, and authentication systems due to its efficiency and reliability. RFID systems consist of tags and readers that communicate wirelessly to transmit identification data in real time. Pai [5] explains that RFID enables contactless verification, reducing manual intervention and minimizing processing errors.

In public service applications, RFID has been employed in access control, inventory management, and identity verification systems. The literature indicates that RFID-based identification enhances processing speed, accuracy, and security compared to traditional card-based or paper-based systems. Hassan and Shukur [6] further discussed the importance of multi-layered authentication mechanisms integrated with RFID systems to prevent unauthorized access and fraudulent activities. Their research supports the implementation of secure verification protocols in systems handling sensitive personal data, such as those related to PWD beneficiaries.

D. Data Analytics in Public Sector Decision-Making

Data analytics has emerged as a transformative tool in organizational and governmental decision-making. Davenport and Harris [7] argue that analytics enables institutions to convert raw operational data into actionable insights, thereby improving strategic planning and resource allocation. In public administration, analytics tools assist in monitoring service utilization, identifying demographic patterns, and forecasting future needs.

Despite its benefits, many local government offices lack integrated analytics systems, resulting in reactive rather than data-driven governance. Integrating analytics within digital platforms allows administrators to generate reports, visualize trends, and evaluate program effectiveness. In the context of PWD service delivery, analytics can provide insights into the number of registered beneficiaries, frequency of benefit usage, and geographic distribution of services. Such information is essential for evidence-based policymaking and inclusive program development.

E. Software Quality and System Evaluation Standards

Ensuring the reliability and usability of digital systems requires adherence to recognized software quality standards. The ISO/IEC 25010:2011 framework defines quality characteristics including functional suitability, reliability, performance efficiency, usability, security, maintainability, and portability [8]. This model provides a structured basis for evaluating whether a developed system meets user requirements and organizational objectives.

Research indicates that applying standardized evaluation metrics improves system acceptance and long-term sustainability. In systems designed for vulnerable populations such as PWDs, usability and accessibility are particularly critical quality attributes. Evaluating systems under established standards ensures that technological solutions are not only functional but also secure, efficient, and user-friendly.

III. Methodology

A. Research Design

This study employed a descriptive-developmental research design. The developmental aspect focused on the design and implementation of the proposed system, PWD CONNECT: A Comprehensive Online Hub Using RFID with Data Analytics, while the descriptive aspect evaluated the developed system using standardized software quality metrics.

The study aimed to design, develop, and assess the acceptability of the system based on the ISO/IEC 25010 software quality model.

The respondents of the study consisted of selected users who evaluated the developed system. They were composed of Persons with Disabilities (PWDs), system administrators, and IT experts who assessed the system based on the ISO/IEC 25010 software quality characteristics.

Table 1

RESPONDENT OF THE STUDY

Participants	No. of Respondents
Administrator (PDAO Head) and Staff	2
PWD Members	11
Store Owner	2
IT Experts	5
Total	20

B. System Architecture

Fig. 1 illustrates the system architecture of PWD Connect: A Comprehensive Online Hub using RFID with Data Analytics. The system is designed using a structured client–server model that integrates web technologies, RFID authentication, and secure data management to streamline services for Persons with Disabilities (PWDs).

The process begins with the PWD user, who interacts with the system through a web-based interface. The frontend layer is developed using HTML, CSS, JavaScript, and Bootstrap to ensure accessibility and responsive design across devices. This interface allows users to register, update personal information, and monitor benefit usage. When the user performs an action, such as submitting a form or requesting data, the system sends an HTTP request to the server. The server processes the request and returns an appropriate response, which is displayed on the user's screen.

The backend layer contains the core application logic. It runs on a web server that handles business processes such as registration validation, authentication, benefit tracking, and report generation. The backend communicates directly with the MySQL database, where all PWD records, RFID unique identifiers (UIDs), transaction logs, and account details are securely stored. The file system manages static resources such as images and supporting web assets.

For real-time identity verification, the system integrates an RFID authentication mechanism at partner establishments. When a PWD presents their RFID card, the establishment scans it using an RFID reader connected to a microcontroller device. The scanned UID is transmitted to the web server, which checks the database to verify whether the PWD is legitimate and registered. If the UID matches an active account, the system confirms eligibility; otherwise, access is denied. This process ensures fast and secure validation during transactions.

To enhance reliability and data security, the architecture includes a mirror database and scheduled backup system. All critical data are periodically backed up to a secondary backup server and cloud storage (e.g., Google Drive). This redundancy mechanism protects against data loss due to hardware failure, cyber threats, or system crashes.

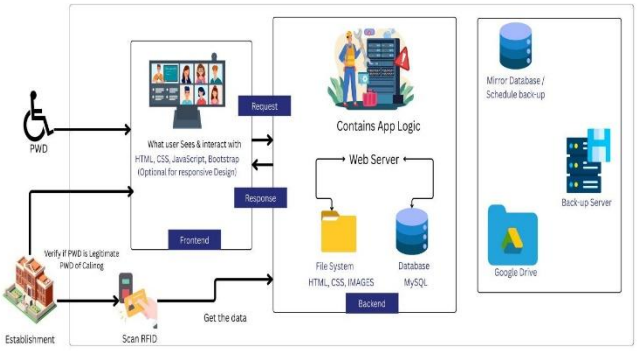

Fig. 1. Illustration of the System Architecture.

C. Algorithms and Processing Logic

The system implemented structured algorithms to ensure efficient and accurate processing of data.

1) Authentication Algorithm: The system provides a secure authentication mechanism that enables registered users to access their respective accounts using a valid username and password. Upon submission of login credentials, the system performs input validation to ensure that all required fields are completed and that the provided data conform to the expected format. This initial validation prevents incomplete or improperly formatted entries from being processed further.

After validation, the submitted credentials are compared against encrypted records stored in the system database. Password verification is conducted using secure hashing techniques to ensure confidentiality and protect sensitive user information from unauthorized access. This approach strengthens system security by preventing the exposure of plaintext passwords.

The system implements Role-Based Access Control (RBAC) with three (3) distinct user roles: Administrator, PWD Member, and Establishment. Each role is assigned predefined permissions and access privileges corresponding to specific system functionalities. For PWD Members, an additional verification step is incorporated to ensure that the account status is marked as active prior to granting access. Accounts that are inactive, pending approval, or suspended are restricted from logging into the system.

As shown in Fig. 2, the Authentication Interface for PWD Users displays a login form requiring the entry of a username and password. The interface is designed to be clear and accessible, promoting usability for persons with disabilities. In cases where invalid credentials are entered or the account status does not meet the required conditions, the system generates an appropriate error message to inform the user.

Similarly, Fig. 3 illustrates the Authentication Interface for PWD Administrators. Although structurally similar to the PWD user login page, this interface is dedicated to administrative access. Upon successful authentication, administrators are redirected to the administrative dashboard, where system management functions such as user verification, account activation, and monitoring of records are available.

If the submitted credentials match the stored encrypted records and all account status requirements are satisfied, the system grants access according to the assigned role and redirects the user to the corresponding dashboard interface.

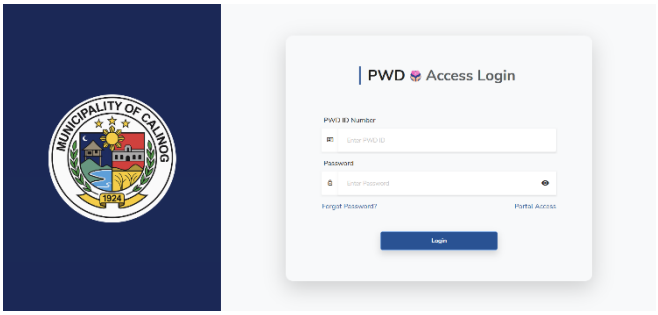

Fig. 2 Authentication Interface for PWD Users

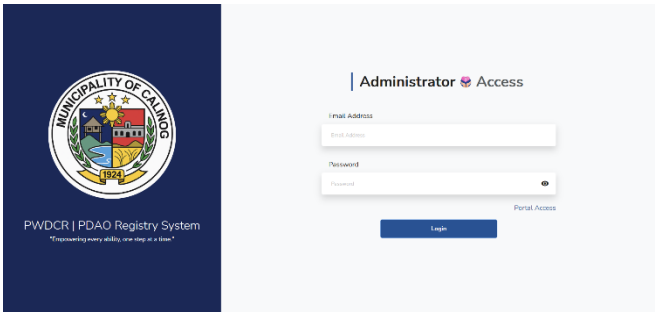

Fig. 3 Authentication Interface for PWD Administrator

2) RFID Verification Algorithm: The system implements an RFID-based identification mechanism to facilitate automated verification of registered PWD members. The RFID card is verified using the ESP8266 NodeMCU reader module, which is responsible for detecting and capturing the unique RFID identifier (UID) embedded within the card. Each RFID card contains a distinct UID that serves as the primary key for identifying the corresponding PWD record in the system database.

As illustrated in Fig. 4, once the RFID card is placed near the scanner, the reader captures the UID and automatically transmits the data to the server through a secured Wi-Fi connection. The server then processes the received UID and performs a database query to determine whether the scanned identifier exists and remains valid. This real-time verification mechanism ensures efficient authentication and minimizes manual data entry errors.

If the scanned RFID UID matches an existing record in the database and the account status is active, the system displays the corresponding PWD profile, including personal details and benefit eligibility information. This enables establishments and administrators to verify privileges quickly and accurately.

Conversely, if the RFID UID is not found in the database, has expired, or is associated with an inactive account, the system generates an alert notification indicating that the card is invalid or no longer active. This safeguard prevents unauthorized access and ensures that only legitimate and active PWD members can avail of system-supported benefits.

Fig. 4 presents the RFID UID Verification Process, showing the interaction between the RFID scanner, wireless communication module, and the centralized server database. Fig. 5 illustrates the Register Unique PWD ID Scanner interface, which is used for enrolling and associating a new RFID UID with a registered PWD profile in the system.

Fig. 4 RFID UID Verification Process

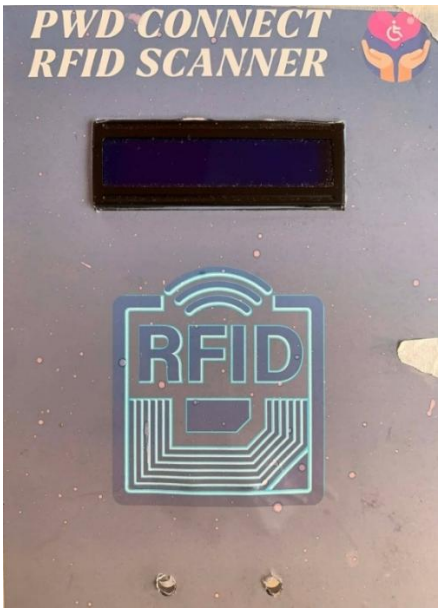

Fig. 5 Register Unique PWD ID Scanner

3) Data Processing: The system provides a structured mechanism for handling both registration and renewal applications of PWD members. As shown in Fig. 4, users are required to submit the necessary information and upload supporting documents as part of the application process. The system performs validation procedures to ensure the completeness, accuracy, and correctness of the submitted data before further processing. Required fields are checked for missing entries, and uploaded files are examined to confirm acceptable formats and content compliance.

Upon successful validation, the uploaded documents are securely stored in temporary storage within the system for administrative review. This temporary staging ensures that unverified records are not immediately integrated into the main database, thereby maintaining data integrity and system reliability.

The administrator is then responsible for reviewing each submitted application. During this stage, the administrator evaluates the authenticity and validity of the provided documents and verifies whether the applicant meets the necessary requirements. Based on the evaluation, the application is either approved or rejected.

If the application is approved, the verified user information and associated records are permanently stored in the system database, and the account status is updated accordingly. Conversely, if the application is rejected, the system notifies the user and may provide feedback regarding incomplete or invalid requirements. This controlled workflow ensures accountability, data accuracy, and proper authorization within the registration and renewal process.

4) Report Generation: The system provides an integrated reporting and analytics module that enables administrators to generate structured reports for monitoring and decision-making purposes. Administrators can select the desired report type, including registration summary, benefits usage, or renewal status, and specify the preferred date range to define the reporting scope. Based on the selected parameters, the system retrieves the relevant records from the centralized database.

The retrieved data undergo processing procedures, including filtering, categorization, and sorting, to ensure accuracy and relevance. After data preprocessing, the system generates analytical summaries that present aggregated results, trends, and key performance indicators. These summaries support evidence-based decision-making and improve administrative oversight.

As illustrated in Fig. 6, the Administrative Analytics Dashboard Interface presents the generated reports in a structured and user-friendly format. The dashboard allows administrators to view summarized information in real time and provides options for exporting the reports for documentation, record-keeping, and compliance purposes.

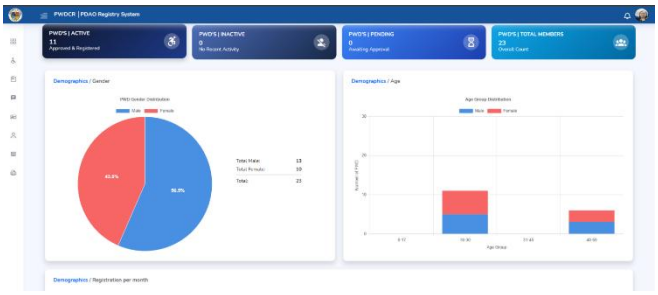

Fig. 6. Administrative Analytics Dashboard Interface.

D. System Development Methodology

1)Requirement Gathering: During the requirement gathering phase, the researchers conducted interviews, brainstorming sessions, and document analysis with key stakeholders, including the PDAO Head, staff, PWD members, store owners, and IT experts. From these engagements, the researchers identified both functional

and non-functional requirements and translated them into user stories to clearly represent system expectations from each user's perspective. The researchers defined user roles such as Admin, Staff, PWD User, and Store Owner to guide feature development. This process enabled the researchers to understand operational challenges and ensured that the proposed system directly addressed the needs of the PWD community and partner establishments.

2) Sprint Planning: In the sprint planning phase, the researchers prioritized the collected user stories based on importance, feasibility, and system impact. The researchers defined specific sprint goals, allocated development tasks, and identified the necessary hardware and software resources. The integration of technologies such as HTML, CSS, Bootstrap 5, JavaScript, PHP, MySQL, and the ESP8266 NodeMCU with RFID reader was carefully planned. By organizing the workload into manageable iterations, the researchers ensured that each sprint produced measurable and functional outputs.

3)Development: During development, the researchers implemented the selected user stories incrementally following a three-tier client–server architecture composed of presentation, application, and database layers. The frontend interface was developed to ensure accessibility and responsiveness, while backend logic was implemented to handle authentication, RFID validation, data processing, and report generation. The MySQL database was structured to securely store PWD records, RFID UIDs, and transaction logs. Each sprint resulted in a working module that was progressively integrated into the overall system.

4) Testing: After completing each development iteration, the researchers conducted systematic testing to verify the system's functionality and overall quality. Unit testing was performed to validate individual components, integration testing ensured proper communication between modules, and system testing evaluated the overall performance of the integrated platform. Additionally, RFID authentication testing was conducted to confirm accurate real-time UID verification and secure transaction recording.

For formal system evaluation, the researchers exclusively utilized the ISO/IEC 25010 Software Quality Model as the assessment framework. The system was evaluated based on the following quality characteristics: functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability. A structured questionnaire derived from ISO/IEC 25010 standards was administered to selected respondents, and the collected data were analyzed using weighted mean and descriptive statistical methods to determine the overall level of system acceptability and quality.

5) Review and Feedback: At the end of every sprint, the researchers presented the developed features to stakeholders for evaluation. Feedback was gathered regarding usability, efficiency, reliability, and security. Based on the comments and suggestions received, necessary improvements were identified and incorporated into the succeeding development cycle. This collaborative evaluation allowed the researchers to refine system features and align the platform with stakeholder expectations.

6) Iteration and Refinement: After each sprint review, the researchers conducted an iteration and refinement phase to improve both the system and the development process. During this phase, the researchers analyzed stakeholder feedback, identified technical issues, evaluated workflow efficiency, and assessed areas that required enhancement. Necessary revisions were implemented, including interface improvements, optimization of backend processes, enhancement of RFID authentication accuracy, and strengthening of security measures. Lessons learned from previous iterations were documented and applied to subsequent development cycles. This continuous refinement process ensured progressive improvement in system functionality, performance, and reliability until all prioritized user stories were fully implemented and the system met the established ISO/IEC 25010 quality standards for deployment.

E. Experimental Setup and Evaluation Procedure

1) Participants of the study: The participants of the study consisted of the PDO Head Officer and staff, who served as the administrators of the system. They were responsible for managing registrations, approving applications, monitoring transactions, and generating reports. The PWD members and establishment owners or staff acted as end users of the system, utilizing its features for registration, verification, and benefit validation. Additionally, IT experts served as validators of the study. They evaluated the technical aspects of the system, including functionality, security, performance, and overall system architecture, to ensure that it met established software quality standards and operational requirements.

2) Evaluation Instrument: An adapted survey instrument based on the ISO/IEC 25010:2011 software quality model was utilized to evaluate the system. The instrument measured key quality characteristics such as functionality, usability, reliability, security, maintainability, and portability. A five-point Likert scale was employed to quantify the respondents' level of agreement and assessment of system performance. The rating scale was interpreted as follows:

Scale Description

5 – Excellent

4 – Very Good

3 – Good

2 – Fair

1 – Poor

This scaling method allowed systematic measurement and statistical analysis of user feedback to determine the overall acceptability and effectiveness of the system.

3) Testing Environment: The testing environment of the system consisted of several components to ensure proper functionality and verification. The admin dashboard was accessed through the Google Chrome web browser, while the backend was supported by a local PHP server. System data was stored and managed using a MySQL relational

database. The RFID verification process was tested using an ESP8266 NodeMCU integrated with an RFID module, which captured unique RFID identifiers (UIDs) from pre-registered RFID cards. Communication between the RFID reader and the server was established through a Wi-Fi network, enabling real-time transmission of UIDs and verification of user profiles and benefit eligibility.

F) Data Analysis

The weighted mean was employed to analyze the collected data. It was computed using the formula:

$$X = \frac{\sum fx}{N}$$

where X represents the mean score, f denotes the frequency of each rating, x is the corresponding rating value, and N is the total number of responses. This method was chosen to account for the varying frequencies of each response, providing a more accurate representation of the overall trends in the data.

IV. Result and Discussion

The developed system, PWD Connect: A Comprehensive Online Hub Using RFID with Data Analytics, was evaluated using the ISO/IEC 25010 software quality model to determine its overall performance and acceptability. The evaluation involved twenty (20) respondents composed of two (2) PDAO staff, two (2) store owners, five (5) IT experts, and eleven (11) registered PWD users. A five-point Likert scale was utilized, where 5 indicates "Excellent" and 1 indicates "Poor."

The evaluation results revealed that the system obtained an overall Grand Mean of 4.71 with a Standard Deviation of 0.05, interpreted as Excellent. The low standard deviation indicates strong consistency in responses and high agreement among stakeholders regarding the system's quality.

In terms of Functional Suitability, the system achieved a mean score of 4.72. Respondents confirmed that the system effectively performed its intended functionalities, including RFID-based registration, real-time identity verification, benefit tracking, renewal processing, and automated report generation. These results demonstrate that the system satisfies operational requirements and user expectations.

For Performance Efficiency, the system obtained a mean of 4.68. During testing, RFID authentication was completed within 2–3 seconds per transaction, and database retrieval exhibited minimal latency. This indicates that the system is capable of handling real-time transactions efficiently.

Compatibility received a mean score of 4.70. The web-based system operated consistently across desktops, laptops, and mobile devices using modern browsers, demonstrating cross-platform capability.

Usability recorded the highest mean score of 4.75. Respondents highlighted the intuitive dashboard layout, simple navigation, and accessible registration and renewal portals. PWD users reported that the system significantly reduced physical visits and simplified monitoring of benefits.

Reliability obtained a mean of 4.69. System testing showed stable uptime, accurate RFID verification, and consistent transaction logging, indicating dependable performance.

Security achieved a mean score of 4.73. The implementation of HTTPS encryption, role-based authentication, unique RFID serial mapping, and activity logs strengthened system protection against unauthorized access and fraudulent claims.

Maintainability received a mean of 4.67. IT experts confirmed that the modular architecture supports system updates, debugging, and future scalability.

Finally, Portability obtained a mean score of 4.71, indicating that the system can be deployed in other municipalities with minimal configuration adjustments.

The consistently high ratings across all quality characteristics confirm that the developed system meets ISO/IEC 25010 standards and provides a secure, efficient, and user-friendly solution for managing PWD services.

Table 2

OVERALL SOFTWARE QUALITY EVALUATION RESULTS

Quality Characteristic	Mean	SD	Interpretation
Functional Suitability	4.72	0.06	Excellent
Performance Efficiency	4.68	0.05	Excellent
Compatibility	4.70	0.04	Excellent
Usability	4.75	0.05	Excellent
Reliability	4.69	0.06	Excellent
Security	4.73	0.05	Excellent
Maintainability	4.67	0.07	Excellent
Portability	4.71	0.05	Excellent
Grand Mean	**4.71**	**0.05**	**Excellent**

V. Conclusion and Future Work

A) Conclusion

This study successfully designed, developed, and evaluated PWD Connect: A Comprehensive Online Hub Using RFID with Data Analytics, a centralized digital platform that modernizes registration, verification, and monitoring processes for Persons with Disabilities (PWDs). The system addressed critical gaps in traditional manual and fragmented administrative procedures by integrating web-based services, RFID-enabled identification, secure authentication mechanisms, and data analytics into a unified client–server architecture.

The implementation of RFID technology enabled real-time, contactless identity verification, significantly reducing processing time and minimizing human error during benefit transactions. Integration of role-based access control, encrypted authentication, and unique RFID UID mapping strengthened system security and mitigated risks of fraudulent claims and data duplication. Furthermore, the embedded analytics module transformed raw transactional data into structured reports and

actionable insights, supporting evidence-based decision-making for PDAO administrators and partner establishments.

The system was rigorously evaluated using the ISO/IEC 25010:2011 software quality model. Results demonstrated an overall Grand Mean of 4.71, interpreted as Excellent, across all assessed characteristics, including functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability. The low standard deviation indicated strong consensus among respondents, confirming the system's robustness, consistency, and overall acceptability.

From a practical perspective, this study contributes to digital transformation initiatives within local government units by providing a scalable and replicable framework for inclusive public service delivery. The system enhances administrative efficiency while promoting accessibility, transparency, and equitable access to government-mandated benefits for the PWD community. By combining secure identification technology with analytics-driven governance, this research demonstrates how emerging technologies can strengthen inclusive public administration.

B) Future Work

Despite achieving excellent evaluation results, several enhancements can further improve the functionality, scalability, and sustainability of PWD Connect. Future development may include dedicated Android and iOS applications to improve accessibility, enabling PWD members to receive real-time notifications, renewal reminders, and updates on their benefits.

Migrating the system to a cloud-hosted infrastructure could enhance scalability, strengthen disaster recovery, and enable inter-municipality integration for broader regional implementation. The analytics module may also be expanded to incorporate predictive analytics and machine learning algorithms, which can forecast benefit demand, identify service gaps, and detect anomalous transaction patterns indicative of fraud.

To further strengthen security, future iterations could integrate biometric multi-factor authentication, such as fingerprint or facial recognition, alongside RFID verification. Interoperability with national government databases, including health, social welfare, and civil registry systems, would streamline verification processes and improve data consistency across agencies. Continuous refinement of accessibility features, including screen reader optimization, voice command integration, and multilingual support, will ensure compliance with evolving accessibility standards and inclusive design principles. Additionally, longitudinal studies may be conducted to evaluate the long-term socio-administrative impact of the system, including improvements in service efficiency, fraud reduction, and overall quality of life among PWD beneficiaries.

REFERENCES

[1] Republic of the Philippines, Republic Act No. 7277: An Act Providing for the Rehabilitation, Self-Development and Self-Reliance of Disabled Persons and Their Integration into the Mainstream of Society and for Other Purposes, Manila, Philippines, 1992.

[2] World Health Organization, International Classification of Functioning, Disability and Health (ICF). Geneva, Switzerland: World Health Organization, 2001.

[3] N. A. Abdul Aziz, N. M. Isa, and N. A. N. M. Noor, "Accessibility issues in e-government websites in Malaysia," in 2011 International Conference on Research and Innovation in Information Systems (ICRIIS), Kuala Lumpur, Malaysia, 2011, pp. 1–6, doi: 10.1109/ICRIIS.2011.6125727.

[4] S. Furnell and K. Evangelatos, "Accessibility and usability of authentication mechanisms," Computers & Security, vol. 63, pp. 159–169, 2016, doi: 10.1016/j.cose.2016.08.010.

[5] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd ed. Hoboken, NJ, USA: Wiley, 2010.

[6] R. Hassan and Z. Shukur, "Review of digital authentication methods for secure systems," International Journal of Advanced Computer Science and Applications, vol. 13, no. 3, pp. 456–463, 2022.

[7] T. H. Davenport and J. G. Harris, Competing on Analytics: The New Science of Winning. Boston, MA, USA: Harvard Business Review Press, 2017.

[8] ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. Geneva, Switzerland: International Organization for Standardization, 2011..