International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

White Card Manages All Cards into One (Driving License, Pan Card, Voter Id, Ration Card)

Mr. R. Sathish Kumar[1], *P. Krishna Kumar*[2]

[1]**MCA, M. Phil.,** Asst. Prof., Department of MCA, Krishnasamy College of Engineering & Technology
[2]**MCA,** Department of MCA, Krishnasamy College of Engineering & Technology

ABSTRACT

The project "White Card Application with Android App" aims to design and develop a secure and dynamic mobile application for reading QR codes. This application is intended to serve as a personal identification card for Indians, known as the White Card. An identity document is a piece of identification that verifies various aspects of a person's identity. The White Card Application with Android App will be designed to encompass multiple forms of identification, including driving licenses, PAN cards (Permanent Account Number), voter IDs, and ration cards. By consolidating these identification documents into a single card, individuals can have a comprehensive and easily accessible means of proving their identity. In countries where formal identity documents may be lacking, driving licenses are often accepted as a valid proof of identity. Additionally, passports are widely accepted as a recognized form of identification across many countries. The White Card, with its adoption of a universal product code, aims to streamline identity verification processes and facilitate easier surveillance and identification of criminals.

Keywords: QR Reading, Code adoption, Identification, Surveillance.

1. INTRODUCTION

The White Card, which will be issued to ration card holders falling under the below poverty line (BPL), above poverty line (APL) and (poorest of the poor) categories, will contain all necessary details like names of the card holders and their family members, addresses, contact numbers, blood group and private account numbers. The move will certainly help us check the increasing number of fake ration cards, and also curb the illegal practice of diverting food grains and other essential commodities by fair price shop owners to open market.

An android application is used to retrieve the information from database to the android mobile. apk file is created by using Eclipse software with android sdk 2.0. In our android mobile, we need to install the apk file. In that android application, we can enter the details to retrieve the data from mysql database.

Android user can login with their username and password through this android application

2. LITERATURE REVIEW

White Card Authentication is a crucial process that involves verifying the White Card number and the accompanying demographic or biometric information of the cardholder. This authentication process is carried out by the Central Identities Data Repository (CIDR) at the request of service providers such as banks, insurance companies, mutual fund companies, or telecom operators who require proof of identification.

White Card Authentication can be completed using various methods, including:

1. One-Time Pin (OTP) Based Authentication: OTP-based authentication is another method used to authenticate White Card holders. During this process, an OTP (One-Time Pin) is generated and sent to the mobile number or email address registered with the White Card authority. The cardholder is required to provide this OTP, along with their White Card number, during the authentication process. The provided OTP is then matched with the OTP generated by the White Card authority. The OTP is time-limited, meaning it has a short validity period, usually a few minutes, to ensure its security and prevent misuse. By matching the provided OTP with the one generated by the White Card authority, the authentication process confirms the cardholder's identity. This method adds an extra layer of security to the authentication process.
2. Biometric-Based Authentication: The White Card number and biometric information submitted by the cardholder, such as fingerprints or iris scans, are compared with the biometric data stored in the CIDR. This ensures a high level of identity verification using biometric modalities stored in the repository.
3. Multi-Factor Authentication: To enhance security, a combination of two or more authentication modes mentioned above can be employed. Service providers, based on their requirements, can choose the suitable modes of authentication for specific services or business functions.

It's important to note that e-KYC (electronic Know Your Customer) authentication is restricted to the use of OTP and/or biometric authentication methods.

Requesting entities, such as banks, insurance companies, EPF (Employees' Provident Fund), or mutual fund companies, can select the appropriate authentication modes based on their specific needs. They may also opt for multiple factors of authentication to further enhance security.

EXISTING SYSTEM:

- In the present system only the officer for verification and validation, public use need to bring original id proof.
- For each different place, different ID proofs are required to carry
- Possibility of loss of proof will lead to suffering the user.

PROPOSED SYSTEM:

In this system, the White Card acts as a comprehensive identification document that combines the information from different forms of identification such as the Driving License, PAN Card, Voter ID, and Ration Card. This consolidated information is represented by a unique 12-digit number.

The 12-digit number associated with the White Card enables individuals to retrieve the status and details of all four ID proofs. By entering this number into the system, users can access information related to their Driving License, PAN Card, Voter ID, and Ration Card, providing a holistic view of their identification status.

The system's centralized repository ensures that the data is securely stored and readily available for authorized individuals. It simplifies the process of managing and verifying multiple forms of identification, offering convenience and efficiency to users.

3. OVERALL DESCRIPTION OF THE PROPOSED SYSTEM

3.1 Module Description: The proposed system consists of the following modules, each serving a specific function within the White Card application:

1. Admin:
   - Login: Allows the system administrator to log in to the application.
   - Create Officer: Enables the administrator to create new officers within the system.
   - Manage Officer: Provides functionality to manage and update officer details.
   - Create White Card: Allows the administrator to create new White Cards and associate them with individuals.
   - Update Proof Details: Enables the administrator to update the details of identification proofs linked to White Cards.
   - Update Status: Allows the administrator to update the status of White Cards based on verification or validation.
   - View Status: Provides a view of the status of White Cards and associated identification proofs.
   - Generate QR Code: Enables the generation of QR codes for White Cards to facilitate scanning and identification.
   - Update Code: Allows the administrator to update the QR code associated with a specific White Card.
2. Officer:
   - RTO Login: Enables RTO officers to log in to the system.
   - Verify License Details: Allows RTO officers to verify and validate driving license details associated with White Cards.
   - Update Status: Enables RTO officers to update the status of driving licenses based on verification outcomes.
   - IT Officer:
   - IT Login: Allows IT officers to log in to the system.
   - Verify IT Return: Provides functionality for IT officers to verify the income tax return details linked to White Cards.
   - Check Status: Allows IT officers to check the status of IT return verification for a specific White Card.
   - Voting Officer:
   - Voter Login: Enables voting officers to log in to the system.
   - Verify Voting Details: Provides functionality for voting officers to verify the voting details associated with White Cards.
   - Check Voting Status: Allows voting officers to check the voting status and eligibility of individuals based on their White Cards.

- Ration Officer:
- Ration Login: Allows ration officers to log in to the system.
- Verify Ration Card Details: Enables ration officers to verify and validate the ration card details linked to White Cards.
- Check Ration Details: Provides functionality for ration officers to check the details and eligibility of individuals for ration cards.

3.2 System Features: The system encompasses the following features across its modules:

- User Authentication: Different levels of user authentication are implemented for admins, officers, and specific officer types.
- User Management: The system allows the creation and management of officer accounts by the admin.
- White Card Creation: The admin can create new White Cards and associate them with individuals.
- Proof Details Management: The admin can update the details of identification proofs linked to White Cards.
- Status Updates: Officers can update the status of identification proofs based on their verification outcomes.
- Status Checking: Officers can check the status of verification and eligibility for different identification proofs.
- QR Code Generation: The system enables the generation of QR codes for White Cards, facilitating efficient scanning and identification.
- QR Code Updates: The admin can update the QR code associated with a specific White Card to ensure accuracy and security.

These features collectively support the efficient management and verification of identification proofs through the White Card application, streamlining processes for various officer roles such as RTO officers, IT officers, voting officers, and ration officers.

Module Description:

Admin:

- Login: This module allows the admin to log in using their credentials. It serves as the starting point for accessing other modules.
- Create Officer: The admin has the ability to create officers for different departments (RTO, Ration, IT, Voting). The admin can input personal information such as officer name, department, address, mobile number, city, and area. The admin also assigns a login ID and password for the officer.
- Manage Officer: The admin can manage the officer database, making modifications as needed. This module enables the admin to update officer details, such as in the case of a transfer.
- Create White Card: The admin can create a White Card by incorporating details from various government proofs such as voter ID, PAN card, driver's license, and ration card. This module allows the admin to upload and handle personal data for the White Card.
- Update Proof Details: The admin can update the details of the government proofs associated with a White Card. This module facilitates the uploading or modification of voter ID, PAN card, driver's license, and ration card details.
- Update Status: After the admin has updated all the necessary details, they can update the status of the White Card process. This module tracks the progress and status of White Cards.
- View Status: Officers can view the status of White Card approvals. Once an officer verifies the details, they can upload the status, and this module allows other officers to view the updated status.
- Generate QR Code: The admin can generate a QR code based on the national identification number. After all verification details are completed by the officers, the admin can generate the QR code.
- Upload Code: The admin uploads the generated QR code to the White Card. Users or admins can scan the QR code to access all the associated details.

Officer: RTO Officer:

- RTO Login: This module provides a login page for RTO officers. They can log in using their credentials to access the subsequent RTO modules.
- Verify License Details: RTO officers verify the license details of users and proceed with the necessary approvals for the next stages.
- Update Status: After verifying the license details, RTO officers can update the status of the license (e.g., in progress, approved, not approved).

IT Officer:

- IT Login: This module offers a login page for IT officers. They can log in using their credentials to access the subsequent IT modules.

- Verify IT Return: IT officers verify the IT return details of users and proceed with the necessary approvals for the next stages.
- Check Status: IT officers can check the status of verified IT return details, such as whether they are in progress, approved, or not approved.

Voting Officer:

- Voter Login: This module provides a login page for voting officers. They can log in using their credentials to access the subsequent voting modules.
- Verify Voting Details: Voting officers verify the voting details of users and proceed with the necessary approvals for the next stages.
- Check Voting Status: After verifying the voting details, voting officers can update the status (e.g., in progress, approved, not approved).

Ration Officer:

- Ration Login: This module offers a login page for ration officers. They can log in using their credentials to access the subsequent ration modules.
- Verify Ration Card Details: Ration officers verify the ration card details of users and proceed with the necessary approvals for the next stages.
- Check Ration Status: After verifying the ration card details, ration officers can update the status (e.g., in progress, approved, not approved).

White Card Creation: This module is responsible for creating a basic white card for each citizen. A white card is also issued to newborns when their birth certificate is generated. The white card contains six major categories and includes the national identification number and blood group. The next module involves generating a barcode for the white card.

Barcode Updating: After generating the white card with basic details, a barcode relevant to the national identification number is generated. This barcode, along with the national identification number, serves as a unique identifier for each citizen. The barcode values are saved in a centralized data repository accessible only through the web application and a specially designed barcode reader.

Centralizing the Data: This crucial module involves storing the updated details, including driving license details, DNA details, PAN card number, ration card details, voter ID details, and citizenship card details, in a centralized server and sub-servers. An admin with specific permissions, such as police officers, income tax officers, and ration shop workers, can access and update these details.

Information Warehouse: A dedicated server is designed to store all the confidential information, with stringent security measures in place. Only cardholders can access their own details, while admins serve as the accessing agents.

Mining Data from the Server: Admins play a significant role in this module. They use a special barcode reader to access white cards from users. Admins can mine data based on their specific roles. For example, a police officer can access license information and update any black marks associated with users. Admins from different areas can view black marks updated by other admins.

Details from Android Application: Users can log into the Android application using their username and password. The application allows users to retrieve personal details, such as voter ID, PAN card, passport, ration card, and driving license, by entering the respective ID. Users can also update complaints through the application, which are then stored in the database.

Note: The module descriptions provided here are based on the information given and may require further refinement or customization based on specific implementation requirements.

3. Design

During the system study phase, a feasibility study is conducted to assess the viability of the proposed system. This study includes analyzing the economic, technical, and social aspects of the project.

Economic Feasibility:

The economic feasibility focuses on evaluating the financial impact of the system on the organization. It is crucial to ensure that the project fits within the allocated budget and that the expenses are justified. In this case, the developed system is considered economically feasible because most of the required technologies are freely available, and only customized products need to be purchased.

Technical Feasibility:

The technical feasibility examines the technical requirements of the system. It is important to ensure that the system does not place a high demand on the available technical resources, as this could burden the client. The developed system is designed to have modest technical requirements, requiring minimal or no changes for implementation.

Social Feasibility:

The social feasibility assesses the acceptance of the system by its users. User training is crucial to ensure that they can efficiently use the system. It is important for users to not feel threatened by the system but rather see it as a necessity. The acceptance of the system depends on the methods used to educate and familiarize users, raising their confidence and encouraging constructive criticism.

Non-functional Requirements:

In addition to the feasibility aspects, non-functional requirements play a significant role in the system's design and execution. These requirements are related to the system's quality attributes and include the following:

Accuracy: The system is designed to be accurate and reliable. If any inaccuracies arise, alternative solutions will be provided.

Usability: The proposed system will have a user-friendly interface, making it simple and easy for users to interact with.

Accessibility: The system will be accessible through the Internet without any known issues, ensuring users can access it conveniently.

Performance: The system's performance will be optimized to ensure efficient functionality, allowing users to perform tasks quickly and smoothly.

Reliability: The system will be designed to be reliable in all circumstances. Any issues that arise will be effectively handled to minimize disruptions.

Security: The proposed system will prioritize high security. Users will be required to register and use username/password credentials. The system will implement proper authorization and authentication processes based on user types and requirements, aiming to prevent misuse of the application and protect user data.

Overall, the system study phase carefully evaluates the feasibility of the project, considering both the technical aspects and the non-functional requirements to ensure the successful development and implementation of the system.

4. SYSTEM TESTING

TYPES OF TESTS

Unit testing

Unit testing is a critical phase in software development where test cases are designed to validate the internal logic of individual program units. The primary goal is to ensure that the program's inputs produce valid outputs and that all decision branches and internal code flow are functioning correctly. This type of testing is conducted on isolated software units, typically after the completion of each unit and before integration with other units.

Unit testing is a form of structural testing that relies on knowledge of the unit's construction and implementation details. It is considered invasive as it involves delving into the internal workings of the unit being tested. The purpose is to identify any defects or issues within the unit and ensure its proper functionality.

During unit testing, specific business processes, applications, or system configurations are tested at a component level. The tests performed focus on a particular unit's functionality and verify that it performs accurately according to the documented specifications. Inputs are provided to the unit, and the expected results are compared to the actual outputs produced by the unit.

Integration testing

By conducting integration testing, software development teams can gain confidence in the functionality, reliability, and performance of the integrated software. Any discrepancies or flaws discovered during this phase can be addressed promptly, improving the overall quality of the software before it is deployed to end-users.

In summary, integration testing is a vital step in the software development lifecycle that focuses on verifying the correct functioning and seamless interaction of integrated components. It is an essential part of ensuring the overall quality and effectiveness of the software system being developed.

Functional testing

A systematic approach to verify that the tested functions of a software system align with the specified business and technical requirements, system documentation, and user manuals. It focuses on demonstrating that the expected functions are available and functioning correctly. The key elements of functional testing include testing valid and invalid inputs, exercising identified functions, testing different output scenarios, and invoking interfacing systems or procedures.

The organization and preparation of functional tests are based on requirements, key functions, and special test cases. It is important to consider systematic coverage by identifying business process flows, data fields, predefined processes, and successive processes for testing. Throughout the process, additional tests may be identified, and the effectiveness of existing tests is evaluated to ensure comprehensive coverage.

System testing, on the other hand, verifies that the entire integrated software system meets the defined requirements. It tests the system configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test, which focuses on process descriptions, flows, pre-driven process links, and integration points.

White Box

Gray Box Testing is a testing approach that combines elements of both white box and black box testing. In gray box testing, the tester has partial knowledge of the internal workings, structure, or language of the software being tested. This allows for a more nuanced understanding of the system's internals than black box testing, while still maintaining some independence from the specific implementation details as in white box testing.

Gray box testing aims to strike a balance between the detailed insight provided by white box testing and the external perspective of black box testing. Testers with access to limited information about the system can design test cases that target specific areas of interest, such as critical algorithms or complex data flows.

By leveraging the partial knowledge of the system, gray box testing can uncover defects that may not be apparent through black box testing alone. Testers can focus on areas that are more likely to contain issues or vulnerabilities, while still validating the overall functionality and behavior of the software from an end-user perspective.

Gray box testing can be particularly useful in situations where full access to the system's internals is not available or practical, such as when testing third-party components or legacy systems with limited documentation. It provides a middle ground that allows for more targeted testing without requiring complete knowledge of the system's implementation details.

Overall, gray box testing complements white box and black box testing approaches by offering a flexible and adaptable approach to software testing. It combines elements of both perspectives to provide a comprehensive assessment of the software's functionality, performance, and security.

Test Strategy and Approach:

For the field testing, a manual approach will be followed, where testers will perform the tests by interacting with the software system directly. Detailed functional tests will be written to ensure thorough coverage and validation of the system's behavior.

Test Objectives:

The objectives of the tests are as follows:

- Ensure that all field entries function properly.
- Verify that pages are activated correctly when accessed through identified links.
- Validate that entry screens, messages, and responses are timely and without delays.

Features to be Tested:

The following features will be tested:

- Format validation of entries to ensure they are in the correct format.
- Prevention of duplicate entries.
- Verification that all links navigate the user to the correct pages.

Integration Testing:

Integration testing aims to identify failures caused by interface defects when two or more integrated software components are tested together on a single platform. The purpose is to ensure that the components or software applications interact without errors.

Test Results:

All the test cases mentioned above have passed successfully, and no defects were encountered during testing.

Acceptance Testing:

User Acceptance Testing (UAT) is a critical phase where end users participate to ensure that the system meets the functional requirements. It involves validating the system's behavior from the user's perspective.

Test Results:

All the test cases mentioned above for acceptance testing have passed successfully, and no defects were encountered.

Test Case:

A test case comprises components that describe the input, action, and expected response to determine if a feature of the application is working correctly. It provides instructions on how to validate a specific test objective, ensuring that the expected behavior of the system is satisfied.

Characteristics of a good test case:

A good test case possesses the following characteristics:

- Accuracy: It accurately reflects the purpose of the test.

- Economical: It avoids unnecessary steps or words.
- Traceable: It can be traced back to the requirements.
- Repeatable: It can be executed multiple times.
- Reusable: It can be reused if needed.

By following these strategies and approaches, conducting thorough testing, and ensuring the effectiveness of test cases, the software system can be validated and its quality can be assured.

7. CONCLUSIONS

The White Card Web Application offers users a user-friendly interface through which they can access and retrieve their personal information effortlessly. This information can be easily browsed or queried, empowering users with quick and convenient access to the details they need. One of the significant advantages of this application is its ability to help users avoid duplication of their personal information.

By leveraging the White Card Web Application with Android App, users no longer need to carry physical copies of their identity proofs everywhere. Instead, they can rely on the application to provide them with instant access to their information whenever necessary. Whether it's verifying their driving license details or confirming their PAN card information, this application streamlines the process and ensures the information is readily available.

The implementation of the White Card Web Application with the Android App involves integrating various identity-proof databases, establishing secure connections, and designing an intuitive user interface for seamless navigation. The application's compatibility with Android devices ensures widespread accessibility for users.

Overall, the White Card Web Application with Android App offers a practical and efficient solution for users to access and manage their personal information. It enhances convenience, eliminates the need for physical documents, and simplifies the process of obtaining information related to identity proofs.

Regenerate response

The white card management system project, here are some potential future work ideas to enhance

and improve the system:

FUTURE ENHANCEMENT

For the white card management system project, here are some potential future work ideas to enhance and improve the system

1. **Mobile Application**: Develop a mobile application that allows users to access their white card information, submit applications, receive notifications, and update their details on the go. The mobile app can provide a more convenient and user-friendly experience.

2. **Integration with Government Databases**: Establish integration with role government database sales to streamline the verification process. This integration can ensure real-time validation of cardholder information, making the system more accurate and efficient.

3. **Biometric Authentication**: Implement biometric authentication methods, such as fingerprint or facial recognition, to enhance the security and reliability of the white card management system. This would help prevent identity theft or unauthorized card usage.

4. **Online Training Modules**: Include an online training module within the system to provide educational resources for cardholders. This could cover topics such as workplace safety guidelines, hazard identification, and emergency response procedures. Users could access these modules and complete them to maintain an active white card status.

5. **Reporting and Analytics:** Enhance the system with reporting and analytics capabilities to provide valuable insights to stakeholders. Generate reports on card issuance, renewal rates, the geographic distribution of cardholders, and other relevant metrics. This information can help identify trends, measure the system&#39;s effectiveness, and make data-driven decisions for process improvement.

8. REFERENCES

The list provided includes several research papers related to QR codes, biometric authentication, and secure authentication schemes. These papers cover various aspects of QR code technology, including beautification, private message sharing, document authentication, and multi-view schemes. Additionally, they explore topics such as secure biometric template generation, template protection, and cost-benefit analysis of authentication systems. Here is a brief summary of each paper:

1. "Efficient QR Code Beautification With High-Quality Visual Content" by SS Lin et al. (2015) focuses on enhancing the visual appearance of QR codes while maintaining their functionality.

2. "Two-Level QR Code for Private Message Sharing and Document Authentication" by I. Tkachenko et al. (2016) proposes a two-level QR code system for secure message sharing and document authentication.
3. "Appearance-Based QR Code Beautifier" by YH Lin et al. (2013) presents a method for enhancing the visual appearance of QR codes using appearance-based techniques.
4. "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code" by Lin Pei-Yu (2016) introduces a distributed secret-sharing approach using QR codes to prevent cheating.
5. "High-Density QR Code With Multi-View Scheme" by JS Chiang et al. (2013) proposes a high-density QR code design that supports multiple views for improved data capacity and error correction.
6. "Secure Biometric Template Generation for Multi-Factor Authentication" by SH Khan et al. (2015) discusses the generation of secure biometric templates for multi-factor authentication systems.
7. "Evaluation of a Template Protection Approach to Integrate Fingerprint Biometrics in a PIN-Based Payment Infrastructure" by J Breebaart et al. (2011) evaluates a template protection approach for integrating fingerprint biometrics in a PIN-based payment infrastructure.
8. "Cost and Benefit Analysis of Authentication Systems" by K Altinkemer and T Wang (2011) presents a cost-benefit analysis of different authentication systems, considering their effectiveness and associated costs.
9. "Transmission of Data Using Arm-Based Privacy Protection QR-Code" by G Prabakaran and R Bhakkiyalakshmi (2014) explores the use of privacy-protected QR codes for secure data transmission.
10. "QR Code-Based Secure OTP Distribution Scheme for Authentication in Net-Banking" by A Tandon et al. (2013) proposes a secure OTP (One-Time Password) distribution scheme using QR codes for authentication in net-banking applications.