RESEARCH ARTICLE OPEN ACCESS

White Card: A Unified Digital Identity Management System Using QR Code and Role-Based Access

Jeffrey S*, Dr. S. Prasanna**
*Student, Department of Computer Application-PG,
Vels Institute of Science, Technology and Advanced Studies, Chennai
**Professor, Department of Computer Application-PG,
Vels Institute of Science, Technology and Advanced Studies, Chennai

ABSTRACT
With the emergence of this digital age, it is now necessary for individuals to carry various identity proofs like Driving License, PAN Card, Voter Id, and Ration Card to access several governmental as well as private services. The need to carry all these separate identity proofs results in an increased burden on the citizens. Therefore, we have come up with the concept of a White Card System, which provides citizens with a single smart card integrated with QR code and pin based verification system. For the design of this concept, we have used three-tier architecture, with HTML, CSS, and JavaScript being used in designing a responsive frontend, a RESTful service provided by spring boot at the backend level, and finally MySQL database. Role based access control will be used for managing rights of administrators and departmental officers like RTO, IT, Voting, and Ration.
Keywords — White Card, Identity Management, QR Code, Spring Boot, MySQL, JWT Authentication, E-Governance.

I. INTRODUCTION

Identification verification assumes great importance in modern service delivery mechanisms. For instance, in most nations, people are supposed to hold multiple identity documents in order to access services from both the public and private sectors. These documents include Driving License, PAN card, Voter ID, and ration cards. The problem with having multiple identity documents is that these papers have been designed for different purposes. Therefore, there is a lot of inefficiency in the system due to this fragmented identity system.

Some of the problems that come with having multiple identity documents include inconveniences associated with carrying many documents, loss of documents, data duplications, and problems with verifying information among others. Besides being inefficient, this approach exposes organizations to greater risks of fraud and inefficiencies. Verifying people's identities in manual ways is cumbersome and may lead to data discrepancies. In the age of technology, there is a great need for an improved identification verification process.

Inorder to address the aforementioned issues, this paper recommends adopting the White Card System, which provides citizens with a single electronic identity solution that integrates all sorts of identity proofs into one entity. Under the proposed framework, each individual is assigned a unique 12-digit White Card ID number along with a PIN and QR code. The QR code includes the necessary identity details and is capable of being decoded by any smartphone to make verification process quick. Moreover, there will be less involvement of physical documents in such a system.

The implementation of White Card ID will involve adoption of the concept of role-based access control mechanism wherein government departments like RTO, IT, Elections commission, Ration, etc. have access to limited information of an individual. This mechanism is quite helpful to ensure both the security as well as efficiency of the entire process. Modern technologies such as Spring boot, MySQL, and web technologies shall be used.

This research aims at developing a strong, flexible, and friendly Identity Management System that will help in simplifying the process of verification, decreasing administrative cost and increasing the level of security. The use of this system as an effective tool of identity management helps in contributing to the development of digital government.

II. LITERATURE REVIEW

The fast evolution of digital technologies is having a profound impact on the advancement of the IDM system in e-governance. Several researchers have advanced various ideas about improving ID verification, data protection and accessibility. Below, important publications related to digital IDs, QR codes, RBAC system, and secure API communications are reviewed.

Sharma and Patel (2022) suggest a blockchain based system for managing digital identities as an effective solution for data security, immutability and integrity. The authors use distributed databases that cannot be tampered with as the main advantages of their solution. Despite that, this technique would be rather complicated and costly, so there might be

difficulties in its deployment by governments.

In turn, Kumar and Reddy (2023) discuss the problem of implementing RBAC in government websites using Spring Boot. The authors emphasize the importance of securing access to government data by applying a special permission structure depending on the user's role in a particular system. As a result, the latter one would be able to use only such resources that pertain to him. Nonetheless, the article discusses access control systems only, and does not provide any methods of combining several identity proofs.

Mehta and Gupta (2021) have worked on various options of e-governance in rural India. The authors emphasize issues such as the need for infrastructure, digital literacy, and system interoperability. According to their results, centralizing government systems can greatly benefit the process of efficient service delivery provided that such systems are simple and scalable. Yet, their research offers no actual framework for implementing a centralized identity.

Raghavan and Suresh (2023) focused on applying JWTs (JSON Web Tokens) for stateless authentication in RESTful APIs. JWTs allow one to establish secure token-based communication with minimal server memory usage. However, this method cannot be used to consolidate identity and facilitate data sharing within departments. Overall, this article addresses the issue of authenticating users but does not deal with their identity.

Apart from those examples, there have been attempts to implement the QR code-based authentication process, which can be used to quickly authenticate the identity of users by encoding relevant information into a code that can be easily scanned and decoded. Although such an approach allows fast, contactless, and reliable authentication with a standard smartphone, its application is usually limited to particular applications.

Nevertheless, current systems mostly work independently, targeting specific areas such as security, access control, or verification time. There is no system that integrates all these elements, including different identity proofs, secure authentication, and role-based access.

The new White Card system can be seen as a breakthrough in this area because it combines all the above-listed functions in one system. It includes the advantages of current systems, such as QR code verification, JWT authentication, and RBAC, but it differs significantly from all previous attempts to create a system of this kind because it unites all government IDs into one digital record.

III. PROPOSED SYSTEM

In order to counter the above-mentioned disadvantages of existing identity management schemes, the proposal for the implementation of the White Card system is presented in the following sections of the paper. It is proposed to design the White Card as the most advanced unified digital platform for storing various identity management data. This solution will allow for streamlining the identity management processes, increasing the level of data security, and improving the interoperability across governmental agencies.

One of the fundamental features of the proposed system is the generation of the unique 12-digit code for every citizen – the White Card number. This number will serve as a primary identifier that would link together all identity records associated with a particular individual, such as Driving License, PAN Card, Voter ID, and Ration Card. Moreover, the white card will have its own PIN code, which will consist of four digits.

It is worth noting that QR code technology can be incorporated in the proposed platform, and a specific QR code will be generated for each White Card. This code will include the number and additional authentication data, which can be quickly decoded through any device capable of reading QR codes or via mobile application.

This application follows the principle of Role-Based Access Control (RBAC) in which only the information relative to user roles in the system will be accessed by them. The two primary types of user roles are as follows:

- **Administrator:** Controls the whole process from issuing new cards to updating existing ones, registering officials from different departments, and monitoring the status of the cards that were issued.
- **Departmental Officers:** Officials from departments including Regional Transport Office (RTO), Income Tax (IT), Voting, and Ration. Departmental officials would be able to access the portal and access information about their department only.

For example, an RTO officer would be able to view the details related to all driving licenses that have been registered through this portal while the income tax department official would only be able to view the PAN card details of the citizens among others.

This proposed software application is built based on three-tier architecture in which there are three separate layers as mentioned below:

1. **Presentation Layer (Front-end):** Built using technologies like HTML, CSS, JS, and Bootstrap.
2. **Application Layer (Back-end):** Application Layer consists of Spring Boot for building RESTful APIs.
3. **Data Layer (Database**): Consists of MySQL Database and Hibernate Framework.

It is crucial for the proposed design to be secure. It uses JSON web token-based authentication to make sure that there is a safe connection between the server and the client. Also, the system utilizes password hashing with BCrypt. Moreover, the system can leverage multi-layer security by means of QR code authentication, PIN authentication, and access control by roles.

The work flow of the system consists of the following. The first step includes issuing a White Card by the administrator. The system generates automatically a QR code, PIN, and a number for the card. After that, the administrator updates corresponding identity records. At the stage of verification, the officer will scan the QR code and enter PIN, after which the system will display relevant data according to the officer's role.

Thus, one can conclude that the White Card System proposed is a reliable and secure centralized platform for managing identity records.

IV. SYSTEM DESIGN

White Card System is meant to be a centralizing digital platform for managing and consolidating various identities through one system. This design is intended to be scalable, secure, modular, and user-friendly. The whole design entails the structure of the system architecture whereby different modules perform different roles towards the management and verification of identities securely.

The total system design can be categorized under the following four categories: System Architecture, Module Design, Data Flow Design, and Database Design. These designs ensure smooth interactions between the user and backend services as well as the database.

A. System Architecture

White Card System follows a three-tier architecture approach that comprises Presentation Layer, Application Layer, and Data Layer. Three-tier architecture improves the system's maintainability by splitting various parts into separate layers.

HTML, CSS, JavaScript, and Bootstrap are used to code the Presentation Layer. It generates responsive web pages for Admin and Officer Users. Presentation Layer includes login pages, dashboard pages, white card creating pages, updating pages, and verification pages.

Spring Boot Framework is employed in coding the Application Layer. REST API, Services, Authentication, logic of generating QR Codes, and Role-based Access Controls form part of Application Layer that receives the request from the front end and processes it through the database.

MySQL Database is employed in the Data Layer, where the information of Citizens, Officers, White Cards, QR Code Reference, and Departments such as Driving License, PAN, Voter ID, and Ration Card is stored.

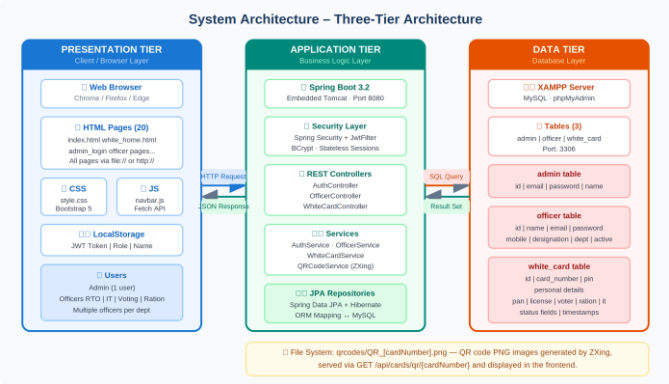

Fig. 1 Three-Tier System Architecture of White Card Application

B. Module Description

White Card System consists of multiple modules to facilitate processes and to ease maintenance**.**

- ***Admin Module:*** The Admin Module oversees the management of the entire system. The administrator can perform actions such as registering officers, creating White Cards, updating citizen information, and checking the status of the identity proofs offered by citizens. The administrator serves as the authority for the White Card System.
- ***Officer Module:*** The Officer Module offers the departmental officers an opportunity to login and check the information of citizens in their respective departments. Only officers from the RTO, IT, Voting, and Ration departments have access to specific information relevant to their departments.
- ***White Card Module:*** The White Card Module assigns each citizen a unique 12-digit card number, a secure PIN, and a QR code. The White Card Module incorporates multiple identity proofs into one single record for a citizen.
- ***Verification Module:*** The Verification Module provides the officer with the opportunity to scan the citizen's QR code and enter their PIN to gain access to the citizen's information.
- ***Security Module:*** The Security Module secures the White Card System with the help of JWT authentication, BCrypt password encryption, and role-based access control.

C. Dataflow Diagram

DFD is the flow of data in the White Card system. This depicts the manner in which the data is processed in the system and stored in the database.

The user provides input data by filling the form through the frontend. Once validation takes place at the backend, the data is stored in the MySQL database. When card production is complete, a QR code and PIN are generated in the system.

The QR code is scanned by the departments' officials along with the PIN so as to view the necessary details of the citizen in the system. The backend extracts the information from the database and allows viewing of department-related information only.

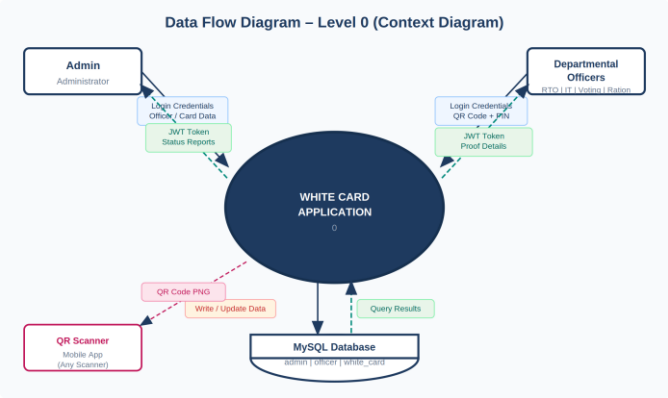

Fig. 2 DFD Level 0 (Context Diagram)

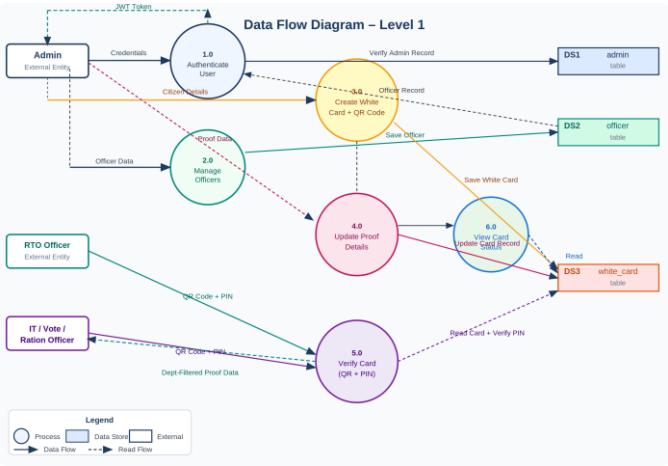

Fig. 3 DFD Level 1 (Detailed Process Flow)

D. Entity Relationship Diagram

The Entity Relationship (ER) Diagram depicts the database architecture and relationship of entities in the database system.

The significant entities in the white card system consist of:

- Admin
- Officer
- White Card
- Driving License
- PAN Details
- Voter Details
- Ration Details
- IT Return Details

The white card entity serves as the central entity that helps connect all the information specific to the departments by making use of the unique card number. An officer is associated with a particular department. Relationships are made by means of the primary and foreign key constraints.

The ER diagram helps maintain well-organized data management and minimize redundancy in the data.

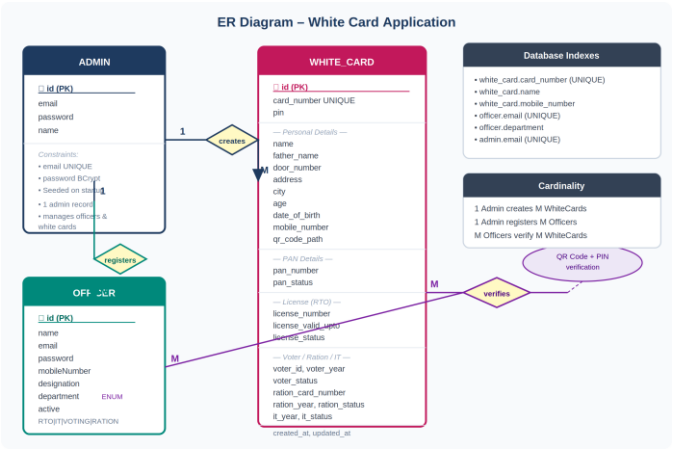

Fig. 4 ER Diagram

V. IMPLEMENTAION

A. Frontend Implementation

The frontend part of White Cards system has been created using HTML, CSS, and JavaScript technologies with Bootstrap framework. It enables a responsive and intuitive interface that works well for Admin and Officer users. It consists of pages of login, dashboard, creation of White Card, updates about details of card, QR verification, and status view. JavaScript technology was used for implementing form validation, making requests to API and processing data.

B. Backend Implementation

Backend implementation of the project has been done based on the use of Spring Boot framework. It performs all necessary activities and implements business logic related to creation of White Cards, generation and verification of QR code. Communication between the server and clients is implemented with JWT-based authentication and role-based restrictions on actions performed by users.

The backend provides APIs for:

- User authentication
- Officer registration

- White Card creation
- Identity detail updates
- QR code verification
- Status management

C. Database Implementation

For the implementation of the database, MySQL is used as the database that stores all the information of the application. The database consists of tables like Admin, Officers, White Cards, as well as other specific departments such as Driving License, PAN, Voter ID, Ration Card, and IT.

VI. RESULTS AND DISCUSSION

The White Card System was evaluated using samples of citizens and officers to analyze the performance of the system, its accuracy, speed of response, and role-based access. During the testing phase, the whole process from start to finish of the application was analyzed. This includes the generation of the White Card, QR Code, officer verification, and management of statuses.

The deployment of the system was done locally using XAMPP server and MySQL database with Spring Boot backend. Different test scenarios were used for testing.

A. Dataset Description

System testing was conducted for the White Card System with the help of sample citizen and officer data to check the performance, accuracy, time taken by the system to generate response, and role-based access control. A. Sample Data Set

The test data used in this project contains:

- 50 Citizen Test Records
- 4 Department Officers
- 4 Types of Identities
- Driving License
- PAN Card
- Voter ID
- Ration Card

Each record has the following details:

- White Card Number
- Personal Information
- PIN Number
- QR Code
- Identity details from respective department

TABLE I
SAMPLE DATASET

White Card No	Name	Department Verified	Status
288786437846	Rubinson	RTO	Approved
562378945612	Arun Kumar	IT	Processing
891245673421	Priya	Voting	Approved
781234567890	Karthik	Ration	Rejected
671245983214	Divya	RTO	Approved

B. Functional Testing Outcome

Functional tests were conducted for all major features of the system. Below is the recorded outcome.

TABLE III
FUNCTIONAL TESTING RESULTS

Module	Test Case	Expected Result	Actual Result	Status
Login Module	Admin Login	Dashboard opens	Successful	Pass
Officer Module	Officer Login	Officer Home displayed	Successful	Pass
White Card Creation	Create New Card	QR and PIN generated	Successful	Pass
QR Verification	Scan QR + PIN	Citizen details shown	Successful	Pass
Update Module	Update DL Details	Database updated	Successful	Pass
Status Module	Change Verification Status	Status updated	Successful	Pass

From the test outcome, it can be seen that all major system components executed successfully without any error.

C. Performance Analysis

System performance tests were conducted using response time when creating cards, verifying cards, and accessing database information**.**

TABLE IIIII
AVERAGE RESPONSE TIME

Operation	Average Time
Login Authentication	1.2 seconds
White Card Creation	2.4 seconds
QR Verification	1.5 seconds
Data Retrieval	1.1 seconds
Status Update	1.3 seconds

It can be observed from the results that the system operates very quickly in executing most of its functions.

D. Graph Test

Below is a graph that shows the efficiency of various system modules.

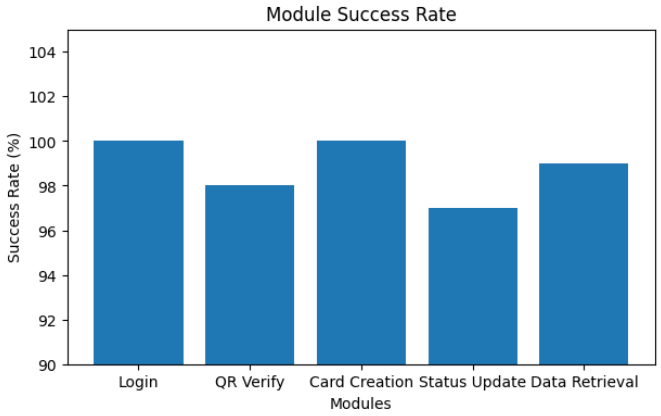

Fig. 5 Module Success Rate

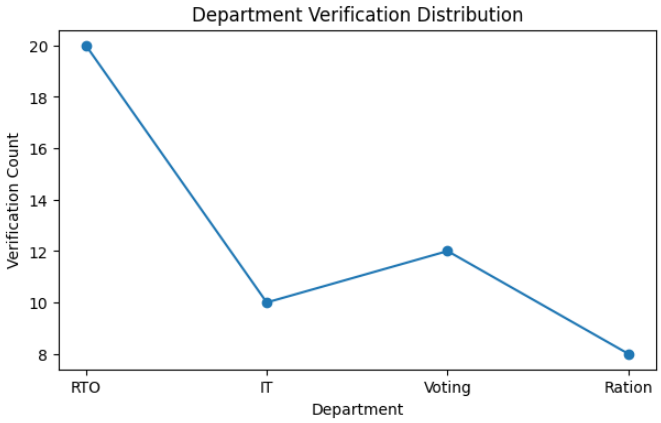

Fig. 7 Department Verification Distribution

From the graphs, it can be observed that the system operates efficiently in verifying identity cards.

E. Discussion

From the above results, it is clear that the White Card System has been implemented successfully as it incorporates various identity cards into one single platform. The use of QR code verification reduces the manual work and makes the process efficient. The RBAC model provides safe and departmentalized data access.

The frontend was user-friendly as the navigation and form filling were dynamic. Handling the API calls, authentication of users and communication with the database was done using Spring Boot. The database used was MySQL which provided the structured storage and quick retrieval of the database.

The performance of the system was satisfactory as there was low response time and successful verification. JWT authentication and BCrypt hashing algorithms were used to ensure the safety and integrity of the system. Therefore, the results obtained show that the White Card System will be able to perform as required.

VII. ADVANTAGES AND LIMITATIONS

A. Advantages

- Unified Identity Management System: A White Card solution that combines several identity documents like driving license, PAN card, voter ID, and ration card.
- Efficient Data Retrieval Process: Efficient access to the data via QR code and PIN.
- Role-Based Access: Each official gets access to the information available only within respective department.
- Reduction in Paperwork: The necessity of carrying various types of physical identity is decreased.
- Unified Database Management: All types of identity data can be managed using a single platform.
- Enhanced Security Features: Authentication and password encryption increase system security.
- Friendly User Interface: Responsive interface helps officers as well as admin to navigate through the platform easily

B. Disadvantages

- Dependence on the Internet: Internet connection must be there for using features offered by the system.
- First-time Complications: Merging all types of identity databases into one database might be a difficult task at the beginning stage.
- Privacy Risks: Centralization of all identity data calls for proper privacy measures.
- Difficulties in Implementation: Proper implementation on a large scale requires proper optimization.
- Infeasibility of Offline Functioning: Access to data via QR code is impossible offline.

VIII. FUTURE ENHANCEMENTS

In order to make the White Card System more efficient, it is necessary to incorporate some technological advancements as well as other government services into the system.

- Development of Mobile Application: It will be a good step to develop a mobile application, which allows easy scanning and verification through mobile phones.
- Use of Blockchain Technology: The use of blockchain technology can also be made to enhance security as well as transparency of the system.
- Use of Biometrics: Fingerprinting and facial recognition technologies can also be adopted to secure the White Card System.

- Use of Cloud Technology: Cloud technology can be useful in improving scalability and efficiency of the system.
- Artificial Intelligence Techniques: AI techniques could be used to counter the problem of fraud in the White Card System.
- Integration with National Identity Cards: White Card System can also be integrated with other services such as Aadhaar.
- Regional Language Interface: Support for regional languages can be provided in the system.
- SMS and Email Services: SMS and emails could be provided to alert users regarding important information.

IX. CONCLUSIONS

The White Card System is an effective and reliable system for managing the digital identity through combining multiple identity proofs into one system. In addition, the process of identity verification is easy because of the employment of QR-code and PIN-number authentication, which eliminates the necessity of having many different documents for this purpose.

It is important to note that role-based access control is employed in order to limit the availability of information depending on the role of department officers, which positively impacts on the overall privacy and security of data. It should be noted that the system employs the technologies such as Spring Boot, MySQL, JWT authentication, and responsive web interfaces.

Testing has shown that the app works efficiently in terms of card creation, its verification, and secure retrieving of necessary data with small amount of response time. Overall, it can be said that the White Card System has the potential to increase efficiency in managing information and performing routine administrative tasks.

REFERENCES

[1] Sharma, A., & Patel, R., "Unified Digital Identity Management Using QR Codes and Blockchain," International Journal of Computer Science and Information Technology (IJCSIT), Vol. 14, No. 3, pp. 45–58, 2022.

[2] Kumar, S., & Reddy, N., "Role-Based Access Control in Government Web Applications: A Spring Boot Approach," Journal of Software Engineering and Applications (JSEA), Vol. 16, No. 5, pp. 112–128, 2023.

[3] Mehta, P., & Gupta, V., "E-Governance Solutions for Rural India: Challenges and Opportunities," Indian Journal of Computer Science and Engineering (IJCSE), Vol. 12, No. 2, pp. 78–91, 2021.

[4] Raghavan, K., & Suresh, T., "JWT-Based Stateless Authentication for RESTful APIs: Security Analysis and Best Practices," International Journal of Web Engineering and Technology (IJWET), Vol. 8, No. 1, pp. 22–35, 2023.

[5] Craig Walls, Spring Boot in Action, 2nd Edition, Manning Publications, 2022.

[6] Welling, L., & Thomson, L., PHP and MySQL Web Development, 6th Edition, Addison-Wesley, 2022.

[7] Ullman, L., MySQL: Visual QuickStart Guide, 2nd Edition, Peachpit Press, 2012.

[8] Flanagan, D., JavaScript: The Definitive Guide, 7th Edition, O'Reilly Media, 2020.

[9] Spring Boot Official Documentation. Available: https://spring.io/projects/spring-boot

[10] MySQL 8.0 Reference Manual. Available: https://dev.mysql.com/doc/refman/8.0/en/

[11] Bootstrap 5 Documentation. Available: https://getbootstrap.com/docs