Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

The Integrated Digital Platform for Managing Patient Records (IDPMPR)

Sneha S. Ashtankar[1], Moiz Hussain[2], Bhavesh C. Zade[3], Manish M. Khawas[4], Mansi M. Mahale[5] and Piyush Meshram[6]

[1] Prof. Department of Computer Technology, KITS Ramtek, INDIA
[2,3,4,5,6] Department of Computer Technology, KITS Ramtek, INDIA

Abstract
A safe and effective hospital system that is integrated in the field of digital healthcare management is urgently needed. In this paper we propose The Integrated Digital Platform for Managing Patient Records (IDPMPR) - a web-based hospital management system. It aims to overcome weaknesses of manual health service administration. Secure data processing, automatic scheduling, and the ability to view medical records in real time simplify how patients, doctors, receptionists and administrators work. For password encryption, this application uses bcrypt, it utilizes JSON Web Tokens (JWT) for authentication and Blockchain as the immutable record storage. The platform security is further strengthened by automatic session expiration and single-device login enforcement. The platform, which was built with React.js, Node.js, Express.js, and MySQL, it provides a user-friendly, scalable, and responsive interface.

Its performance was confirmed by testing, which showed strong, robust access control, data integrity, and low latency. The system improves identity verification and reduces password vulnerabilities with QR code-based authentication. IDPMPR creates a strong basis for upcoming developments, such as AI-driven diagnostics, IoT-enabled health monitoring, and telemedicine integration, despite its reliance on reliable network connectivity. This promotes a more intelligent and accessible digital healthcare ecosystem.

Keywords: Hospital Management System, Secure Authentication, Patient Data Management, Role-Based Access Control, Healthcare Analytics.

1. Introduction

Healthcare worldwide is experiencing a dramatic and pressing transformation into a digital healthcare environment; due to the urgent requirement for the safe, efficient and timely management of very sensitive medical information. Traditionally, hospitals have managed clinical information using paper based methods and laborious manual methods; however both of these traditional methods possess significant shortcomings, notably data loss and fragmentation, delayed diagnosis and retrieval and significant risk to patient confidentiality.

A digital platform for managing patient records is developed to address the critical operational and security issues identified through the development of this project and provides a single, secure digital platform that supports multiple user roles (patients, doctors, receptionists and administrators). A unique

feature of the digital platform is the inclusion of blockchain technology to enable the secure, tamper proof and immutable storage of medical records to meet regulatory and auditing requirements. To further enhance the integrity of the data stored on the platform, a multi layered security architecture is employed that includes end to end encryption of sensitive data, bcrypt hashing to protect user credentials, and secure authentication of users through JSON Web Tokens (JWT) that automatically expire after a predefined time period. Additionally, the platform employs role based access control (RBAC) [1], to restrict the functionality available to each user based upon their assigned role, and the platform utilizes several additional features to provide enhanced security to users, including secure QR code scanning for enhanced login and retrieval of clinical information, and mandatory certification of doctor's authenticity prior to accessing patient records [2].

2. Literature Review

The platform's architecture is built on the advances of current research and intellectual property regarding healthcare informatics security, e.g., access control for role based access to system, secure identity authentication as well as data integrity mechanisms, QR code technology for efficient data access and which all collectively improve system design

.

2.1 Role-Based Access Control Authentication

The Technology's architecture is based on strong principles of Role Based Access Control (RBAC). RBAC restricts the level of access granted to users based upon their role within the hospital: Admin, Doctor, Receptionist or Patient. Secure identity authentication is achieved in part through JSON Web Tokens (JWT) which enforce an organization's authorization policy and provide a means of managing the security of user sessions. The structure for secure access control is also inspired by a concept called Hierarchical Trust RBAC (HT-RBAC) which allows for dynamic tailoring of access rights [1].

2.2 Secure QR Code Technology

The Secure QR Code (SQR) technology serves as an important security mechanism. Through the use of QR Code technology, the system mitigates the risks associated with using traditional password-based authentication techniques such as brute-force and phishing attacks. In designing the system, I drew from a number of studies that propose creating cryptographic frameworks to integrate AES encryption with access control limitations so that sensitive medical information such as electronic prescriptions and reports will only be able to be accessed through codes that have been digitally signed and encrypted thereby preventing forgery or modification [2] [3].

2.3 Mechanism and Protection of Data Integrity

The platform utilizes state-of-the-art security technologies, including but not limited to several proposed methods for safeguarding sensitive patient information in a cloud computing environment. The major aspect of innovation with the platform is the ability to utilize blockchain technology to store medical records in an immutable state and provide compliance and audit capabilities. In addition to the uses of blockchain technology. To prevent unauthorized access to the user's credential, the platform will store the password using a bcrypt hash [4].

3. Methodology and Proposed Approach

The platform is a comprehensive integrated digital solution that will provide a singular, unified and secure framework to facilitate all healthcare operations in one place.

3.1 Centralized Data Storage with Secure Patient Records

All patient-related data (demographic, medical, and scheduling) will be stored in a central database. This database will utilize an architectural structure based on blockchain technology that will allow for immutability and an audit trail, making any unauthorized changes to the patient data unfeasible.

3.2 Role-Based Access Control and Session Management

The platform has adopted an improved police and procedures for managing user responsibility by utilizing an enhanced Role-Based Access Control (RBAC) model. The RBAC Model will offer:

- Administrator (Admin): Centralized governance over the system and user accounts (creation, activation and deactivation) and user's ability to view analytics of their responsibility to the system.
- Doctor: Access to patient's records once the user has verified their certification as a Doctor (after verification of the Doctor's professional credentials) can provide all records necessary for patient appointments, manage the schedule of doctors and issue digital prescriptions.
- Receptionist: All schedules will be managed by the Receptionist, who will also assist with patient registration and any other duties assigned by the Administrator .
- Patient: Book appointments and view/download prescriptions electronically, total Medical records, and other records are confidential.

3.3 Secure Authentication Mechanisms

This system has several layers of authentication to replace the traditional weak logon methods.

i. Password Security: The system uses bcrypt to hash passwords, which provides added security. The passwords can be regenerated through email verification link.
ii. Doctor Verification: When doctor logs in each time, the doctor certificate is validated, their unique certificate number is used to verify their authenticity to access patient data.
iii. QR-based Access: Secure QR codes will allow a more efficient method for Authentication and provide secure access to sensitive reports and other activities that are more appropriate.

3.4 Prescriptions and Appointments Workflow

The system provides an Integrated Module for easy access to appointment booking based on the availability of the doctor. After the consultation, the doctor generates a digital prescription and stores it securely, allowing the patient to download directly from the system, eliminating the need for paperwork. All diagnostic reports are also uploaded securely and shared between the patient and doctor digitally to create a Comprehensive Digital Medical Record.

4. System Design and Architecture

The architecture has been designed to allow for scalability, increased security, and improved functionality for all aspect of the project.

4.1 Dataflow Diagram (DFD) Overview

The Data Flow Diagram (DFD) shows how information is transferred between outside entities (Users, External Triggers) and Core Validation Processes. When a User logs in, their data flows into the Authentication System; that System then assigns Role-Based Access Control (RBAC) and Session Management permissions based on the User's role. Only those inputs that have successfully passed a Validation, Authentication, and Authorization process are passed into the Database Management and File Generation processes (PDFs for Prescriptions and QR Codes), all maintained with traceability through System Logs.

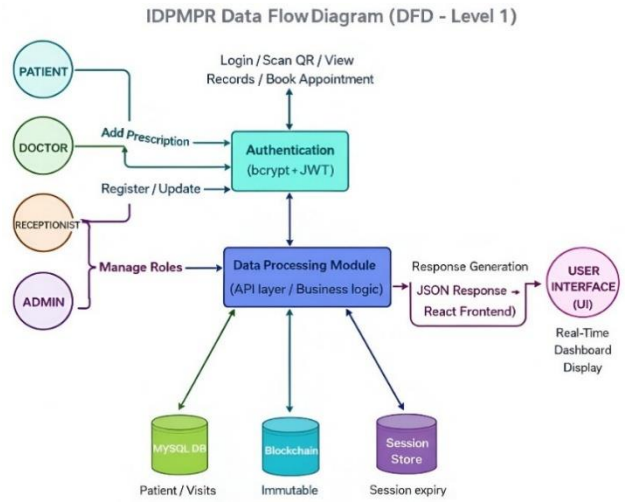

Fig.1. Data Flow Diagram

4.2 Architectural Layers

i. Presentation Layer: React.js and Tailwind CSS have been used to create a responsive, interactive, and user- friendly experience that works across devices including desktop computers, tablets and smartphones.

ii. Application Layer: Application Layer is managed within Node.js and Express.js and represents the core of the application's business logic and function process. This layer also manages routing, API creation, and session control, and provides implementation of Access Policies through the services of the API Gateway.

iii. Database Layer: All data is securely stored within the MySQL relational database for structured data (Users, Appointments, and Schedules & Prescriptions). In addition, the Database Layer has optional NoSQL Databases for storing dynamic data such as logs and Analytics. Blockchain storage is integrated for immutable medical data entries.

iv. Security Layer: The Security Layer includes the implementation of JWT, RBAC, and User Session Expiry for Single-Device Login, Idle User Session Timeout/Logout, and the use of AES Encryption Method for all End-to-End communications.

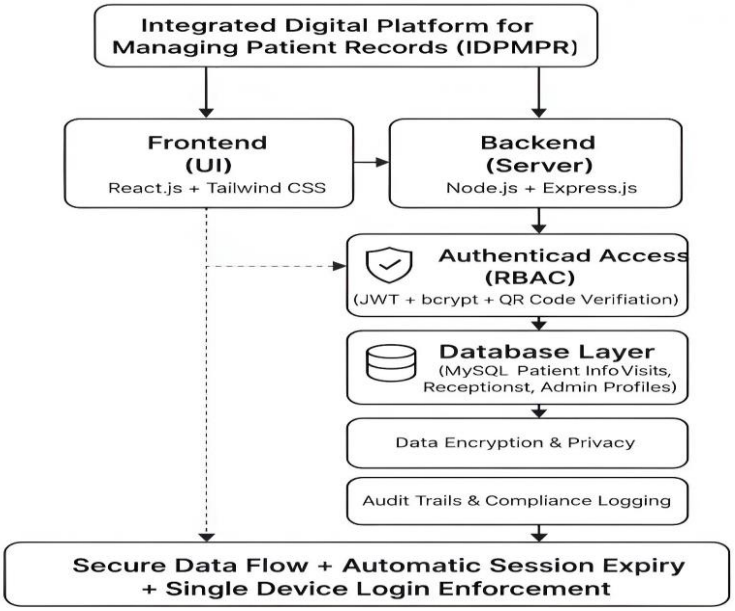

Fig.2. System Architecture

4.3 Entity-Relationship (ER) Diagram Overview

The data structure of the database encompasses the following major entities:

- Users (including Admins, Doctors, and Receptionists) and Patients contain both Core Identification and Role Data.
- Appointments contain patient ID and doctor ID to track the status of appointments.
- Doctor Schedules and Availability specify recurring and specific dates for appointments to ensure efficient Booking Management.
- The Prescription connects Doctors and Patients with Prescription Medicines, forming a one-to-many connection for Detailed Clinical Output.

5. Implementation and Technology Stack

5.1 Frontend

Frontend will be built using React.js to create reusable components to present the user interface for our application. The advantage to using the Virtual DOM is the browser will be able to render each of the components, optimizing the performance as it does so. Responsive design and a professional appearance will be accomplished using Bootstrap styling and Tailwind CSS. JavaScript to incorporate interactivity, validate all forms delivery notification messages, and perform the calls to our API using a REST protocol.

5.2 Backend

The backbone of our backend of our application will be Node.js JavaScript and the Express.js framework. Express.js is an excellent framework for handling multiple simultaneous requests and for implementing all of the business logic for our application. There are REST API endpoints for each of the CRUD functions for patient records, appointments with physicians, and prescriptions. Express.js middleware will enforce input validation, check the validity of the access tokens (JWT), and control resource who has access to them.

5.3 Data and Database Management

We will use MySQL as the database to hold structured data whose referential integrity is to be maintained by the primary and foreign key paradigm. The management of "unstructured data", like analytics logs and session information, will happen in a separate NoSQL Database. The treatment of critical patient records as immutable will be secured by the Blockchain Storage module. Interaction with the database will only be possible through APIs, guaranteeing a secure interaction with our database.

5.4 Security and Authentication Implementation

We will secure our application with the following:

- Token-Based Authentication (JWT): Will be implemented for the stateless session and security feature implementations such as single-device logins etc.
- Encryption: To be used for sensitive data, leveraging AES to encrypt the data at rest as well as secure protocol transmission
- Role-Based Access: (HT-RBAC) which ensures roles can only reach the data according to the permission levels across all four user roles [1].
- Secure QR Verification: Will use Node.js QR Code libraries to generate and authenticate secure QR codes for instantly authenticating logins and access to medical reports. [2]

6. Result and Discussion

6.1 System Functionality, Performance, and Analysis

The platform is designed for all roles and includes comprehensive role-based functionality, as well as dependable operation and efficient flow of operation through the use of the system. Patients have the ability to schedule visits through the system and retrieve their information from their medical records; physicians use the site to administer their patients' pharmaceuticals and to organize their appointments with patients and, with administration console the administrators can manage the user accounts and access to analytics dashboards.

6.2 Security Evaluation

Evidence of the success of the multi-layer security model has indicated that it was robust. Blockchain technology was successfully integrated into the platform to provide reliability and tamper-proof data trail verification of critical health records, thus establishing high levels of trust and auditability. The authentication component of the system used a combination of technologies such as JWT, bcrypt, and QR code verification to ensure protection against credential theft and session hijacking.

6.3 User Experience and Usability

According to users' feedback, the overall user experience and usability of the platform met with a high level of user satisfaction. Users indicated a high degree of usability based on the SUS score of the platform due to the ease of navigating through the intuitive interface of the platform and the quickness of information retrieval from multiple devices.

7. Conclusion and Future Work

"The Integrated Digital Platform for Patient Record Management is designed to provide privacy and

security for patient information and to efficiently consolidate the multiple workflows involved in both Administrative and Clinical aspects.

7.1 Limitations

Although the platform has made significant advancements in health record management, several limitations still exist. Specifically, the platform is dependent on having reliable internet access to provide real-time updates and synchronization of patient's records. Another limitation is that the caregivers and patients must be adequately trained to use the platform in a way that demonstrates digital literacy. In addition, while the platform is designed to provide a means of communicating with other National Electronic Health Record (EHR) frameworks, the entire interoperability process has yet to be completed.

References

1. C. Pasomsup and Y. Limpiyakorn, "HT-RBAC: A Design of Role-based Access Control," in 2021 International Conference on Big Data Engineering and Education (BDEE), Guiyang, Guizhou Province, China., 2021.
2. H. A. M. Wahsheh and M. S. Al-Zahrani, "Secure and Usable QR Codes for Healthcare Systems: The Case of Covid-19 Pandemic," in 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021.
3. S. Dutta, S. Singh and P. Ghodke, "Secure Login System Using QR-Image," International Journal of Computer Applications Technology and Research.(ISSN: 2319–8656), vol. 8, no. 1, pp. 1-3, 2019.
4. S. Shinde, R. Shinde, S. Zanje, S. Bidgar and P. C. Deshpande, "Patient Report Management System," International Research Journal of Modernization in Engineering, Technology and Science, vol. 5, no. 11, p. 1831–1834, 2023.