IT313 G15

Functional Requirements:

User Registration and Authentication:

- Users (patients, doctors, receptionists, admins) must be able to register and log in with unique usernames and passwords.
- Passwords should be securely stored using hashing and salting techniques.

User Roles and Permissions:

- Define different user roles (patient, doctor, receptionist, admin) with distinct permissions and access levels.
- Admins should have the authority to assign roles and permissions.

Patient Management:

- Patients can create, update, and view their profiles.
- Patients can access and update their medical history, including diagnoses, prescriptions, and treatment records.

Doctor Management:

- Doctors can create, update, and view their profiles.
- Doctors can view their appointment schedules and manage appointments.

Receptionist Functions:

- Receptionists can schedule and reschedule appointments for patients.
- Receptionists can access patient records and administrative tasks.

Admin Functions:

- Admins can manage user roles and permissions.
- Admins can configure system settings and monitor system usage.

Appointment Management:

- Patients can schedule appointments with available doctors.
- Doctors can view and manage their appointment schedules.
- Receptionists can manage appointment inquiries and reschedule appointments.

Medical History Access:

- Patients can access their medical history, including diagnoses, prescriptions, and treatment records.
- Doctors can access and review the medical histories of their patients.

Security and Access Control:

- Implement security measures such as rate limiting, input validation, and role-based access control (RBAC) to protect user data and system resources.

Non-Functional Requirements:

Performance:

- The system should respond to user requests within a reasonable time frame.
- It should support a scalable architecture to handle an increasing number of users and data.

Reliability:

- The system should be available and reliable, with minimal downtime.
- Data integrity should be maintained to prevent data loss or corruption.

Security:

- User data should be stored and transmitted securely using encryption.
- Implement protection mechanisms to guard against common security threats (e.g., SQL injection, cross-site scripting).

Usability:

- The user interface should be intuitive and user-friendly.
- Provide clear and concise instructions for users.

Scalability:

- The system should be designed to accommodate future growth by easily adding more users, doctors, and patients.
- Scalability should be achieved without significant performance degradation.

Compatibility:

- Ensure compatibility with various web browsers and devices to allow users to access the system from different platforms.

Monitoring and Logging:

- Implement monitoring tools to track system health and performance.
- Maintain logs of user activities and system events for auditing and troubleshooting.