Contents

1. Introduction

1.1 Purpose

This document outlines the functional and non-functional requirements for the development of an Online Examination System (OES) designed for secure and efficient standardized test management within a government organization. The OES comprises three main components: Admin Panel, Candidate Portal, and Proctoring Module. This document serves as a guide for all stakeholders, including developers, project managers, marketing staff, users, testers, and documentation writers, involved in the system's development and operation.

1.2 Document Conventions

This document follows standard software documentation conventions

- **Text Styles**:
  - **Bold Text**: Represents section headings and key terms.
  - *Italicized Text:* Used for emphasis and examples.
- **Requirement Notation**:
  - Functional requirements are labeled as **FR-n**
  - Non-functional requirements are labeled as **NFR-n**.

Manual labeling format for adding new requirements:

- Use a structured numbering system, e.g., *FeatureName-n* where "n" is an incrementing integer.

1.3 Project Scope

The Online Examination System (OES) modernizes standardized testing for a government organization. It replaces paper-based exams with a secure, scalable digital platform, enhancing efficiency, reducing costs, and ensuring exam integrity.

Key functionalities include:

- Admin Panel: Exam creation, scheduling, result management, question bank uploads.
- Candidate Portal: Registration, exam scheduling, online test-taking.
- Proctoring Module: AI-powered features like facial recognition and cheating detection.

The OES offers:

- Real-time monitoring and grading for objective questions.
- Secure handling of subjective question evaluation.
- Scalability to support up to 100,000 concurrent candidates.

1.4 References

This document references the **IEEE Standard 830-1998**: Software Requirements Specifications guidelines.

  - Source: IEEE Standards Association
  - URL: IEEE 830-1998

2. Overall Description

2.1 Product Perspective

Online Examination System (OES) is a new digital platform replacing traditional paper-based testing. It serves the needs of government organizations conducting large-scale standardized exams, offering efficiency, security, and scalability. Though standalone, OES may interface with:

- Machine learning APIs for proctoring.
- Database systems for secure data storage.
- Email/SMS services for candidate notifications.

2.2 User Classes and Characteristics

The Online Examination System (OES) serves several user classes:

- **Administrators**: Proficient with the admin portal, require secure access, knowledgeable about system usage.
- **Candidates:** Varying technical proficiency, need user-friendly interfaces, use various devices (desktop, mobile, tablet).
- **Proctors**: Limited admin panel interaction, familiar with AI proctoring tools, monitor flagged activities.
- **System Administrators**: High technical expertise, access all system modules and logs for troubleshooting.
- **Favored User Classes**: Administrators and Candidates.

2.3 Operating Environment

- **Hardware Platforms**: Desktops, laptops, tablets, smartphones (with webcams and mics).
- **Operating Systems**: Windows, macOS, Linux, Android, iOS.
- **Browsers**: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari.
- **Geographical Locations**: Pakistan, mostly Urban Areas.
- **Software Components**:
    - Machine learning APIs (facial recognition, cheating detection).
    - DBMS (MySQL, PostgreSQL) for secure user/exam data storage.
    - Email/SMS services for candidate notifications.

2.4 Design and Implementation Constraints

- Support peak loads of up to 100,000 simultaneous users.
- Use pre-trained ML models integrated via external APIs.
- Python for backend, ReactJS for frontend to ensure maintainability and compatibility.
- Adhere to data protection and user privacy regulations like GDPR.
- Ensure all libraries and frameworks used are open source or properly licensed.

2.5 Assumptions and Dependencies

2.5.1 Assumptions:

- **Government Regulations**: Compliance with data protection laws *(e.g., GDPR)* is assumed.
- **Security Protocols:** Encryption mechanisms (SSL/TLS) are adequate to protect data.

- **User Device Availability**: Candidates have internet-enabled devices with webcams and microphones.
- **Stable Internet Connection**: Candidates have a stable connection (min 1 Mbps).
- **Data Retention Period**: User data retained for five years, then securely deleted.

- **AI-based Proctoring Reliability**: Machine learning models for facial recognition and cheating detection are effective and accurate.

2.5.2 Dependencies:

- **Machine Learning APIs**: Proctoring relies on third-party ML APIs.
- **Cloud Infrastructure**: Scalable cloud infrastructure for 100K concurrent users.
- **Government Data Protection Laws**: Compliance with current data protection laws.
- **Internet Connectivity**: Reliable internet access for candidates is crucial.
- **Web Browser Compatibility**: Support for modern web browsers.
- **External Notification Services**: Dependence on email and SMS services.
- **Data Center Hosting**: Dependence on cloud-based data centers for hosting.

3. System Features

3.1 Admin Panel

3.1.1 Description

Provides tools for administrators to manage exams, question banks, schedules, candidates, and results. **High priority** for critical admin tasks.

3.1.2 Functional Requirements

- **FR-1: Exam Creation**: Create various question formats and schedule exams.
- **FR-2: Question Bank Management**: Upload, edit, delete, and categorize questions.
- **FR-3: Exam Result Management**: View/download results with interfaces for auto-graded and manual evaluations.
- **FR-4: User Management**: Manage user accounts and roles.
- **FR-5: Error Handling**: Display error messages for invalid inputs and warnings for incomplete setups.

3.2 Candidate Portal

3.2.1 Description

Main interface for candidates to register, schedule, and take exams. **High priority**.

3.2.2 Functional Requirements

- **FR-6: Registration and Profile Management**: Register and update personal details.
- **FR-7: Exam Scheduling**: View available slots and receive notifications.
- **FR-8: Participation**: Access exams within scheduled times with automatic start/end.
- **FR-9: Error Handling**: Display error messages for failed registrations and prevent early/late exam access.

3.3 Proctoring Module

3.3.1 Description

Uses AI for facial recognition and cheating detection to ensure exam integrity. **High priority**.

3.3.2 Functional Requirements

- **FR-10: Facial Recognition**: Authenticate candidates before exams.

- **FR-11: Cheating Detection**: Monitor suspicious activities and alert proctors.
- **FR-12: Real-Time Monitoring**: Stream and record video/audio for exam review.
- **FR-13: Error Handling**: Flag and notify on facial recognition issues and device malfunctions.

3.4 Exam Grading System

3.4.1 Description

Manages grading of objective (auto-graded) and subjective (manual evaluation) questions. **High priority**.

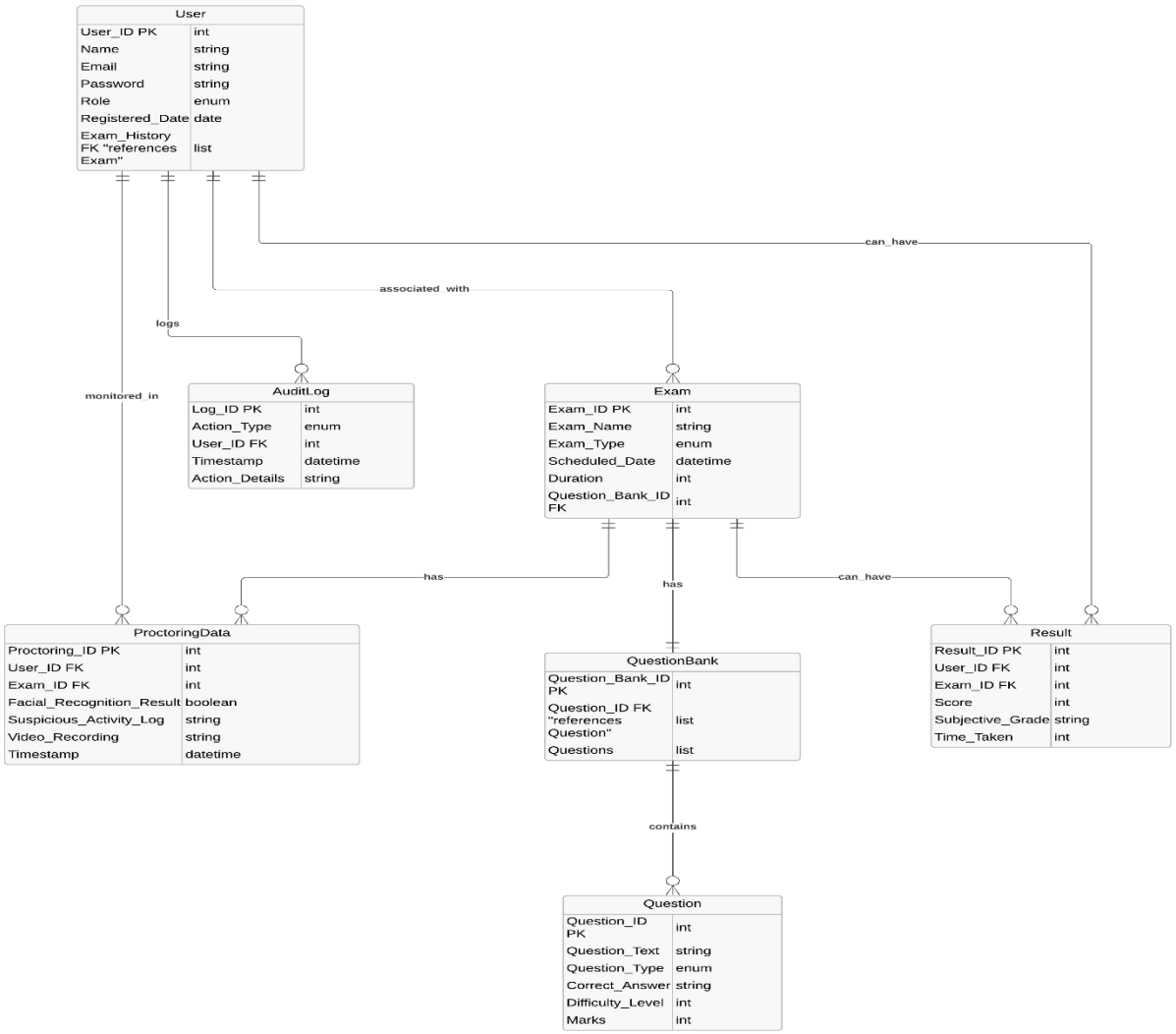
3.4.2 Functional Requirements

- **FR-14: Objective Grading**: Automatically grade MCQs and display scores.
- **FR-15: Subjective Grading**: Allow manual grading with feedback.
- **FR-16: Result Finalization**: Combine objective and subjective scores with manual adjustments.
- **FR-17: Error Handling**: Notify on grading issues and warn on auto-grading failures.

4. Data Requirements

4.1 Logical Data Model

4.1.2 ER-Diagram



4.1.2.1 Appendix B: Analysis Models

Entity-Relationship Diagram (ERD)

Purpose: Represent the relationships among data entities within the OES, providing a visual structure of the database.

Key Entities:

- Users
- Exam
- QuestionBank
- Result
- ProctoringData
- AuditLog
- Question

Relationships

- **User - Exam:** One-to-many relationship (a user can take multiple exams).
- **User - AuditLog:** One-to-many relationship (a user can perform many actions).
- **User - Result:** One-to-many relationship (a user can have multiple results).
- **Exam - QuestionBank:** One-to-one relationship (an exam has one question bank).
- **QuestionBank - Question:** One-to-many relationship (a question bank contains multiple questions).

4.2 Data Dictionary

Entity	Attribute	Data Type	Length/Format	Description
USER	User ID	String	Auto-generated UUID	Unique identifier for the user.
	Name	String	50 Chars	Full name of the user.
	Email	String	Valid Format	User's email address.
	Role	String	Admin/Candidate/Proctor	Role assigned to the user.
Exam	Exam ID	String	Auto-generated UUID	Unique identifier for the exam.
	Exam Name	String	100 Chars	Name of the exam.
	Date	DateTime	DD-MM-YYYY	Scheduled exam date.
	Duration	Integer	Minutes	Total exam duration
Question	Question ID	String	Auto-generated UUID	Unique identifier for the question.
	Text	String	500 Chars	Content of the question.
	Type	String	MCQ/Subjective	Question type.
	Marks	Integer	Range: 0-100	Marks allocated to the question.
Result	Candidate ID	String	Auto-generated UUID	Unique identifier for the candidate.
	Exam ID	String	Auto-generated UUID	Unique identifier for the exam.
	Total Score	float	Up to 2 decimal places	Total score achieved by candidate.
	Rank	Integer	Positive integer	Candidate's rank in the exam.
Proctoring	Proctoring ID	String	Auto-generated UUID	Unique identifier for the proctoring data.
	Suspicious Activity	String	Text	Description of flagged suspicious activity.
Audit Log	Log ID	String	Auto-generated UUID	Unique identifier for the log.
	Action	String	Text	User's action.

4.3 Reports

4.3.1 Exam Performance Report:

- **Purpose:** Show candidate performance.
- **Fields:** Name, ID, Exam, Total Score, Breakdown, Rank, Time.
- **Sort:** Exam Name > Total Score (Desc).
- **Filters:** Date, exam type, score thresholds.

4.3.2 Cheating Detection Report:

- **Purpose:** Flag suspicious activities.
- **Fields:** Name, ID, Exam, Suspicious Type, Timestamp, Status.
- **Sort:** Exam Name > Candidate ID.
- **Total:** Incidents per exam.

4.3.3 Candidate Activity Report:

- **Purpose:** Log candidate actions.
- **Fields:** Name, ID, Action, Date/Time, Exam.
- **Sort:** Candidate ID > Date (Desc).
- **Total:** Exams taken/scheduled.

4.3.4 System Usage Report:

- **Purpose:** Track system performance.
- **Fields:** Exam, Concurrent Users, Max Users, Latency.
- **Sort:** Exam > Concurrent Users (Desc).
- **Total:** Concurrent users per exam.

4.3.5 Audit Log Report:

- **Purpose:** Record system interactions.
- **Fields:** Action, User, Role, Date/Time, Details.
- **Sort:** User Name > Date (Desc).
- **Total:** Actions per user.

4.3.6 Constraints:

- **Formats:** Exportable to PDF, Excel, CSV.
- **Retention:** Data stored for 5 years.
- **Layouts:** Tabular or predefined as needed

4.4 Data Acquisition, Integrity, Retention, and Disposal

4.4.1 Data Acquisition

- **Sources**: Candidate registrations, exam scheduling, exam responses (objective/subjective), and proctoring logs.
- **Initial Setup**: Full import of question banks, user data, and schedules, followed by real-time incremental updates.
- **Frequency**: Real-time updates for registrations, schedules, and logs to ensure data accuracy.

4.4.2 Data Integrity

- **Validation**:
  - Format checks (e.g.*, valid email, unique ID*).
  - Schedule conflict detection.
- **Accuracy Verification**: Periodic checks using techniques like checksums for corruption detection.
- **Backup and Mirroring**:
  - Daily/weekly backups with mirrored copies stored in a separate location.
  - Immutable audit logs for all transactions.
- **Error Handling**: Invalid data is flagged, with entry prevented until corrected.

4.4.3 Data Retention

- **Retention Periods**:
  - Candidate and exam data: 5 years.
  - Proctoring logs: 30 days (deleted for privacy).
- **Temporary Data**: Session-based data is auto-purged after exams.

4.4.4 Data Disposal

- **Deletion Policies**:
  - Secure erasure of expired data, including residual and cached files.
  - Candidate data and exam results permanently deleted after 5 years or upon request.
- **Techniques**: Cryptographic wiping, overwriting, or compliant third-party disposal.

5. External Interface Requirements

5.1 User Interfaces

5.1.1 Admin Panel Interface

- **Layout**: Clean, hierarchical structure with a left-side navigation menu and dropdowns for key categories like exam creation, results management, and question uploads.
- **Buttons**: Standard buttons ("Save," "Cancel," "Submit") consistently located at the bottom or right; "Help" button in the top-right corner.
- **Validation**: Input checks for correct data (e.g., *valid email, non-overlapping schedules*) with immediate error messaging.

5.1.2 Candidate Portal Interface

- **Layout**: Dashboard view showing upcoming exams, results, and schedules; horizontal navigation bar for "Register," "Take Exam," and "View Results."
- **Buttons**: Prominent "Start Exam," "View Schedule," and "Log Out"; "Help" button for instructions and troubleshooting.
- **Notifications**: Alerts (e.g., *exam reminders*) displayed as pop-ups; system messages shown prominently.

5.1.3 Proctoring Module Interface

- **Layout**: Real-time monitoring dashboard with live video feeds, flagged activities, and action logs.
- **Navigation**: Single-page design; key controls ("Mute Candidate," "Flag for Review") in a floating toolbar.
- **Validation**: Notes field restricted to text input; all flagged ctions auto-timestamped and logged.

5.1.4 General UI Guidelines

- **Fonts**: Web-safe fonts (Arial, Helvetica, Verdana); 12px minimum for body text, 14px for headings.

- **Colors**: Blue and white scheme; green for success, red for errors, yellow for warnings; WCAG 2.1 AA compliance for contrast.
- **Shortcuts**: Examples: Ctrl + S (save), Esc (exit/cancel).
- **Resolution**: Optimized for mobile and desktop (320x480 px to 1920x1080 px).

5.2 Software Interfaces

5.2.1 Database Management System (DBMS)

- **Software**: MySQL 8.0 / PostgreSQL 13.x
- **Purpose**: Store and manage data for users, exams, results, and logs.
- **Data Exchange**:
  - **Input**: SQL queries for data management.
  - **Output**: Query results in JSON/XML format.
- **Non-functional Requirements**:
  - Response time: Queries within 2 seconds.
  - Security: AES-256 encryption for sensitive data.

5.2.2 Machine Learning API for Proctoring

- **Software**: Custom API (e.g., *Amazon Rekognition, Microsoft Azure Face API*)
- **Purpose**: Facial recognition and cheating detection.
- **Data Exchange**:
  - **Input**: Webcam feed (JPEG/PNG).
  - **Output**: JSON with recognition data and flags.
- **Non-functional Requirements**:
  - Confidence: 95% accuracy for identification.
  - Response: Results within 2 seconds.
  - Security: HTTPS encryption for data exchange.

5.2.3 Email/SMS Service

- **Software**: SendGrid (Email) / Twilio (SMS)
- **Purpose**: Notifications for exam schedules, reminders, and results.
- **Data Exchange**:
  - **Input**: JSON with recipient details and message content.
  - **Output**: Delivery status (success/failure).
- **Non-functional Requirements**:
  - Delivery: Notifications sent within 30 seconds.
  - Security: TLS encryption for communication.

5.2.4 Security and Encryption Libraries

- **Software**: OpenSSL 1.1.1 or equivalent
- **Purpose**: Encrypt sensitive data (e.g., *passwords, tokens*).
- **Data Exchange**:
  - **Input**: Data for encryption.
  - **Output**: Encrypted data (AES-256/RSA).
- **Non-functional Requirements**:
  - Performance: Operations within 1 second.
  - Compliance: FIPS 140-2 standards for cryptography.

5.3 Hardware Interfaces

5.3.1 Candidate Device Interface

- **Device Types Supported:** Laptops, Desktops, Tablets, Mobile Phones (Android/iOS).
- **Communication Protocols:** HTTP/HTTPS, WebSockets/REST APIs, WebRTC (for proctoring).
- **Inputs:** User actions, webcam/microphone (for proctoring).
- **Outputs:** Web page content, exam data, results, notifications.
- **Timing Issues:** Minimize latency for real-time feedback.

5.3.2 Server Hardware Interface

- **Device Types Supported:** Dedicated Servers or Cloud Instances (AWS EC2, Google Cloud).
- **Communication Protocols:** HTTP/HTTPS, TCP/IP.
- **Inputs:** Requests from client devices.
- **Outputs:** HTML pages, exam data, results.
- **Timing Issues:** Response time under 3 seconds, handle multiple simultaneous requests.

5.3.3 Webcam & Microphone Interface (for Proctoring)

- **Device Types Supported:** USB or built-in webcams and microphones.
- **Communication Protocols:** WebRTC, JavaScript API (getUserMedia).
- **Inputs:** Video (JPEG/PNG), audio (WAV/MP3).
- **Outputs:** Real-time data for proctoring.
- **Timing Issues:** Minimize latency (<2 seconds), synchronize video and audio.

5.3.4 Printer Interface (for Certificates)

- **Device Types Supported:** Inkjet/laser printers.
- **Communication Protocols:** IPP (network), USB (local).
- **Inputs:** Print commands.
- **Outputs:** Printed document.
- **Timing Issues:** Printer ready within 30 seconds.

5.4 Communication Interfaces

5.4.1 Email Communication Interface

- **Purpose:** Used for notifying candidates about exams, results, and updates.
- **Format:** HTML (rich text) and plain-text email formats.
- **Security:** TLS encryption for secure transmission, PGP/S/MIME for sensitive data.
- **Attachments:** Max 5 MB; allowed formats: PDF, JPG, PNG, TXT.
- **Timing:** Emails sent within 2-3 seconds, delivery within 1 minute.
- **Constraints:** Validate email addresses; no raw passwords, secure links for password resets.

5.4.2 Web Browser Communication Interface

- **Purpose:** Used by candidates and administrators to access the system.
- **Format:** Data in JSON/XML; responses in HTML.
- **Security:** HTTPS for secure communication, session cookies for authentication.
- **Timing:** Server response within 3 seconds; page load within 5 seconds.
- **Constraints:** Ensure responsiveness across devices and handle browser incompatibilities.

5.4.3 Network Protocols

- **Purpose:** Standard protocols (HTTP/HTTPS) for communication between client and server.
- **Format:** JSON for API interactions.

- **Security:** SSL/TLS encryption, OAuth 2.0 or JWT for API authentication.
- **Timing:** Data requests processed within 500 ms; latency under 2 seconds during peak traffic.
- **Synchronization:** TCP/IP for reliable communication; client-server handshaking on session start.

5.4.4 Communication Security and Encryption

- **Encryption:** AES-256 for data at rest, TLS 1.2+ for data in transit.
- **Security:** Secure all communication channels against MITM and SQL Injection; use CAPTCHA/MFA for login.

6. Quality Attributes

6.1 Non-Functional Requirements

NFR-1 Performance

- Response time for database queries: within 2 seconds.
- Server response time: under 3 seconds.
- Data requests processed within 500 ms; latency under 2 seconds during peak traffic.

NFR-2 Scalability

- Support peak loads of up to 100,000 simultaneous users.

NFR-3 Security

- Data encryption: AES-256 for sensitive data at rest and TLS for data in transit.
- Compliance with data protection regulations (e.g., *GDPR*).
- Use of secure communication protocols (SSL/TLS).

NFR-4 Reliability

- Daily/weekly backups with mirrored copies for data integrity.
- Immutable audit logs for all transactions.

NFR-5 Usability

- User-friendly interfaces for candidates and administrators.
- Accessibility compliance (WCAG 2.1 AA).

NFR-6 Compatibility

- Support for modern web browsers (Chrome, Firefox, Edge, Safari).
- Compatibility with various operating systems (Windows, macOS, Linux, Android, iOS).

NFR-7 Maintainability

- Use of open-source or properly licensed libraries and frameworks.
- Python for backend and ReactJS for frontend to ensure maintainability.

NFR-8 Data Retention

- User data retained for five years, then securely deleted.
- Proctoring logs retained for 30 days.

7. Internationalization and localization requirements

7.1 Language Support

- Multilingual interface (e.g., *English, Urdu*).
- National spelling conventions (American vs. British English).

7.2 Date and Time Formatting

- Support various date formats (DD/MM/YYYY, MM/DD/YYYY).
- Display time in 12-hour or 24-hour formats.

7.3 Number and Currency Formatting

- Local number formatting (decimal and thousand separators).
- Support multiple currencies for payments.

7.4 Address and Telephone Formatting

- Adapt address fields for different country formats.
- Format telephone numbers with international dialing standards.

7.5 Time Zones

- Adjust exam schedules based on user's time zone.

7.6 Regulatory Compliance

- Comply with local data protection and privacy laws.

7.7 Technical Standards

- Provide guidelines for local electrical and internet standards.

Appendix A: Glossary

- **AI**: Artificial Intelligence – Technology that simulates human intelligence processes.
- **API:** Application Programming Interface – A set of functions and procedures for accessing features of an application.
- **DBMS:** Database Management System – Software for creating and managing databases.
- **FR:** Functional Requirement – A specification of what the system should do.
- **GDPR:** General Data Protection Regulation – A regulation in EU law on data protection and privacy.
- **MCQ:** Multiple Choice Question – A type of question with several answer options.
- **NFR:** Non-Functional Requirement – A specification of how the system performs a function.
- **OES:** Online Examination System – A digital platform for managing standardized tests.
- **SSL:** Secure Sockets Layer – A standard technology for establishing a secure connection.
- **TLS:** Transport Layer Security – A protocol that ensures privacy between communicating applications.
- **UI:** User Interface – The means by which a user interacts with a computer system.
- **UX:** User Experience – The overall experience a user has when interacting with a system.
- **VPN:** Virtual Private Network – A service that encrypts your internet connection for privacy.
- **HTTP:** Hypertext Transfer Protocol – The foundation of data communication on the web.
- **HTTPS:** Hypertext Transfer Protocol Secure – An extension of HTTP that uses encryption for secure communication.

- **JSON:** JavaScript Object Notation – A lightweight data interchange format.
- **XML:** eXtensible Markup Language – A markup language that defines rules for encoding documents.
- **MFA:** Multi-Factor Authentication – A security system that requires more than one form of verification.
- **CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans Apart – A security measure to determine if the user is human.
- **ERD:** Entity-Relationship Diagram – A visual representation of data entities and their relationships.
- **PDF:** Portable Document Format – A file format used to present documents in a manner independent of application software, hardware, and operating systems.
- **CSV:** Comma-Separated Values – A file format used to store tabular data in plain text.
- **WCAG:** Web Content Accessibility Guidelines – A set of guidelines for making web content more accessible to people with disabilities.

Questions:

Q1. What are the security measures for preventing cheating and ensuring data privacy?

Answer:

To prevent cheating and ensure data privacy in an Online Examination System (OES), several key security measures can be implemented. First, identity verification through facial recognition and ID checks helps confirm the candidate's identity. A secure exam environment can be established using browser lockdowns and screen monitoring to restrict access to unauthorized resources. Proctoring, both AI-driven and live, allows for real-time monitoring of candidates during the exam. Randomized question banks with dynamic selection and variations minimize the chances of answer sharing. Strict time management, including time limits and auto-submission, ensures candidates cannot exceed allotted time. Data encryption, using SSL/TLS for transmission and encryption for stored data, protects sensitive information. Access control through role-based permissions and multi-factor authentication (MFA) enhances account security. Maintaining audit trails by logging user activities and conducting regular audits helps identify any anomalies. Educating candidates on exam integrity and establishing clear policies further reinforce the system's security. Lastly, compliance with data privacy regulations like GDPR and implementing clear data retention policies safeguard candidate information. Together, these measures create a robust framework for maintaining the integrity and confidentiality of the examination process.

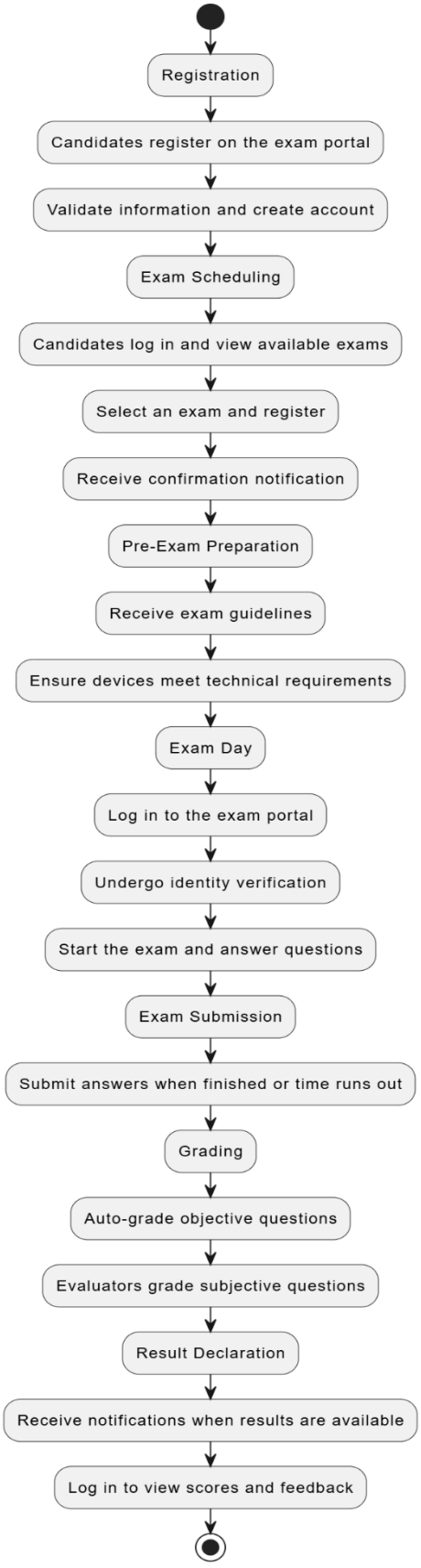
Q2. What constraints, such as bandwidth and device compatibility, must be considered?

Answer:

When designing an Online Examination System (OES), several constraints must be considered to ensure effective operation. Bandwidth constraints are crucial, requiring a minimum internet speed (e.g., 1 Mbps) to support smooth access, especially during peak exam times with many concurrent users. Device compatibility is essential, as the system should work on various devices (desktops, laptops, tablets, smartphones) and across multiple operating systems (Windows, macOS, Linux, Android, iOS) and browsers (Chrome, Firefox, Safari, Edge). Hardware requirements include functional webcams and microphones for identity verification and proctoring. Security constraints necessitate compliance with data protection regulations (e.g., GDPR) and secure connections (HTTPS) to protect candidate data. Additionally, the user interface must be intuitive and accessible, accommodating users with varying technical skills and ensuring compliance with accessibility standards. Finally, environmental factors, such as geographical limitations and reliable power supply, should be considered to provide equitable access to all candidates.

Q3. Describe the workflow for conducting an exam, from registration to result declaration.

Answer:



Q4. Develop a sequence diagram for the online exam process.

Answer: