Software Requirements Specification

for

AADHAR CARD MANAGEMENT SYSTEM

(features including Registration and Enrollment, Security & Updating Aadhar Card, etc.,)

Version 1.0 approved

Prepared by Nimba Sumeeth Singh

Lovely Professional University

30th March 2024

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

This document describes the software requirements and
specification for Aadhar Card Management System, which outlines the overarching goals and objectives of the system. It provides a clear understanding of why the system is being developed.

1.2 Document Conventions

Official documentations, tutorials and guides, online courses and other learning platforms, books and e-books, YouTube channels, GitHub repositories and other open-source projects.

1.3 Intended Audience and Reading Suggestions

The document is intended for all the stakeholders customer and the developers,
designers, testers, maintainers involved in the development of the Aadhar Card Management System.

1.4 Definitions, abbreviations

1.4.1 Definitions

- Registration and Enrollment:

1. Capture biometric (such as fingerprints and iris scans) and demographic (such as name, date of birth, and address) data of individuals applying for Aadhar cards.
2. Assign a unique Aadhar number to each applicant.

- Update and Correction Module:

1. Allow individuals to update their demographic information (e.g., address, phone number) and biometric data (if required).
2. Verify the changes submitted by individuals through appropriate validation processes.

- Authentication Module:

1. Provide various methods for Aadhar authentication, such as biometric authentication (fingerprint, iris scan) and one-time passwords (OTP) sent to registered mobile numbers.
2. Authenticate individuals' identity for availing government services, subsidies, or other benefits.

- Security Module:

1. Implement robust security measures to safeguard Aadhar data against unauthorized access, manipulation, or theft.
2. Authenticate authorized users (administrators, operators) accessing the Aadhar database.
3. Monitor and audit user activities to detect and prevent security breaches.

1.4.2 Abbreviations

Throughout this document the following abbreviations are used:

- UIDAI: Unique Identification Authority of India
- OTP: One-Time Password
- API: Application Programming Interface
- GUI: Graphical User Interface

1.5 Project Scope

Aadhar Card Management System defined in the Software Requirements Specification (SRS) encompasses the complete range of functionalities and objectives to be achieved by the system. It delineates the boundaries within which the system operates, detailing its core functionalities such as registration, update and correction, authentication, data management, security, and integration with other systems. The scope outlines the system's ability to capture and manage biometric and demographic data of individuals, generate unique Aadhar numbers, issue Aadhar cards, and authenticate individuals for availing government services.

1.6 References

<List any other documents or Web addresses to which this SRS refers. These may include user interface style guides, contracts, standards, system requirements specifications, use case documents, or a vision and scope document. Provide enough information so that the

reader could access a copy of each reference, including title, author, version number, date, and source or location.>

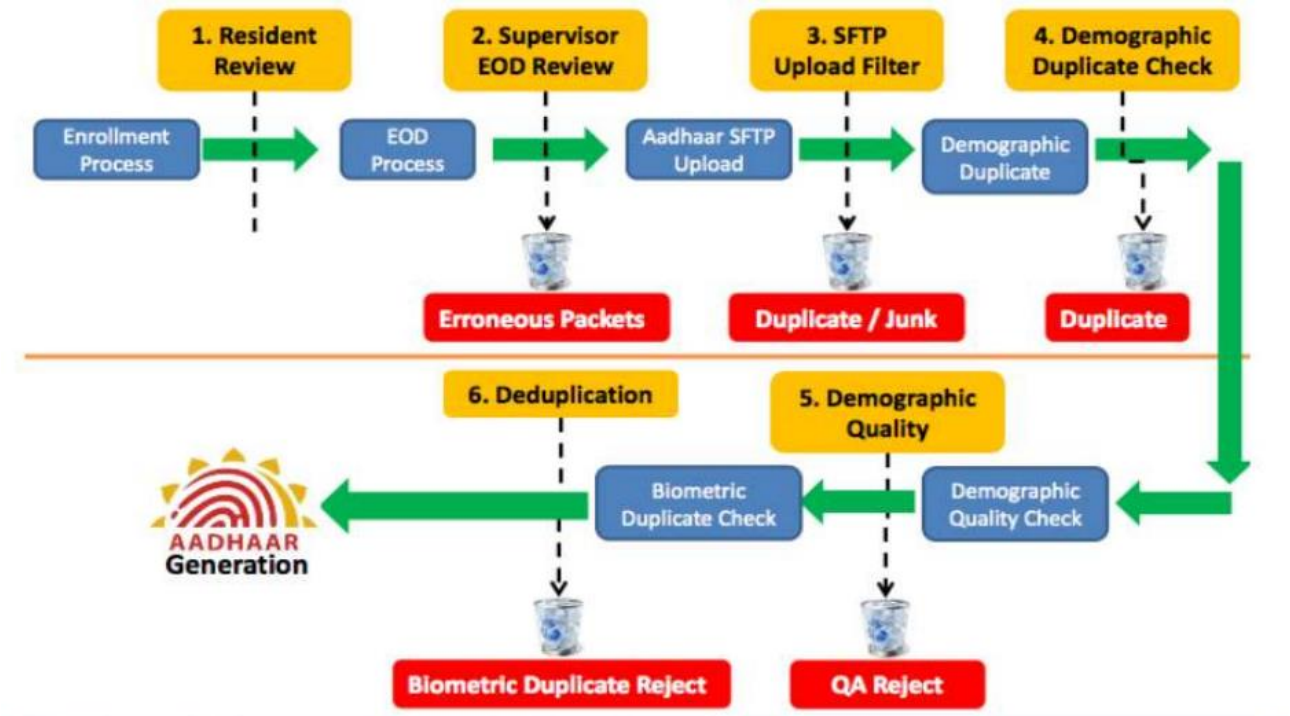
2. Overall Description

2.1 Product Perspective

The Software Requirements Specification (SRS) for the Aadhar Card Management System provides an overview of how the system fits into the broader context of its environment, including its interactions with external systems and stakeholders.

The Aadhar Card Management System is positioned within the larger ecosystem of government identity management systems, serving as a foundational component for identity verification and service delivery. It interfaces with various external systems, including government databases, authentication services, and third-party applications, to facilitate seamless integration and data exchange.

As a centralized system, it maintains a comprehensive repository of biometric and demographic data for individuals, ensuring uniqueness and accuracy in Aadhar numbers generation. The system serves diverse stakeholders, including citizens, government agencies, service providers, and regulatory bodies, by providing reliable identity verification services and enabling access to government benefits and services.



2.2 Product Features

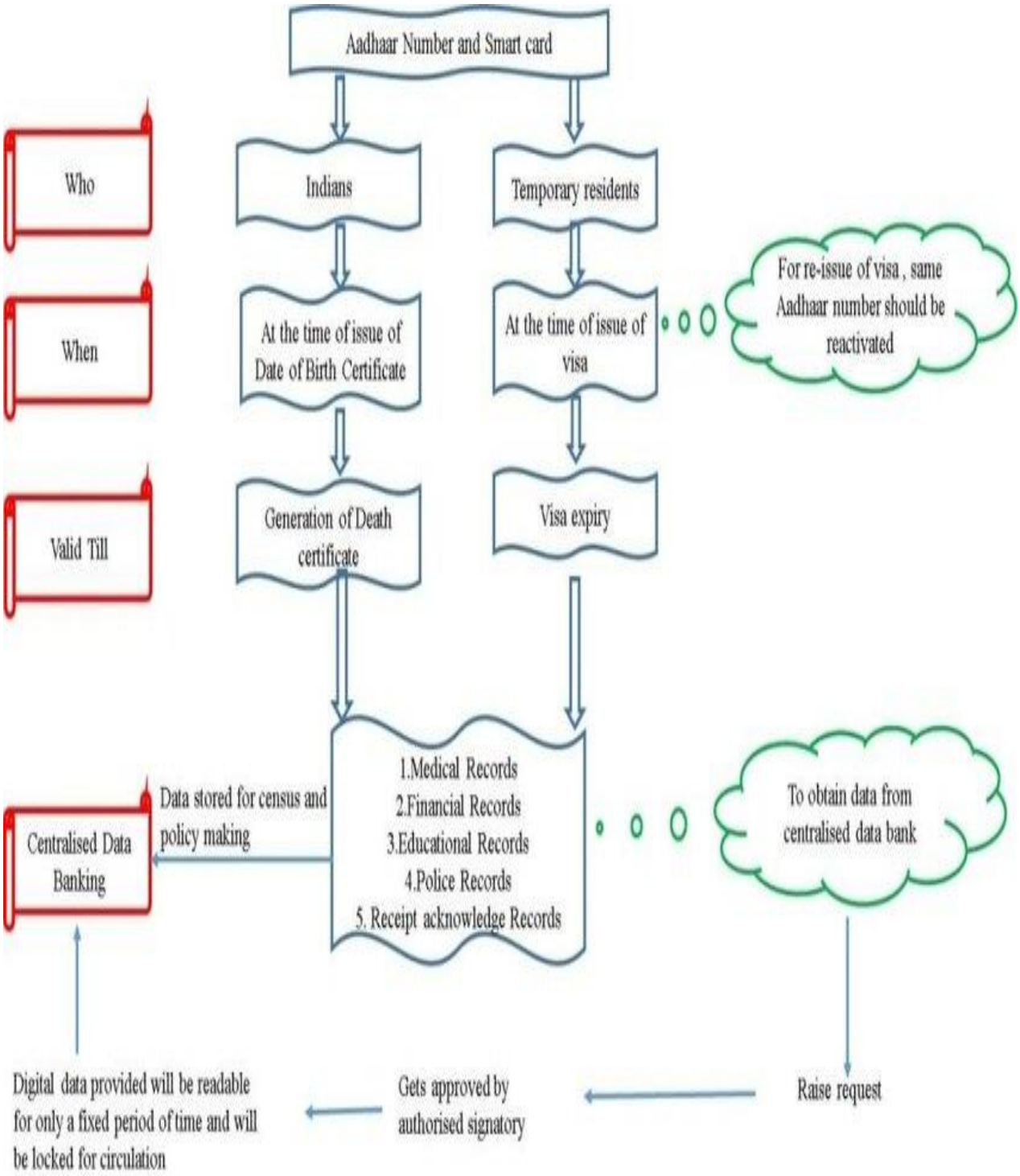
The Aadhar Card Management System offers the following features:

- Registration Module:
  - Capture biometric (fingerprint, iris scan) and demographic (name, address, date of birth) data.
  - Verify and validate identity information provided by individuals.
  - Generate unique Aadhar numbers and issue Aadhar cards.

- Authentication Module:
  - Provide various methods for Aadhar authentication, including biometric authentication and one-time passwords (OTP).
  - Authenticate individuals' identity for accessing government services, subsidies, or other benefits.

- Data Management Module:
  - Store and manage Aadhar data securely in a centralized database.
  - Implement data deduplication techniques to ensure uniqueness of Aadhar numbers.
  - Encrypt sensitive data to protect privacy and confidentiality.

- User Management Module:
  - Manage user accounts and permissions for administrators, operators, and other authorized personnel.
  - Enforce strong authentication mechanisms for user login to prevent unauthorized access.
  - Track and audit user activities to ensure compliance with regulations and policies.


Aadhaar Number and Smart card
Who
When
Valid Till
Indians
Temporary residents
At the time of issue of Date of Birth Certificate
At the time of issue of visa
For re-issue of visa , same Aadhaar number should be reactivated
Generation of Death certificate
Visa expiry
1.Medical Records
2.Financial Records
3.Educational Records
4.Police Records
5. Receipt acknowledge Records
Data stored for census and policy making
Centralised Data Banking
To obtain data from centralised data bank
Digital data provided will be readable for only a fixed period of time and will be locked for circulation
Gets approved by authorised signatory
Raise request

2.3 User Classes and Characteristics

In the Aadhar Card Management System, various user classes with different characteristics interact with the system:-

• Service Providers:

- Entities offering government or private services requiring Aadhar authentication.
- Include government agencies, financial institutions, telecom companies, etc.

• Administrators:

- Employees responsible for managing the Aadhar Card Management System.
- Trained in system administration and security practices.

• Operators:

- Employees responsible for day-to-day operations of the Aadhar Card Management system.
- Trained in system usage and customer service.
- Perform data entry and verification tasks.

2.4 Operating Environment

The Aadhar Card Management System operates in residential environments, with the following specifications:

• Hardware Requirements:

1. Server Infrastructure: High-performance servers capable of handling database operations, authentication requests, and data processing.
2. Storage Devices: Sufficient storage capacity to store biometric and demographic data of millions of individuals securely.

• Software Requirements:

1. Operating System: Server operating systems such as Linux (e.g., CentOS, Ubuntu) or Windows Server for hosting the application and database servers.
2. Database Management System: Relational database management system (RDBMS) such as MySQL, PostgreSQL, or Oracle for storing and managing Aadhar data.

- Network Infrastructure:

1. Local Area Network (LAN): High-speed Ethernet network for connecting server infrastructure, client devices, and biometric capture devices within the organization's premises.
2. Wide Area Network (WAN): Secure network connectivity to facilitate data exchange with external systems and government databases.

2.5 Design and Implementation Constraints

- **Regulatory Compliance**: Compliance with legal and regulatory requirements governing Aadhar data management, privacy, and security (e.g., Aadhar Act, data protection laws). Ensure adherence to standards and guidelines set forth by regulatory bodies (e.g., Unique Identification Authority of India - UIDAI).

- **Data Privacy and Security**: Implementation of encryption protocols (e.g., TLS/SSL) to secure data transmission over the network and protect sensitive information stored in databases. Compliance with data retention policies and procedures to ensure privacy and confidentiality of Aadhar data.

- **Scalability and Performance**: Designing the system to handle large volumes of data and concurrent user requests efficiently. Scalability considerations to accommodate future growth in the number of Aadhar registrations and authentication requests.

- **Interoperability**: Integration with existing government databases, systems, and services to facilitate data exchange and interoperability. Compatibility with diverse hardware and software environments used by stakeholders, including biometric capture devices and client applications.

- **Resource Constraints**: Limitations on hardware resources (e.g., server capacity, storage space) that may impact system performance and scalability. Budget constraints affecting the procurement of necessary hardware, software licenses, and infrastructure resources.

- **Technology Constraints**: Compatibility with specific technologies or platforms mandated by regulatory requirements or organizational policies. Dependency on third-party APIs, libraries, or frameworks for implementing certain functionalities (e.g., biometric SDKs, authentication services).

- **Geographical Constraints**: Considerations for geographic distribution and accessibility of Aadhar registration and authentication facilities, particularly in remote or underserved areas.

- **User Experience Constraints**: Accessibility requirements to ensure the system is usable by individuals with disabilities or special needs. Localization and multilingual support to accommodate users from diverse linguistic backgrounds.

- **Environmental Considerations**: Environmental factors affecting system operation, such as temperature, humidity, and physical security measures for data centres and server facilities. Compliance with environmental regulations and standards for energy efficiency, waste management, and sustainable practices.
- **Maintenance and Support**: Availability of skilled personnel for system maintenance, support, and troubleshooting. Documentation and training requirements to ensure users and administrators can effectively operate and maintain the system.

2.6 User Documentation

How to Apply for Aadhar Card:- To apply for an Aadhar Card, follow these steps:

Locate the nearest Aadhar Enrollment Center.

- Fill out the Aadhar Enrollment Form.
- Submit required documents (proof of identity, address, and date of birth).
- Have your biometric data (photograph, fingerprints, and iris scan) taken.

Documents Required:- The following documents are required for Aadhar Card enrollment:

- Proof of identity (e.g., passport, PAN card, driving license).
- Proof of address (e.g., utility bill, ration card, passport).
- Proof of date of birth (e.g., birth certificate, SSLC certificate).

Aadhar Card Enrollment Process:-

- Visit the Aadhar Enrollment Center.
- Fill out the enrollment form with accurate information.
- Submit the required documents.

Checking Aadhar Card Status:- To check the status of your Aadhar Card:

- Visit the official UIDAI website.
- Enter your enrollment number and date/time of enrollment.
- Verify the security code and click on "Check Status".

Updating Aadhar Card Information:- If you need to update any information on your Aadhar Card:

- Visit the nearest Aadhar Enrollment Center.
- Fill out the Aadhar Update Form.
- Submit the required documents for the update.

Using Aadhar Card for Authentication:- Aadhar Card can be used for various purposes, including:

- Identity verification for government and private services.
- Opening bank accounts and applying for loans.
- Availing subsidies and welfare benefits.

2.7 Assumptions and Dependencies

Data Accuracy: It's assumed that the data provided by users during enrollment or update processes is accurate and authentic. Any errors or discrepancies in the provided information may lead to issues with the Aadhar Card.

Biometric Accuracy: The system assumes that the biometric data collected during enrollment (such as fingerprints and iris scans) is accurate and reliably captured. Any issues with biometric data capture could impact the authentication process.

User Cooperation: The successful functioning of the system assumes that users will cooperate during enrollment, update, and authentication processes by providing required documents and biometric data accurately and without resistance.

Infrastructure Availability: It's assumed that the necessary infrastructure, including enrollment centers, biometric devices, and network connectivity, is available and operational to support Aadhar Card enrollment and authentication processes.

Security Measures: It's assumed that appropriate security measures are in place to protect the confidentiality, integrity, and availability of Aadhar Card data, including encryption, access controls, and regular security audits.

Government Support: The successful implementation and operation of the Aadhar Card system depend on continued support and funding from the government of India, as it is a government-initiated project.

Regulatory Changes: Dependencies exist on any changes or updates to regulatory requirements related to Aadhar Card enrollment, usage, and data protection. The system must adapt to any changes in regulations issued by UIDAI or other relevant authorities.

Integration with External Systems: If the Aadhar Card system needs to integrate with other government or private systems for authentication or data sharing purposes, dependencies exist on the availability and compatibility of those external systems.

User Awareness and Education: Successful adoption and usage of the Aadhar Card system depend on user awareness and education about its purpose, benefits, and processes. Dependencies exist on government-led campaigns or initiatives to educate the public about Aadhar Card usage and related services.

Vendor Support: If the system relies on third-party vendors for software, hardware, or services, dependencies exist on the availability of vendor support, including timely updates, maintenance, and troubleshooting assistance.

3. Specific Requirements

3.1 Functional Requirements

User Management

- The system shall allow registration of users including demographic details such as name, date of birth, address, etc.

- Users should be able to update their information (e.g., address change, phone number update) securely.
- Users must be able to retrieve their Aadhar card details through authentication mechanisms.

Aadhar Card Generation

- The system shall generate a unique Aadhar number for each registered individual.
- Aadhar cards must contain demographic information, including name, date of birth, gender, and photograph.
- Aadhar cards should be downloadable and printable in a PDF format.

Authentication and Verification –

- The system must provide a secure authentication mechanism for government agencies and authorized entities to verify Aadhar details.
- Aadhar authentication should be available through APIs for integration with third-party applications.

Data Security

- The system should comply with data protection regulations and ensure the security of personal information.
- Access to sensitive information should be restricted based on user roles and permissions. - Encryption must be used to protect data during transmission and storage.

Non-Functional Requirements

Performance

- The system should be capable of handling a large volume of concurrent requests without performance degradation.
- Response times for authentication and data retrieval should be minimal.

Scalability

- The system architecture should support scalability to accommodate future growth in the number of users and transactions.
- Scalability should be achieved through load balancing and distributed computing techniques.

Reliability

- The system must be highly available, with minimum downtime for maintenance or upgrades.
- Regular backups of the database should be performed to prevent data loss.

Security

- The system should implement robust authentication mechanisms to prevent unauthorized access.

- Audit logs must be maintained to track user activities and detect any security breaches.
- Regular security audits and penetration testing should be conducted to identify and address vulnerabilities.

3.2 Requirements of the Aadhar Card Management System

- The system shall allow individuals to register for an Aadhar card by providing necessary demographic information (e.g., name, date of birth, address).
- The system shall validate the provided information and assign a unique Aadhar number to each individual upon successful registration.
- The system shall support multiple authentication methods, including biometric (fingerprint, iris scan), OTP (One-Time Password), and demographic authentication.
- The system shall verify the authenticity of Aadhar cardholders during authentication processes.
- The system shall securely store and manage Aadhar cardholder information, including demographic details and biometric data.
- The system shall allow authorized personnel to update Aadhar cardholder information as necessary, with appropriate audit trails.

4. External Interface Requirements

4.1 User Interfaces

- The system shall provide a user-friendly interface for individuals to register for Aadhar card.
- The registration interface shall include fields for entering demographic information such as name, date of birth, address, etc.
- Error handling mechanisms shall be implemented to guide users in providing accurate information during registration.
- The system shall offer multiple authentication interfaces for users, including biometric authentication (fingerprint, iris scan), OTP (One-Time Password), and demographic authentication.
- The system shall provide a secure interface for individuals to download/print their Aadhar cards.
- Aadhar card issuance interfaces shall display accurate demographic information along with the individual's photograph and Aadhar number.
- Options for downloading/printing Aadhar cards shall be clearly presented, with appropriate security measures in place to prevent unauthorized access.

4.2 Hardware Interfaces

- The system shall interface with biometric devices (e.g., fingerprint scanners, iris scanners) for capturing biometric data during registration and authentication processes.
- Hardware interfaces shall be compatible with industry-standard biometric devices and adhere to relevant protocols for data exchange.
- The system shall support integration with printing devices for generating physical copies of Aadhar cards.
- Printing devices shall be capable of producing high-quality prints with accurate representation of Aadhar card information.
- Interfaces with printing devices shall ensure data privacy and security during the printing process.

4.3 Software Interfaces

- The system shall interact with a database management system (DBMS) for storing and retrieving Aadhar cardholder information.
- Software interfaces shall support CRUD (Create, Read, Update, Delete) operations for managing Aadhar card data.
- The system shall integrate with authentication services for verifying the authenticity of Aadhar cardholders during authentication processes.
- Software interfaces shall facilitate seamless communication between the Aadhar Card Management System and authentication services, adhering to predefined protocols and standards.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

- The system shall utilize system resources efficiently, with CPU utilization not exceeding 70% under peak load conditions.
- Memory usage shall be optimized to ensure the system remains responsive and stable, with memory consumption not exceeding 80% of available RAM.
- Batch processing tasks, such as data synchronization and backup, shall be completed within predefined time windows to minimize disruption to user-facing services.
- Data retrieval operations shall be optimized to minimize latency, with database queries executing within 500 milliseconds for typical search operations.
- The system shall support concurrent access by multiple users without data corruption or integrity issues.

5.2 Safety Requirements

- All sensitive data, including Aadhar cardholder information and biometric data, shall be encrypted both in transit and at rest using industry-standard encryption algorithms.
- Role-based access control (RBAC) shall be implemented to restrict access to Aadhar cardholder information based on user roles and privileges.
- The system shall maintain detailed audit logs of all user activities, including login attempts, data access, and administrative actions.
- Real-time security monitoring mechanisms shall be implemented to detect and mitigate security threats such as unauthorized access attempts and suspicious activities.
- Physical access to servers and data centers hosting Aadhar card data shall be restricted to authorized personnel only, with appropriate security measures such as access control systems and surveillance cameras.

- The system shall have provisions for emergency shutdown procedures to be initiated in the event of a security breach or other critical incidents.

5.3 Security Requirements

- The system shall enforce strong authentication mechanisms for user access, including biometric authentication (fingerprint, iris scan), OTP (One-Time Password), and demographic authentication.
- Privacy impact assessments (PIAs) shall be performed to identify and mitigate potential privacy risks associated with system operations and data processing activities.
- Data centers shall be equipped with surveillance cameras, intrusion detection systems, and environmental controls to ensure the physical security and integrity of critical infrastructure.
- Transport Layer Security (TLS) shall be enforced to provide end-to-end encryption and secure communication channels between system components.
- Cryptographic hash functions shall be used to generate checksums for stored data, allowing for verification of data integrity during retrieval and processing.

5.4 Software Quality Attributes

5.4.1 Availability:

- The system shall have a minimum uptime of 99.9%, excluding scheduled maintenance windows.
- High availability mechanisms, such as redundancy and failover, shall be implemented to minimize downtime and ensure continuous service availability.

5.4.2 Security:

The Aadhar Card Management System should prioritize maximum security. To enhance transparency and security:

- The system shall comply with industry-standard security practices and regulations, including encryption of sensitive data and access control mechanisms.
- Regular security assessments and penetration testing shall be conducted to identify and address vulnerabilities proactively.
- The system shall maintain detailed audit logs of user activities and security-related events to support forensic analysis and compliance auditing.

5.4.3 Maintainability:

- The system shall be designed with modularity and maintainability in mind, allowing for easy updates and enhancements.
- Code documentation shall be comprehensive, with clear comments and annotations to facilitate understanding and future maintenance.
- Automated testing and continuous integration practices shall be adopted to ensure code quality and stability throughout the development lifecycle.

5.4.4 Usability

- The user interface shall be intuitive and user-friendly, with clear navigation and minimal learning curve.
- Help documentation and tutorials shall be provided to assist users in understanding and using the system effectively.
- Error messages shall be informative and actionable, guiding users in resolving issues and completing tasks accurately.

5.4.5 Portability

- The system shall be platform-independent, capable of running on various operating systems and hardware configurations.
- Deployment procedures shall be well-documented and automated to facilitate easy installation and configuration in different environments.
- Compatibility with standard web browsers and mobile devices shall be ensured to support a wide range of user devices.

6. Other Requirements

User Feedback and Continuous Improvement:

- Mechanisms for collecting user feedback, such as surveys, feedback forms, or customer support channels, shall be implemented to gather input on system usability, performance, and functionality.

- Processes for evaluating user feedback and incorporating user suggestions for system enhancements shall be established to drive continuous improvement and innovation.

- Release management procedures shall be defined to manage software updates, patches, and new feature releases based on user feedback and business requirements.

Error Handling and Recovery:

- Error handling mechanisms shall be implemented to detect, report, and recover from system errors, exceptions, and faults.

- Procedures for error logging, notification, and escalation shall be defined to ensure timely resolution of system issues and minimize disruption to users.

Appendix A: Glossary

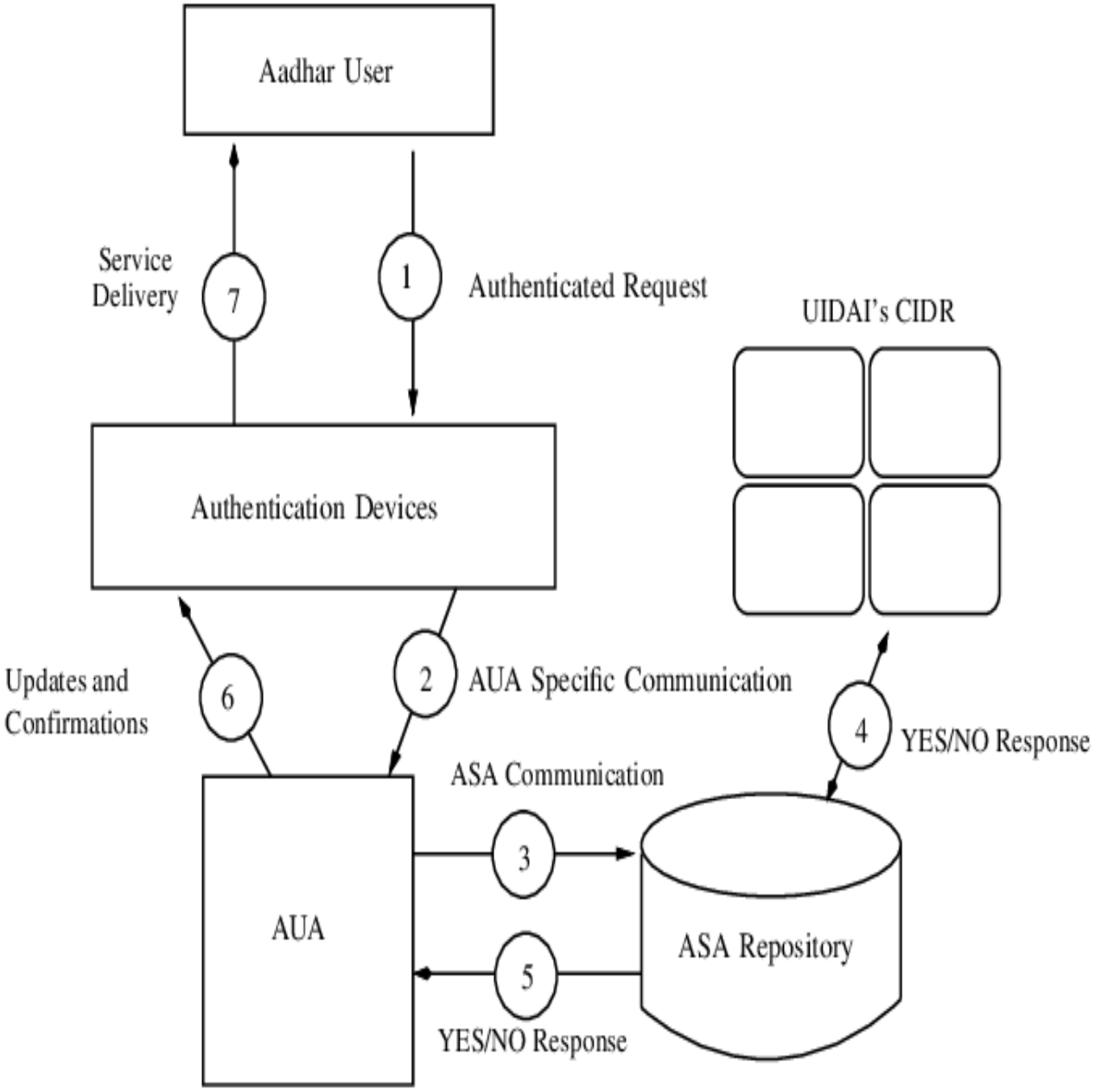
Acronyms and Abbreviations

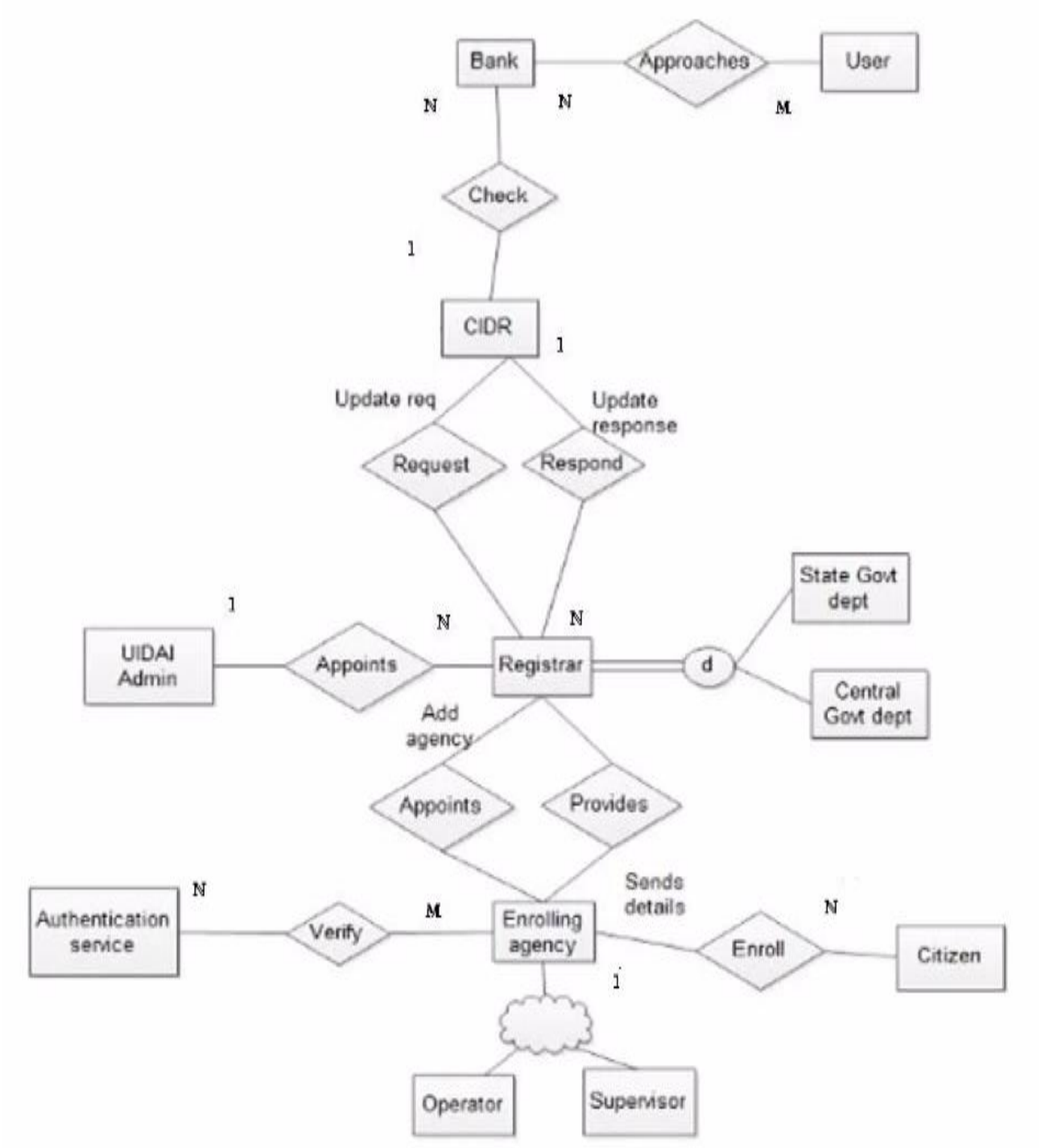
- ACMS: Aadhar Card Management System
- SRS: Software Requirements Specification
- SyRS: System Requirements Specification
- PRD: Product Requirements Document

Terms

- Aadhar Card: A unique identity card of a person.
- Aadhar Number: A unique 12-digit identification number issued by the Unique Identification Authority of India (UIDAI) to residents of India.
- Functional Requirements: Necessary features and functions of the software.
- Aadhar Card Management System: A system designed to protect a Aadhar Card from unauthorized intrusion, burglary, and other threats.
- Non-Functional Requirements: Characteristics of the software such as performance, usability, security, and reliability.
- State Diagram: A diagram showing the various states of a system and the transitions between them.
- Use Case: A description of a particular use of the system.
- User Authentication: The process of verifying the identity of a user.
- User Interface: The part of the system with which users interact.
- User Management: The process of managing users and their access to the system.

Appendix B: Analysis Models


Aadhar User
Service Delivery
7
1
Authenticated Request
UIDAI's CIDR
Authentication Devices
Updates and Confirmations
6
2
AUA Specific Communication
4
YES/NO Response
ASA Communication
AUA
3
ASA Repository
5
YES/NO Response


Bank
Approaches
User
N
N
M
Check
1
CIDR
1
Update req
Update response
Request
Respond
1
N
N
UIDAI Admin
Appoints
Registrar
d
State Govt dept
Central Govt dept
Add agency
Appoints
Provides
N
M
Sends details
N
Authentication service
Verify
Enrolling agency
Enroll
Citizen
1
Operator
Supervisor

Appendix C: Issues List

- **Issue ID: ACMS-01**
    - Description: Unclear definition of user roles and permissions.
    - Resolution: Requires clarification from stakeholders regarding the roles and responsibilities of different user types (e.g., administrators, operators, users).
- **Issue ID: ACMS-02**
    - Description: Lack of clarity on data retention policies and regulatory compliance requirements.
    - Resolution: Requires review and alignment with legal and regulatory frameworks governing data protection and privacy (e.g., Aadhar Act, GDPR).
- **Issue ID: ACMS-03**
    - Description: Performance benchmarking requirements need further elaboration.
    - Resolution: Requires collaboration with performance testing team to define specific performance metrics, scenarios, and acceptance criteria.
- **Issue ID: ACMS-04**
    - Description: Concerns raised regarding the security of biometric data storage and authentication mechanisms.
    - Resolution: Requires a security review and risk assessment to address potential vulnerabilities and ensure robust security measures are in place.
- **Issue ID: ACMS-05**
    - Description: Uncertain interoperability requirements with external systems and services.
    - Resolution: Requires coordination with external stakeholders to clarify integration needs and compatibility requirements.
- **Issue ID: ACMS-06**

- Description: Lack of documentation for API specifications and system interfaces.
- Resolution: Requires development of comprehensive documentation outlining APIs, data exchange formats, and integration protocols.

- **Issue ID: ACMS-07**

  - Description: Concerns raised regarding system usability and user training needs.
  - Resolution: Requires usability testing and user feedback sessions to identify areas for improvement and develop user training materials.

- **Issue ID: ACMS-08**

  - Description: Uncertainty regarding disaster recovery and business continuity plans.
  - Resolution: Requires development of detailed contingency plans and procedures to mitigate the impact of system failures or disasters.