Table of Contents

Table of Contents

List of Tables

List of figures.

Abstract

This platform aims to improve the existing residential identity management system by introducing a multi-purpose ID system. One of the primary challenges faced by society is the prevalence of multiple IDs serving the same purpose, leading to inefficiencies and difficulties in replacing lost IDs. The proposed platform addresses these issues by streamlining identity management for users and providing advanced tools for high-level administrators, such as police officers, to access credential information easily. In addition to registering users, the platform aids investigators by generating detailed reports and enabling effective biometric searches. This dual-purpose system enhances user convenience and supports investigative processes, ultimately improving the overall efficiency and security of identity management systems.

Chapter One: Introduction

The growth of identity fraud in Ethiopia, especially in Sheger City, has led to significant political and economic problems. Among the main concerns is the unlawful acquisition and abuse of land ownership certificates, with severe implications. A research study conducted by the Minister of Justice in partnership with the National Bank of Ethiopia highlights the gravity of the issue at hand.[1] Between 2014 and 2019, financial institutions incurred cumulative losses amounting to 1.8 billion birr, mostly because of identity fraud and the lack of a centralized system to authenticate residential identification.[2] This is compounded by the absence of consistency between different identification systems, including ATM cards, driver's licenses, school ID cards, and work IDs, upon which individuals depend in their daily lives. There is a need to address these challenges in an effort to curtail fraud, secure property rights, and encourage economic stability.

To address this challenge, Ethiopia began the National Identification Program, which it implemented with the issuance of a digital ID program called Fayda.[3] The program offers citizens a 12-digit ID number upon the completion of registration procedures. The Fayda ID seeks to build a safer and more reliable identity management system. The project is already being rolled out in 119 districts and 11 sub-cities of Addis Ababa and will continue to expand within six months. By centralizing identity verification processes and enabling the distribution of digital identification, Fayda aims to minimize the possibility of fraudulent activities and trust between public and private institutions. Yet, although Fayda is a big step forward, it has a relatively narrow scope since it is more nationalistic in scope and does not have the multi-dimensional capabilities to tackle larger issues successfully.

The best framework in this case is the proposed Multi-Purpose Digital Resident ID system for Sherger City. This system, as opposed to Fayda, integrates different identification frameworks into one system. It achieves this by integrating residential identification documents and combining them with other identification, such as driver's licenses and school ID cards.

1.1. Statement of the Problem

The current identification system often requires people to have several forms of identification, including national identification cards, driver's licenses, and other governmental papers. Multiplicity can cause serious inconvenience, particularly in the event that an identification card is lost or stolen. The retrieval or obtaining of a replacement identification document is typically a long and complex process, forcing people to endure bureaucratic red tape and bear extra charges. These inefficiencies are resulting in a burdensome experience for individuals while creating administrative problems on the part of issuing authorities of such identification documents. The goal of this project is to alleviate such problems through a proposed integrated system where digital devices are utilized as a single, common digital platform for identification. Leveraging the prevalence and extent of mobile phones, this system is designed to streamline identification processes, minimize reliance on physical identification documents, and maximize convenience to users.

On a larger level, the use of biometric data within this system is highly beneficial for governments and security organizations.[4] Biometric registration ensures every citizen possesses an authentic and distinctive digital identity that reduces chances of fraud or replication.[5] This information can be critical in enabling swift and efficient crime investigation, which enables law enforcement bodies to possess veritable identification systems. For instance, linking biometric data to a central ID system can accelerate the identification of suspects, authenticate identities in the course of investigations, and keep databases current. Through the resolution of both user-centric and institutional issues, the project presents a holistic solution for updating identification systems while optimizing security and efficiency of operations.

Additionally, this initiative accentuates the demand for a converged and trusted digital identity framework. Through the integration and interconnection of identification frameworks, the proposed architecture not only saves redundancies but also enhances the availability of data to rightful parties. This shift towards digital identification is a massive stride forward.

1.2. Objectives

1.2.1. General Objective

The main goal of this study is to develop a multipurpose digital ID system that securely integrates and manages various forms of identification, providing individuals with seamless access to multiple services. The system improves accessibility while maintaining security and scalability by integrating flexible registration methods, such as the use of biometric devices or commonly accessible tools like laptops and mobile phones.

1.2.2. Specific Objectives

- Specify and record user, functional, and non-functional specifications.
- Assess the feasibility of capturing biometric data on mobile and laptop devices.
- Specify security, scalability, and interoperability limits for the system.
- Identify use case scenarios for individual and administrator users.
- Design a secure and scalable system architecture.
- Design a database schema for encrypted biometric templates and ID data.
- Design an intuitive user interface for mobile and laptop devices.
- Implement biometric data capture by using device camera and sensor capabilities.
- Integrate the system with third-party ID providers.
- Implement encryption and storage of data securely.
- Provide administrative tools for biometric searches and report generation.
- Conduct unit and system testing to ensure proper functionality.
- Conduct user acceptance testing to get feedback from stakeholders.

- Deploy the system on a cloud-based platform for scalability.
- Develop a maintenance plan to ensure long-term reliability and security.

1.3. Scope and Limitation

1.3.1 Scope

This project is centered on creating a Multi-Purpose Digital Residential ID system specifically designed for Sheger City.

Web Application for User Control: We will develop an intuitive web app that allows residents to see their IDs and be notified for scheduled ID related services.

Web Application for User Registration: We will develop an intuitive web app that allows institutional admins to register residents using biometric information. This will involve capturing biometric data, linking it to existing IDs, and producing a unique digital ID for each user.

Web Application for Administrative Control: A web-based platform will be established for administrators to oversee user data, conduct searches, generate reports, and provide authorized access to biometric and ID-related information for government and security agencies.
Integration of Multiple IDs: The system will bring together various identification documents, such as driver's licenses, work IDs, and school IDs, into a single digital platform for easier management.
Crime Analysis Support: The administrative web app will feature tools that enable security agencies to perform quick and precise crime analysis using the registered biometric data.

1.3.2 Limitation

Inability to Integrate with ATM Cards: Due to security concerns and the complexities involved in integrating with financial systems, the digital ID will not be connected to ATM cards or other banking services. This choice ensures that the focus remains on residential and administrative uses while upholding high security standards for user data.

Limited Geographic Coverage: The initial rollout is specifically tailored for Sheger City, and there are no plans to expand to other areas in this current phase of the project.

Dependence on Device Capabilities: The biometric registration process depends on the hardware capabilities of users' mobile devices and laptops, which can differ significantly in quality and accuracy.

User Acceptance : Will the user accept the new proposed system while the old one exists?

1.4. Methodology

1.4.1 Data Collection Techniques

Data will be collected using the following methods[6]:

1. **Interviews and Surveys**: Direct input from potential users and stakeholders will be gathered to understand the specific needs of residents, government agencies, and security personnel.
2. **Existing Documentation**: Information from government and security agencies regarding current ID systems, biometric data use, and crime analysis procedures will be reviewed to ensure the new system integrates seamlessly.

1.4.2 Data Analysis Strategies

Once the data is collected, the following analysis strategies will be used:

- **Thematic Analysis**: For qualitative data (e.g., interview and survey responses), thematic analysis will be used to identify common trends and requirements.
- **Statistical Analysis**: Quantitative data related to system performance, efficiency, and user satisfaction will be analyzed [7] using descriptive and inferential statistics to measure success and identify areas for improvement.

1.4.3 System Design and Implementation

The development of the Multi-Purpose Digital Residential ID system will follow the **Agile** software development methodology. This will ensure that the system is flexible, iterative, and responsive to changes in user requirements and feedback during the project lifecycle. The main components of the system include:

- **User Registration System**: A web app will be designed to capture biometric data (e.g., facial recognition, fingerprints) using the a camera and fingerprint sensor. It will also integrate various forms of ID (e.g., driver's licenses, school/work IDs) into a single digital ID profile.
- **Admin Control System**: A web application will be developed for administrative users (government and security personnel) to manage user data, perform search queries, and generate reports.
- **Integration with External ID Providers**: The system will be designed to integrate with various existing ID databases to ensure users' multiple IDs are linked correctly.

1.4.5 Technology Stack

The system will be built using the following technologies:

- **Frontend**:
  - **Web App**: React.js for the web-based admin control interface.[9], [10]
- **Backend**:
  - **Server**: Django for server-side processing and API development. [11]
  - **Database**: PostgreSQL for storing user data and ID information securely.[12]
  - **Biometric Processing**: Use of device-native biometric libraries for facial recognition

and fingerprint scanning.[9]

- **Security**:
    - **Encryption**: AES (Advanced Encryption Standard) for encrypting biometric data and personal information.
    - **Authentication**: OAuth 2.0 for secure user login and authorization.
    - **Data Storage**: Secure storage of biometric data using hashing and encryption methods to ensure user privacy.

Table 1.1. Technology Stack Comparison

Category	Tech Stack	Performance	Scalability	Security	Ease of Development	Cost	Conclusion
Frontend - Web App	React.js (Chosen)	High	High	High	High	Medium	Best for modularity and performance.
	Angular.js	Medium	High	High	Medium	Medium	More complex for small-scale projects
	Vue.js	Medium	Medium	High	High	Medium	Simple but less scalable
Backend - Server	Django (Chosen)	High	High	High	High	Low	Robust and secure for APIs.
	Node.js	High	High	Medium	High	Low	Suitable for real-time apps.
	Spring Boot (Java)	High	High	High	Medium	Medium	Great for enterprise-level apps.
Database	PostgreSQL (Chosen)	High	High	High	Medium	Low	Best for structured data and security
	MySQL	High	High	Medium	High	Low	Good but slightly less secure.

	MongoDB	High	High	Low	Medium	Low	Best for unstructured data.

1.4.6 **Testing and Deployment**

To ensure the quality and reliability of the system, the following testing methods and deployment strategies will be employed:

Unit Testing: Each module of the system (e.g., registration, data integration, admin controls) will undergo unit testing to verify individual functionality. We will use Jest for JavaScript and TypeScript and unittest for django.

Integration Testing: The interaction between different modules, including mobile registration and web admin systems, will be tested to ensure seamless communication.

User Acceptance Testing (UAT): A beta version of the system will be deployed to a select group of users for feedback and validation.

Performance Testing: Load testing will be conducted to ensure the system can handle high volumes of data and user interactions.

Security Testing: Penetration testing will be carried out to identify and address potential vulnerabilities in the system.

Deployment: The system will be deployed on Vercel to ensure scalability, reliability, and availability. Continuous monitoring will be set up to track system performance and security post-deployment. The backend will be deployed on Render.

1.5. Plan of Activities

Table 1.2 Plan of Activities

Activities	Objective	Key Milestones and Deliverables	Duration (Weeks)
1. Project Initiation	Establish the foundation for the project.	- Approved project proposal. - Identified stakeholders, deliverables, and feasibility report.	2 weeks

2. Research and Analysis	Conduct a comprehensive study of related systems.	- Literature review completed (Aadhaar, e-Residency, Huduma Namba). -Conduct interviews and surveys with residents, government agencies, and security personnel.	4 weeks
3. System Design	Define the architecture and design for the digital ID.	- System architecture diagram. - UI/UX wireframes. - Security and data privacy framework.	4 weeks
4. Prototype Development	Build a working prototype of the system.	- Functional prototype with core features: registration, authentication, and AI integration.	6 weeks
5. Testing and Validation	Ensure the system meets functional and security needs.	- Testing reports (functional, performance, and security). - Pilot feedback report and system refinement.	4 weeks
6. Final Report & Presentation	Document results and demonstrate outcomes.	- Final project report. - Presentation materials and system demonstration.	2 weeks
7. Project Closure	Review and document project outcomes.	- Post-project review document. - Final deliverables submitted.	2 weeks

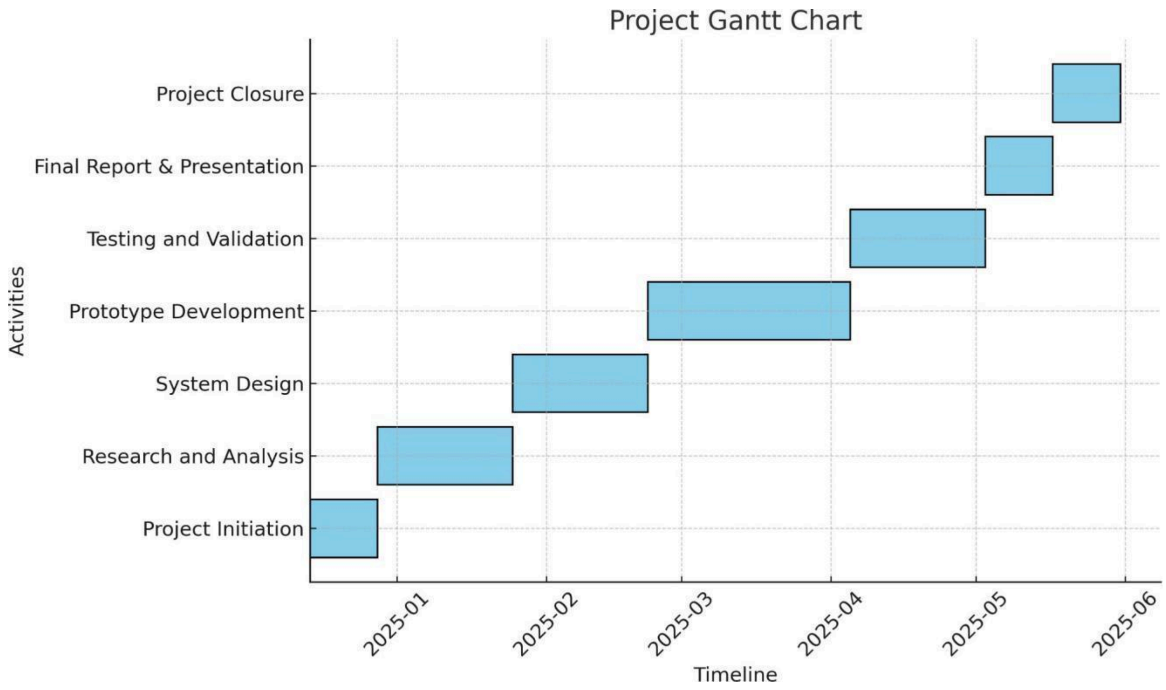

Fig 1.1 Plan of Activities Gantt Chart

1.7. Significance of the Study

Economic Impact: The system helps reduce fraud, thereby protecting property rights and bolstering the local economy.[13]
Social Benefit: A more reliable identification system fosters greater trust among citizens, leading to increased satisfaction and engagement.
Technological Advancement: It showcases the innovative application of mobile devices and biometric technology in areas with limited resources.
Policy Implications: The findings offer a scalable framework for updating identification systems in other cities or regions.

1.7.1 Expected Outcomes

1. **Improved Identification System:** A unified digital ID platform reducing reliance on physical IDs.
2. **Enhanced Security:** Biometric data integration minimizes identity fraud and duplication.
3. **Administrative Efficiency:** Streamlined workflows for government and security agencies.
4. **User Convenience:** Accessible mobile-based registration and centralized ID management.
5. **Crime Analysis Support:** Tools for quick and effective identification and investigation.

1.8 Outline of the Study

This is a chapter of introduction that gives an overview of the multi-functional identification system project, its importance in facilitating identification processes, and improving ease of access to various services. It prescribes the general and project-specific objectives of the project, which are aimed at creating a centralized, secure, and efficient identification system to address the needs of various stakeholders. The chapter also gives the intended activities and methods, setting a clear map for the achievement of the project objectives.

The following chapters will go further into the foundational research and literature review, putting it into context by examining current systems, determining the flaws, and investigating emerging solutions. This is the basis for a close look at the technical and operational details in the later chapters, thereby building a basis for an effective and viable solution.

Chapter two: Literature Review

2.1 Study Related Works

Overview of Digital Identity Systems in India, Estonia, and Kenya

- **India: Aadhaar**

  It is among the largest biometric-based digital ID systems in the world, which provides a 12-digit unique identification to more than 1.3 billion residents. This system is likely to reduce duplication in identity, enhance service delivery, and guarantee financial inclusion. Basically, Aadhaar uses biometric (fingerprints and iris scans) and demographic data with a central registry. While linkage of Aadhaar with welfare programs enhanced transparency, concerns over privacy and exclusion due to biometric failures remain palpable.

Estonia: e-Residency

- The e-Residency program initiated by Estonia in 2014 gives a government-issued digital identity to founders around the world for easily starting and managing businesses remotely. It allows access to Estonia's e-government services that range from company registration to the secure signing of documents. The initiative is built on very well-developed digital infrastructure integrated with blockchain technology, hence promoting global entrepreneurship. It nevertheless has its limitations in scope, dependence on digital literacy, and potential misuse.

Kenya: Huduma Namba

- Huduma Namba attempts to combine the different identification systems into a single one to ease access to services and eliminate fraud cases. It captures biometric and demographic information, with the resultant benefits ranging from efficient service delivery and resource allocation. However, it has been plagued by court cases, private concerns of data, and inclusivity issues, especially in reaching marginal groups.

2.2 Milestones and gaps

Milestones

Global digital identity systems have achieved significant milestones, revolutionizing governance, service delivery, and socio-economic development.

- **Implementation at Scale:** Systems like India's Aadhaar, the world's largest biometric ID, have successfully enrolled over 1.3 billion people, showcasing scalability even in resource-limited settings.

- **Biometric Integration:** Technologies like fingerprints and iris scans have enhanced identity verification. Estonia’s e-Residency employs secure digital signatures and multi-factor authentication.
- **Streamlined Service Delivery:** Aadhaar has improved welfare distribution by reducing fraud, while Estonia’s e-Residency enables global business operations.
- **Cross-Border Innovation:** Estonia’s e-Residency has redefined citizenship, inspiring nations to explore transnational digital identities.
- **Legal Frameworks:** Regulations like India’s Aadhaar Act and Kenya’s Huduma Namba laws ensure governance and accountability.
- **Financial Inclusion:** Linking identities to banking systems, Aadhaar has provided millions access to credit, savings, and insurance.
- **Public-Private Partnerships:** Collaboration with private entities has driven innovation and scalability, as seen in Aadhaar’s ecosystem.
- **Global Influence:** Systems like Aadhaar and e-Residency have become benchmarks, inspiring similar initiatives worldwide.

Gaps
Despite advancements, challenges remain in achieving inclusivity, security, and efficiency.

- **Privacy and Security:** Systems like Aadhaar and Huduma Namba have faced data breaches and surveillance concerns, undermining trust.
- **Exclusion of Marginalized Groups:** Rural and undocumented populations often lack access, perpetuating inequality.
- **Legal Challenges:** Gaps in regulations, such as limited privacy protections in India and Kenya, hinder effective implementation.
- **Interoperability Issues:** Fragmentation between systems and databases limits efficiency and integration.
- **High Costs:** Financial constraints challenge sustainability, particularly in developing nations like Kenya.
- **Public Awareness:** Resistance due to inadequate communication, as seen in Huduma Namba, highlights the need for transparent engagement.
- **Infrastructure Limitations:** Limited internet and power access hinder adoption, especially in rural regions.
- **Ethical Concerns:** Risks of surveillance, discrimination, and misuse necessitate oversight and accountability.

2.3. Lessons Learned in Digital Identity Systems

The implementation of systems like India’s Aadhaar, Estonia’s e-Residency, and Kenya’s Huduma Namba offers valuable insights for designing inclusive, secure, and efficient digital ID initiatives.

1. **Inclusivity**
   Ensuring access for marginalized populations is critical. Offline enrollment, mobile units for rural areas, and simplified registration processes promote accessibility and equity.
2. **Balancing Privacy with Functionality**
   Robust privacy frameworks and advanced security measures, like encryption and multi-factor authentication, enhance user trust while maintaining functionality, as seen in Estonia's e-Residency.
3. **Legal and Institutional Frameworks**
   Strong laws governing data use, user consent, and accountability, as in India's Aadhaar Act, foster public trust. Gaps, however, can lead to legal challenges, as with Huduma Namba.
4. **Beyond Technology**
   Technology alone cannot guarantee success. Investments in public awareness, capacity building, and infrastructure (e.g., reliable internet and power) are equally vital for system effectiveness.
5. **Public Awareness and Engagement**
   Transparent communication about benefits, safeguards, and processes builds public trust. Estonia's user-centric approach contrasts with Kenya's challenges in gaining acceptance due to misinformation.
6. **Interoperability**
   Integrating systems with other government databases enhances efficiency and reduces redundancy. Estonia's interconnected ecosystem offers a model for seamless integration.
7. **Phased Implementation**
   Starting small with pilot programs allows for testing and refinement before scaling. Estonia's gradual rollout contrasts with Aadhaar's immediate large-scale implementation, which faced logistical challenges.
8. **Collaboration**
   Partnerships with private sector players and international organizations, as seen in Aadhaar and e-Residency, drive innovation, scalability, and sustainability.
9. **Adaptability**
   Continuous updates and future-ready designs, like Estonia's evolving infrastructure, ensure systems remain effective amid technological and societal changes.

Chapter Three: Problem Analysis and Modeling

3.1 Existing System and Its Problems

3.1.1 Current System Overview

The identity management system in Ethiopia is fragmented and uncoordinated. There is no single framework, so citizens depend on physical IDs like driver's licenses, work IDs, school IDs, and general IDs issued and managed independently by other institutions. It is a paper-based, labor-intensive process with a lot of inefficiencies, high operational costs, and low access. Technical challenges, regulatory gaps, and inadequacy of infrastructure are some of the challenges facing the adoption of digital identity in Ethiopia. Most of these systems are not interconnected, and most of their operations are manual, further contributing to inefficiencies and data redundancies. Additionally, the current systems do not meet the needs of rural populations, exacerbating inequities in access to essential services.

3.1.2 Problems and Limitations

1. **Fragmentation and Duplication of Data**
    - Each institution independently issues its own IDs, leading to redundant data collection, increased administrative workload, and higher operational costs. Citizens are burdened with managing multiple IDs for different services.
    - Supporting Evidence:
        - Over 60% of Ethiopia's population lacks access to a unified digital ID service, as reported by the World Bank. This fragmentation perpetuates inefficiencies across sectors.
        - A 2023 report from the World Bank highlights the absence of standardized ID systems in Ethiopia, causing duplication and inconvenience for users and institutions alike.
2. **Lack of Centralized Verification**
    - Identity verification relies on manual processes across various organizations. This delays service delivery, increases operational costs, and exposes the system to identity fraud.
    - Supporting Evidence:
        - According to the World Bank, Ethiopia's decentralized ID system has made it difficult to prevent identity fraud or streamline verification processes.
        - In contrast, centralized systems like India’s Aadhaar provide seamless verification, reducing fraud and improving efficiency.
3. **Limited Biometric Integration**
    - While some institutions are adopting biometrics (e.g., fingerprints), the process lacks standardization and scalability. The absence of advanced biometric systems limits Ethiopia's ability to use such data for forensic and criminal investigations.

   - Supporting Evidence:
      - The World Bank's **Ethiopia Digital ID for Inclusion and Services Project** (2023) aims to address this gap by integrating inclusive and secure biometric systems for 90 million people, highlighting the current system's deficiencies.

4. **Access Barriers**
   - Digital ID systems are inaccessible to many rural areas due to limited internet connectivity (19% of the population, per the World Bank). This exclusion is compounded by the absence of multilingual support, which affects Ethiopia's linguistically diverse population.
   - Supporting Evidence:
      - Women are 15 percentage points less likely than men to possess the primary kebele ID, according to the World Bank's **Gender Gap in ID Ownership** report. This gender disparity underscores the need for inclusive systems that address access inequalities.
5. **Security Concerns**
   - The reliance on paper-based IDs makes the system vulnerable to forgery, unauthorized access, and fraud. Insufficient digital infrastructure exacerbates these risks.
   - Supporting Evidence:
      - A study by the **World Bank ID4D** initiative highlights that Ethiopia’s current ID system suffers from inadequate personal data protection, exposing citizens to privacy violations.
      - India's Aadhaar system addresses these challenges by using encryption and robust data protection frameworks.
6. **Administrative Challenges**
   - Managing roles and access levels for institutions is cumbersome. Institutions often perform redundant checks for the same individual across multiple systems.
   - Supporting Evidence:
      - The **World Bank Digital ID Project** notes the inefficiencies in Ethiopia's current system, emphasizing the need for streamlined administrative processes to reduce duplication.
7. **Inconsistent Scheduling and Expiration Tracking**
   - Users struggle to track ID expiration dates and schedules, leading to missed renewals and penalties. A unified digital ID could address this issue by automating reminders and simplifying renewals.

3.1.3 Impact on Stakeholders

1. **Citizens**
   - Citizens face the burden of managing multiple IDs, inefficient service delivery, and privacy risks due to the lack of robust security measures.

    - Reduced trust in the system and exclusion of vulnerable groups, particularly women and rural populations, amplify inequities.
2. **Institutions**
    - High operational costs and redundancies slow down service delivery and hinder inter-agency coordination.
3. **Government**
    - The lack of an integrated system reduces the government's ability to provide efficient public services and leverage identity data for national initiatives like social welfare or crime control.
4. **Law Enforcement**
    - Difficulty accessing unified identity data hampers forensic investigations and

3.1.4 Interview: Mr. Gemeda Gudeta, Head of Shaggar Science and Technology Office

The interview findings reveal significant inefficiencies and challenges in Sheger City’s current ID management system, which is heavily reliant on traditional paper-based processes. Issuing IDs takes 1–2 weeks and involves complex, manual procedures requiring citizens to interact with multiple offices, such as police stations and administrative departments. Fraud, decentralized data management, and the prevalence of fake or duplicate IDs further hinder the system's reliability. Additionally, the lack of a unified system makes it difficult to effectively track and identify citizens, leading to delays in accessing essential services.

While there is an ongoing initiative to introduce digital IDs in two sub-cities, Burayu and Sululta, the current system remains decentralized and is not designed to serve multiple purposes. This partial adoption highlights the potential of digital IDs but also underscores the need for a more cohesive, city-wide solution that integrates various identification documents (e.g., driver’s license, work ID) into a single, secure platform. A multi-purpose digital ID system, enhanced with biometric technologies like fingerprints and facial recognition, could significantly reduce fraud, improve efficiency, and ensure better data accuracy. It would also streamline access to services like healthcare and education, enhancing the overall citizen experience.

However, potential barriers to adoption include literacy gaps, limited access to smartphones, and privacy concerns. Employees emphasized the importance of providing training, resources, and robust data security measures to address these challenges and ensure a smooth transition. The introduction of a unified digital ID system promises to resolve inefficiencies in the existing framework while building on the initial efforts in Burayu and Sululta, paving the way for a more connected and responsive governance model in Sheger City.

3.2 Specifying the Requirements of the proposed solution

Each of the requirements needs a mechanism to be uniquely identified so that team members can communicate easily without misunderstandings. This document uses symbolic identification to tag each requirement with a unique requirement ID.

Functional Requirements

Table 3.1. System Requirements: Functional Requirements

Acronym	Definition
SAR	Super Admin Requirements
USR	User Requirements
IAR	Institutional Admin Requirements
OIR	Other ID Issuing Institutions Requirements

Non-Functional Requirements

Table 3.2 System Requirements: Non-Functional Requirements

Acronym	Definition
AVL	Availability Requirements
SEC	Security Requirements
PRF	Performance Requirements
INT	Integration Requirements
AUD	Audit Requirements

3.2.1 Functional Requirement

We will try to clarify the services the system should provide, how the system should respond to specific inputs, and how the system should behave in specific circumstances in our Functional Requirements. Our project includes many functional requirements. These requirements are gathered, organized, and ordered through the requirement gathering methods mentioned above, and finally, we have used the elicitation process to choose the best one, more appropriate, and these functionalities are used as a backbone for the system.

Super Admin Requirements (SAR)

- **SAR01** [HIGH]: Login to the system using secure authentication mechanisms.
- **SAR02** [HIGH]: Manage and monitor all registered users across institutions.
- **SAR03** [HIGH]: Grant and revoke access for institutional admins and users.
- **SAR04** [MEDIUM]: Generate system-wide reports on usage, performance, and security.
- **SAR05** [MEDIUM]: Configure and maintain role-based access permissions for institutions.
- **SAR06** [MEDIUM]: Oversee integration with external systems, such as driving license or school databases.

Institutional Admin Requirements (IAR)

- **IAR01** [HIGH]: Login to the system using institution-specific credentials.
- **IAR02** [HIGH]: View and manage user IDs within their institution's domain.
- **IAR03** [HIGH]: Approve or deny user requests for ID updates or renewals.
- **IAR04** [MEDIUM]: Access reports related to institution-specific operations.
- **IAR05** [MEDIUM]: Perform biometric validations for ID issuance.
- **IAR06** [LOW]: Communicate with the super admin regarding system issues or updates.

User Requirements (USR)

- **USR01** [HIGH]: Register on the system using personal and biometric data.
- **USR02** [HIGH]: Login to the system to view and update their multi-purpose ID information.
- **USR03** [HIGH]: Download their ID in PDF or QR code format.
- **USR04** [HIGH]: Check ID expiration dates and renewal schedules.
- **USR05** [MEDIUM]: Receive notifications and alerts regarding their ID status.
- **USR06** [LOW]: Submit requests for updates to their ID information, such as name changes.

Other ID Issuing Institutions Requirements (OIR)

- **OIR01** [HIGH]: Provide API access for the system to fetch driving license, work ID, or school ID data.
- **OIR02** [HIGH]: Ensure data from their databases is accurate, up-to-date, and accessible via the integration.
- **OIR03** [MEDIUM]: Collaborate with the system administrators to validate data-sharing agreements.
- **OIR04** [MEDIUM]: Ensure that institutional database systems meet security and privacy standards required by the system.

3.2.2 Non-Functional Requirement

Availability Requirements (AVL)

- **AVL01** [HIGH]: Ensure the system is available 99.9% of the time for all users.
- **AVL02** [HIGH]: Implement failover mechanisms to handle server downtime.

- **AVL03** [MEDIUM]: Provide a maintenance schedule to minimize disruptions.

Interoperability Requirements (INT)

- **INT01** [HIGH]: Support seamless integration with external systems, such as driving license and school ID databases.
- **INT02** [HIGH]: Ensure compatibility with institutional APIs for data fetching and updates.
- **INT03** [MEDIUM]: Allow cross-platform compatibility for mobile and web applications.

Maintainability Requirements (MNT)

- **MNT01** [HIGH]: Ensure the system codebase follows clean coding practices for easier updates.
- **MNT02** [MEDIUM]: Provide comprehensive documentation for developers and administrators.
- **MNT03** [MEDIUM]: Regularly monitor and update dependencies to avoid compatibility issues.

Performance Requirements (PER)

- **PER01** [HIGH]: Ensure that biometric data processing takes no longer than 2 seconds.
- **PER02** [HIGH]: Optimize the system to handle up to 10,000 concurrent users without degradation.
- **PER03** [MEDIUM]: Ensure response times for API calls do not exceed 1 second on average.

Reliability Requirements (REL)

- **REL01** [HIGH]: Design the system to recover automatically from failures within 10 seconds.
- **REL02** [MEDIUM]: Perform regular backup operations to prevent data loss.
- **REL03** [MEDIUM]: Test system reliability under load conditions twice a year.

Security Requirements (SEC)

- **SEC01** [HIGH]: Use AES encryption for all stored biometric and personal data.
- **SEC02** [HIGH]: Implement OAuth 2.0 for secure authentication and authorization.
- **SEC03** [HIGH]: Regularly perform penetration testing to identify and resolve vulnerabilities.
- **SEC04** [MEDIUM]: Encrypt all communication between the client and server using TLS.

Usability Requirements (USE)

- **USE01** [HIGH]: Design an intuitive and user-friendly interface for both mobile and web apps.
- **USE02** [HIGH]: Provide multilingual support to cater to Ethiopia’s diverse linguistic groups.
- **USE03** [MEDIUM]: Include accessibility features such as voice navigation and screen reader support.

3.3 System Modeling

3.3.1 Overview

This chapter examines the basic requirements elicited throughout the requirement elicitation process. Different requirement modeling approaches are used to examine and elaborate on the system's needs and identify critical components in order to develop a system that will efficiently fulfill its goals.

This chapter is divided into three sections focused on different types of modeling. The first section deals with scenario-based modeling represented by the use case and activity diagrams. Then, the second section will show how to do behavioral modeling with the sequence and state diagrams. The last section will treat class-based modeling by using class diagrams.

3.3.2 Scenario Based Modeling

This section tries to describe the various scenarios linked with the system and its users. It will contain subsections like actor identification, which describes the actors of the system, use case identification, describing all the use cases associated with the system, and use case mapping, which will connect the actors to the use case. Details of each use case were drawn using the use case diagrams and use case descriptions. The final section shall contain the activity diagram showing activities involved in realizing the different use cases.

3.3.2.1 Actor Identification

Table 3.3 System Actors

Actor ID	Actor	Description
AC001	Super Administrator	The central authority responsible for managing the entire identity system, including assigning roles and overseeing compliance with system policies.
AC002	User	Individuals who use the identity management system to access services, manage their profiles, or obtain identity documents.
AC003	Institutional Admin	Administrators from institutions (e.g city offices) responsible for managing and verifying the IDs of their members.
AC004	Other ID Issuing Institutions	External organizations or agencies that issue specific IDs (e.g., driver's licenses, work IDs) and integrate them into the broader identity system.

3.3.2.2 Use Case Identification

Table 3.4 Use Case

ID	Use Case Name	Brief Description

UC01	Login	Enables Super Admin, Institutional Admin, and Users to log in securely using their credentials.
UC02	Logout	Allows Super Admin, Institutional Admin, and Users to log out and terminate their session securely.
UC03	Manage Institutions	Allows Super Admin to add, update, or deactivate institutions.
UC04	Manage Institution Records	Enables Super Admin and Institutional Admin to manage records specific to their institutions.
UC05	Register User for an ID	Allows Institutional Admin to register a new user and issue an ID.
UC06	Request ID Update	Allows Users to request updates or modifications to their existing ID information.
UC07	Update User ID	Enables Institutional Admin to process ID update requests from users and make necessary modifications.
UC08	Notify User for ID Renewal	Allows Institutional Admin to notify users when their ID is due for renewal.
UC09	Schedule ID Renewal	Enables Users to schedule a renewal for their ID after receiving a notification.
UC10	Link External IDs	Allows Institutional Admin to link external IDs such as driving licenses or school IDs to a user’s account.
UC11	View Linked ID Details	Allows Super Admin, Institutional Admin, and Users to view details of linked external IDs.
UC12	Fetch External ID Data	Enables Institutional Admin and Other ID Issuing Institutions to retrieve data from external ID databases.

UC13	Validate External ID Data	Allows Institutional Admin and Other ID Issuing Institutions to validate the accuracy of linked external ID data.
UC14	Manage Integration Health	Enables Institutional Admin to monitor and manage the health of external integrations with the system.

3.3.2.3 Use Case Mapping

The purpose of this section is demonstrating which actor is associated with each use case

Table 3.5 Use Case Mapping

ID	Use Case Name	Actors
UC01	Login	Super Admin, Institutional Admin, User
UC02	Logout	Super Admin, Institutional Admin, User
UC03	Manage Institutions	Super Admin
UC04	Manage Institution Records	Super Admin, Institutional Admin
UC05	Register User for an ID	Institutional Admin
UC06	Request ID Update	User
UC07	Update User ID	Institutional Admin
UC08	Notify User for ID Renewal	Institutional admin
UC09	Schedule ID Renewal	User
UC10	Link External IDs	Institutional admin
UC11	View Linked ID Details	Super Admin, Institutional Admin, User
UC12	Fetch External ID Data	Institutional Admin, Other ID Institutions
UC13	Validate External ID Data	Institutional Admin, Other ID Institutions
UC14	Manage Integration Health	Institutional Admin

3.3.2.4 Use Case Diagram

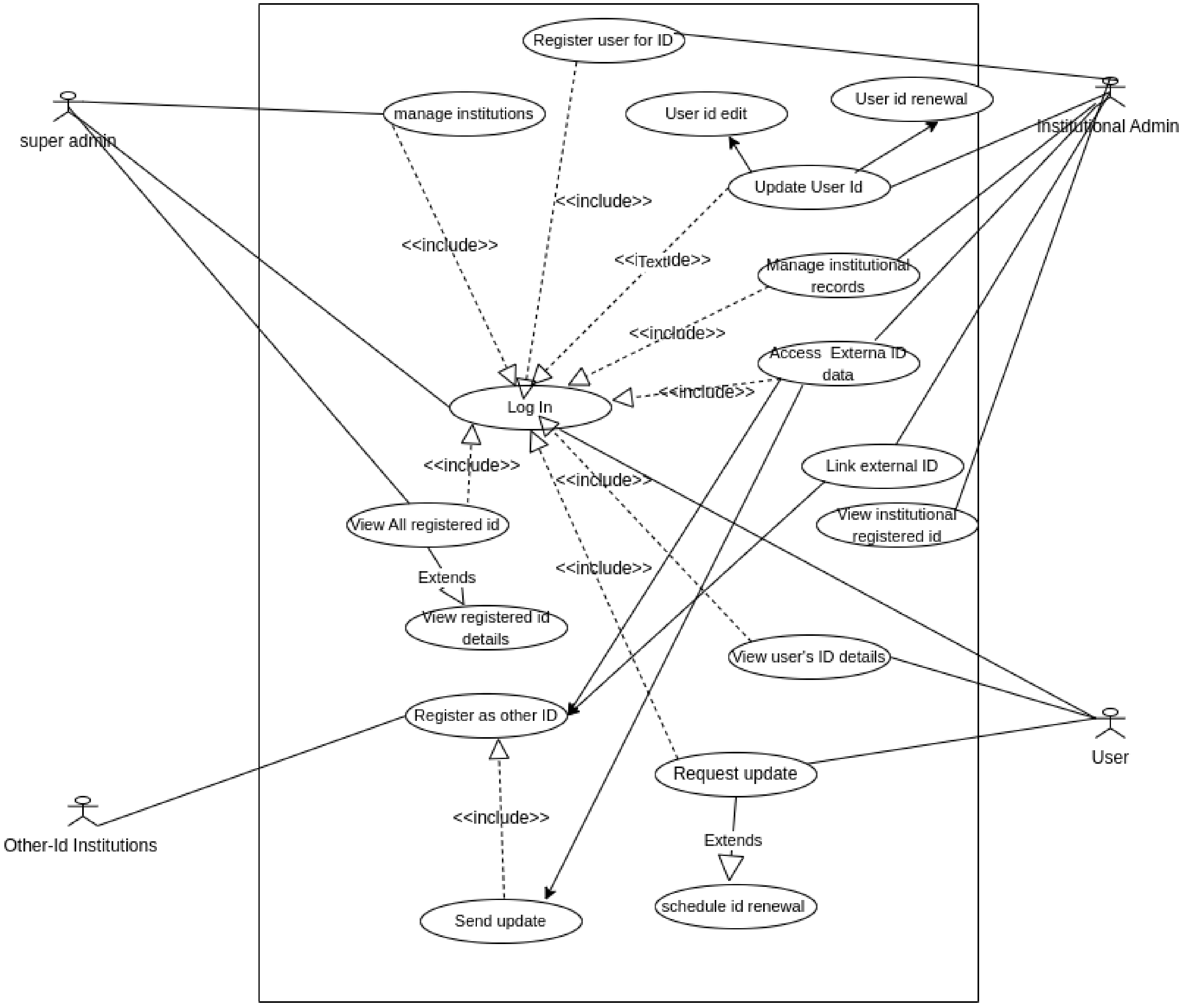

Fig 3.1 Use Case Diagram : Internal Usage

3.3.2.5 Use Case Description

This section will list out all the use cases with their respective details

Table 3.6 Use case description: Login

Use Case ID	UC01	
Use Case Name	Login	
Priority	[HIGH]	
Description	Allows users to log in to the system using secure credentials	
Trigger	A user clicks the “Login” button on the landing page.	
Actors	Super Admin, Institutional Admin, User	
Preconditions	Users must have valid credentials.	
Main Flow	**User** Navigates to the login page and views input fields for email and password along with the "Login" button	**System**
		Checks for empty fields, email format, and password complexity.
		Queries the database for the user account associated with the provided email address.
	Enter their email and password and click the “Login” button.	Compares the provided password with the stored, encrypted password If **Match** continues to the next step If **No Match** displays an error message.
		Identifies the user's role (Super Admin, Institutional Admin, or User) based on the account details.
		Creates a session for the user

		Redirects the user to their role-specific dashboard
		Confirms successful login with a welcome message or notification
Alternate Flow	None	
Exception	Invalid credentials entered.	
Postcondition	Users are logged in with appropriate access.	

Table 3.7 Use case description: Logout

Use Case ID	UC02	
Use Case Name	Logout	
Priority	[HIGH]	
Description	Allows users to securely log out from the system.	
Trigger	User selects the “Logout” option from the dashboard.	
Actors	Super Admin, Institutional Admin, User	
Preconditions	User must be logged in.	
Main Flow	**User**	**System**
	Selects the “Logout” option from the dashboard menu or interface.	Captures the logout request and confirms the user’s intent if a confirmation dialog is shown.
		Invalidates the user’s session (removes user’s session, clears cookies from local storage)
	Views the landing page, confirming they have successfully logged out.	Logs the user’s logout activity in the system logs for auditing or tracking purposes.
		Redirects the user to the landing page (or login page), displaying a confirmation message.
Alternate Flow	None	
Exception	System fails to clear session data.	
Postcondition	User is logged out, and session data is cleared.	

Table 3.8 Use case description: Manage Institutions

Use Case ID	UC03
Use Case Name	Manage Institutions - Manage Roles and Access Levels
Priority	[HIGH]

Description	Allows the Super Admin to manage institutions and user roles/permissions.	
Trigger	Super Admin selects “Manage Institutions” or "Manage Roles" from the dashboard.	
Actors	Super Admin	
Preconditions	System is online, and institutions/users exist in the system.	
Main Flow	**User**	**System**
	Navigates to the “Manage Institutions” or “Manage Roles” option from the dashboard.	Displays a list of existing institutions and roles with options to add, update, or delete.
	Selects an action : Add Institution, Update Institution, Add Role, Update Role	Validates the input data for accuracy and completeness.
		Updates the database with the new or modified institution/role data.
	Review the updated list to confirm changes have been applied.	Displays a confirmation message indicating the update or addition was successful.

Alternate Flow	None
Exception	Input validation fails.
Postcondition	Institutions and user roles/permissions are updated successfully.

Table 3.9 Use case description: Manage Institution Records

Use Case ID	UC04
Use Case Name	Manage Institution Records
Priority	[MEDIUM]
Description	Allows Institutional Admin to add or update records for their institution.
Trigger	Institutional Admin selects “Manage Records” from the menu.
Actors	Institutional Admin
Preconditions	Records must already exist in the database.

Main Flow	**User**	**System**
	Navigates to the **“Manage Records”** option in the menu.	Displays a list of existing institution records with options to add or update.
	Selects an action: Add Record, Update Record	Validates the input data to ensure correctness and completeness.
		Updates the database with the new or modified record information.
	Reviews the updated records to confirm changes have been applied.	Displays a confirmation message indicating the record was successfully added or updated.
Alternate Flow	None	
Exception	Input validation fails.	
Postcondition	Institution records updated successfully.	

Table 3.10 Use case description: Register for an ID

Use Case ID	UC05
Use Case Name	Register for an ID
Priority	[HIGH]
Description	Allows Institutional Admin to register and apply for an ID on behalf of a user.
Trigger	Admin selects “Register ID” option.
Actors	Institutional Admin
Preconditions	Admin must provide all required details.

Main Flow	**User**	**System**
	Selects the “Register ID” option.	Displays the registration form to input user details.
	Completes the registration form by providing all required details	Validates the provided data for correctness and completeness with external data.

	including biometric data.	Saves the valid data to the database.
	Reviews the confirmation to ensure the registration was completed.	Displays a confirmation message indicating that the user has been successfully registered.
Alternate Flow	None	
Exception	Required data not provided.	
Postcondition	User registered successfully..	

Table 3.11. Use case description: Request for Update

Use Case ID	UC06	
Use Case Name	Request for Update	
Priority	[HIGH]	
Description	Allows Users to request updates to their ID information.	
Trigger	User selects the “Request Update” option.	
Actors	User	
Preconditions	User must have an existing ID in the system.	
Main Flow	User	System
	Selects the “Request Update” option.	Displays the update request form for the user to fill out.
		Validates the update request for completeness and correctness.
	Fills out the update request form with the necessary changes to their ID information.	Forwards the validated request to the admin for approval.
		Displays a confirmation message indicating that the update request has been submitted successfully.
Alternate Flow	None	
Exception	Request validation fails.	
Postcondition	Update request submitted successfully.	

Table 3.12. Use case description: Update User ID

Use Case ID	UC07	
Use Case Name	Update User ID	
Priority	[HIGH]	
Description	Enables Institutional Admin to update user ID information based on approved requests.	
Trigger	Admin selects a pending request and approves it.	
Actors	Institutional Admin	
Preconditions	Update requests must exist and be approved.	
Main Flow	User	System
	Selects a pending request for updating user ID information.	Updates the user ID information in the database based on the approved request.
	Approves the request and modifies the user's ID data as required.	
	Reviews the updated user ID information to confirm the changes were applied successfully.	Sends a notification to the user informing them that their ID has been updated.
Alternate Flow	None	
Exception	Update operation fails.	
Postcondition	User ID updated successfully.	

Table 3.13. Use case description: Notify User for ID Renewal

Use Case ID	UC08
Use Case Name	Notify User for ID Renewal
Priority	[HIGH]
Description	Sends notifications to users for ID renewals.
Trigger	System identifies users whose IDs are about to expire.
Actors	Institutional Admin

Preconditions	ID renewal notifications feature must be configured.	
Main Flow	**User**	**System**
	Receives a notification from the system about users who need to be reminded of ID renewal.	Identifies users whose IDs are about to expire based on pre-configured rules.
	Monitors the renewal status and ensures notifications are sent as per the rules.	Sends out notifications to users whose IDs are nearing expiration, reminding them to renew.
Alternate Flow	None	
Exception	Notification system fails.	
Postcondition	Users notified for renewal.	

Table 3.14 Use case description: Schedule ID Renewal

Use Case ID	UC09	
Use Case Name	Schedule ID Renewal	
Priority	[HIGH]	
Description	Allows Users to schedule ID renewal appointments.	
Trigger	User selects “Schedule Renewal”.	
Actors	User	
Preconditions	User must be logged in and notified for renewal.	
Main Flow	User	System
	Selects the “Schedule Renewal” option.	Displays available dates and times for ID renewal appointments.
		Validates the selected date and time for availability.
	Selects a preferred date and time for the renewal appointment.	Confirms the appointment and updates the system schedule.
		Sends a confirmation notification to the user with the appointment details.
Alternate Flow	None	

Exception	Appointment scheduling fails.	
Postcondition	ID renewal appointment scheduled.	

Table 3.15 Use case description: Link External IDs

Use Case ID	UC10	
Use Case Name	Link External IDs	
Priority	[HIGH]	
Description	Allows users to link their external IDs for unified management.	
Trigger	Admin clicks “Link External ID”.	
Actors	Institutional admin	
Preconditions	External IDs must exist in the partner database.	
Main Flow	User	System
		Displays a form for the admin to enter the user's primary details (e.g., user ID, name).
	Clicks the “Link External ID” option.	Automatically fetches the user's external ID details from the partner database using the provided primary details.
	Enters and submits the user's primary details.	Verifies the fetched external ID details for accuracy and validity.
		Stores the verified external ID linkage data in the system.
		Displays a confirmation message indicating the external ID was successfully fetched and linked.
Alternate Flow	None	
Exception	External ID verification fails.	
Postcondition	External ID linked successfully.	

Table 3.16 Use case description: View Linked ID Details

Use Case ID	UC11

Use Case Name	View Linked ID Details
Priority	[MEDIUM]

Description	Enables users to view details of their linked external IDs.	
Trigger	User selects “View Linked ID Details”.	
Actors	Super Admin, Institutional Admin, User	
Preconditions	Users must have an existing ID in the system.	
Main Flow	**User**	**System**
		Fetches linked ID details from the database.
	Selects the “View ID Details” option.	Verifies the data integrity and ensures all necessary details are available.
		Displays the linked ID details to the actor in a clear and organized manner.
Alternate Flow	None	
Exception	External ID fetch fails.	
Postcondition	Linked ID details displayed successfully.	

Table 3.17 Use case description: Fetch External ID Data

Use Case ID	UC12	
Use Case Name	Fetch External ID Data	
Priority	[HIGH]	
Description	Allows Institutional Admin or Other ID Institutions to fetch data associated with an external ID.	
Trigger	Admin selects “Fetch External ID Data”.	
Actors	Institutional Admin, Other ID Institutions	
Preconditions	Valid external ID linkage must exist.	
Main Flow	User	System

	Enters the details of the fetched ID.	Fetches the associated data from the external database or linked system.
	Selects the “Fetch External ID Data” option.	Fetches the associated data from the external database or linked system. Displays the retrieved external ID data to the actor in a structured and accessible format.
Alternate Flow	None	
Exception	External ID data retrieved successfully.	
Postcondition	External ID data retrieved successfully.	

Table 3.18 Use case description: Validate External ID Data

Use Case ID	UC13	
Use Case Name	Validate External ID Data	
Priority	[HIGH]	
Description	Allows Institutional Admin or Other ID Institutions to validate data of an external ID.	
Trigger	Admin selects “Validate External ID Data”.	
Actors	Institutional Admin, Other ID Institutions	
Preconditions	External ID data must be available for validation.	
Main Flow	**User**	**System**
	Provides user ID details	Compares the submitted data with the stored or external database records.
	Prompt’s the system to fetch related external data	Confirms if the data is valid or flags inconsistencies in the external ID data. Provides a detailed report of the validation status, including flagged issues if any.
Alternate Flow	None	
Exception	Data validation fails due to inconsistencies.	
Postcondition	External ID data validated successfully.	

3.3.3 Behavioral / Dynamic Modeling

In this system, behavioral modeling captures the flow of processes and interactions between users, administrators, and the system. It highlights how key functionalities, such as ID registration, updates, and renewal scheduling, operate dynamically over time. This approach ensures that the system's workflows, including login, logout, external ID integration, and notification handling, are logically structured and efficient. By illustrating how the system adapts to user actions and external events, the modeling ensures that all components work cohesively to deliver a seamless user experience.

3.3.3.1 Sequence Diagram

The sequence diagram provides a clear visualization of the interactions between users, administrators, and the system components in a time-ordered sequence. It demonstrates how requests and responses are exchanged to perform critical operations like user authentication, ID registration, updates, external data fetching, and renewal scheduling. By detailing the flow of messages and processes, the sequence diagram ensures alignment between system requirements and user expectations, facilitating a better understanding of how the system handles tasks dynamically.

Login and Logout

The sequence diagram for login and logout illustrates the interactions between the user and the system. During login, the process begins with the user entering their credentials (email and password) and submitting them. The system validates the input, verifies the credentials against the database, and determines the user's role. Upon successful validation, the system establishes a session and redirects the user to the appropriate dashboard based on their role (Super Admin, Institutional Admin, or User). If the credentials are invalid, the system notifies the user with an error message.

For logout, the user initiates the action by selecting the logout option. The system terminates the session, clears the authorization data, and redirects the user to the landing page.

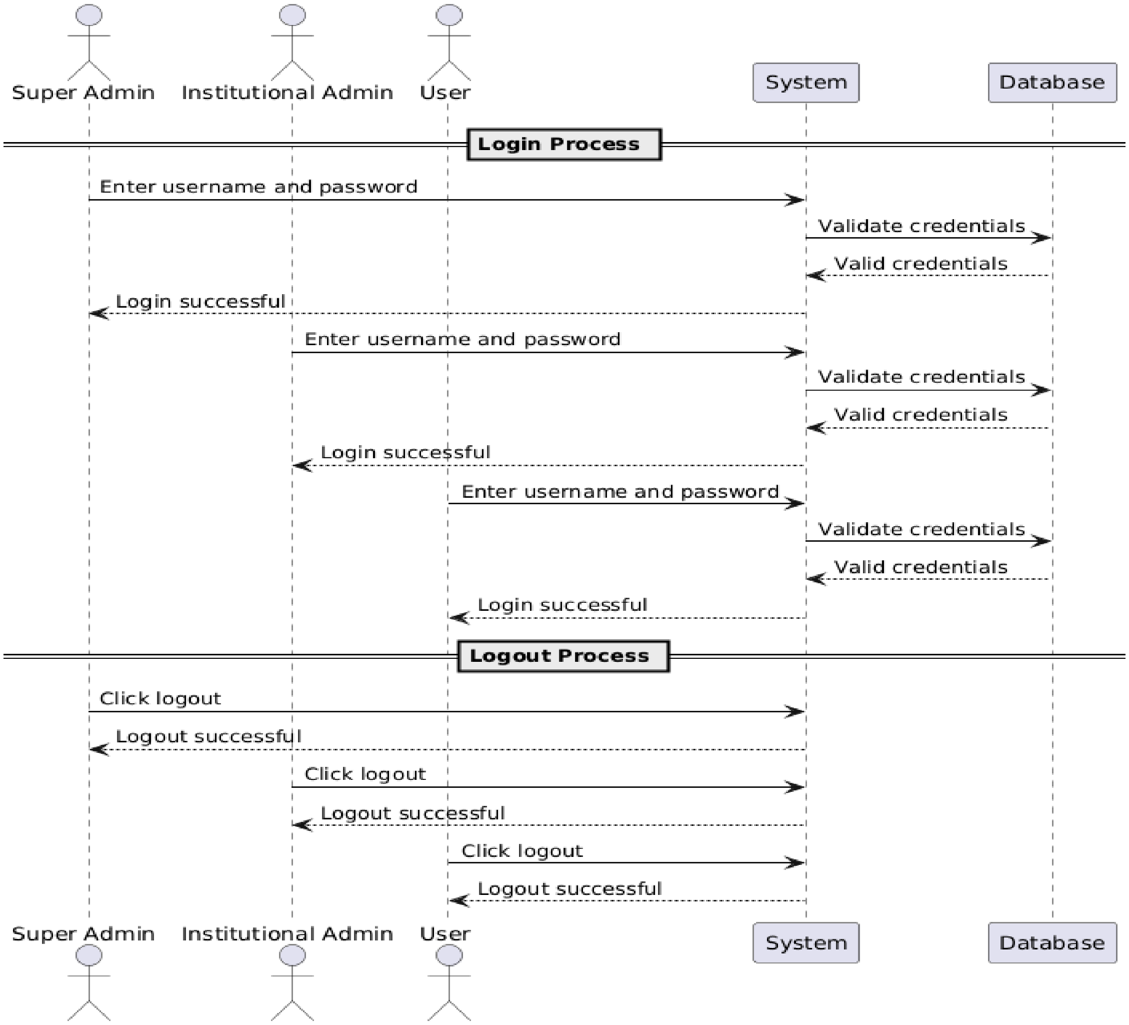

Fig 3.3 Login and Logout Sequence Diagram

Register, Update, Notify, and Schedule ID Renewal

This sequence covers ID registration, updates, renewal notifications, and scheduling. Institutional Admins register users by submitting their details, which the system validates and stores. Updates to user information are made by the admin upon request, with the system validating and reflecting changes. For IDs nearing expiration, the system sends automated renewal notifications. Users can then schedule renewal appointments, with the system confirming and managing the schedule. This streamlined process ensures accurate user data and proactive ID management.

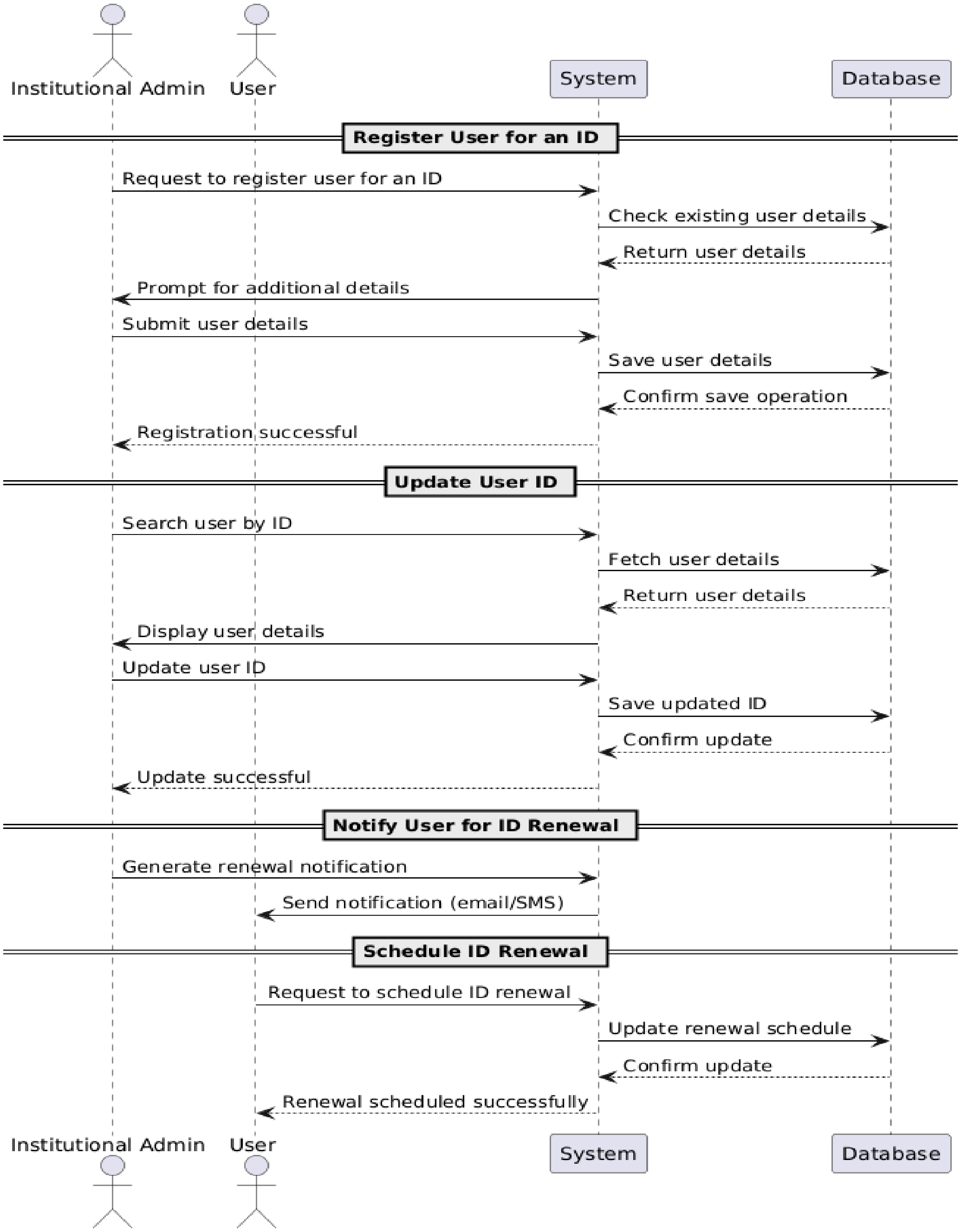

Fig 3.4 User Registration Sequence Diagram

Manage Institutions

The sequence diagram for managing institutions outlines the steps the Super Admin takes to add or update institution records. The process starts when the Super Admin selects the "Manage Institutions" option. They input details such as the institution's name, type, and contact information and submit the request. The system validates the data, checks for duplicates, and updates the database by either adding a new institution or modifying an existing one. Once the process is complete, the system provides confirmation to the Super Admin and updates the institution list for future reference.

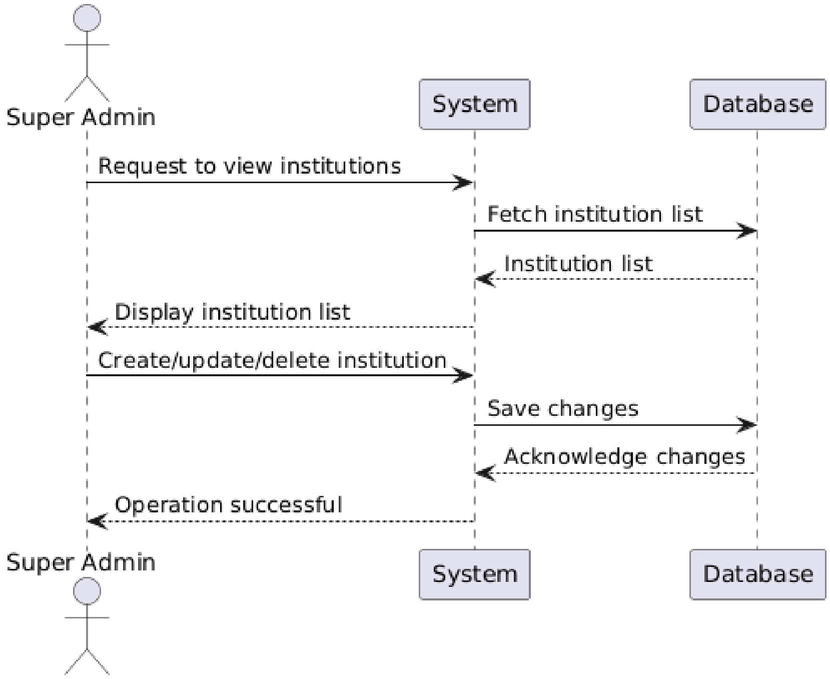

Fig 3.5 Manage Institutions Sequence Diagram

Fig 3.3.3 Manage Institutions

External-ID Process

The External ID process begins with fetching an external ID from partner databases based on user-provided details. Once retrieved, the system validates the ID by verifying its authenticity and matching it with the user's existing records. Upon successful validation, the ID is linked to the user's profile within the system, ensuring seamless integration. Finally, the system displays the finalized linked ID details, providing users with a consolidated view of their external and internal ID information for streamlined identity management.

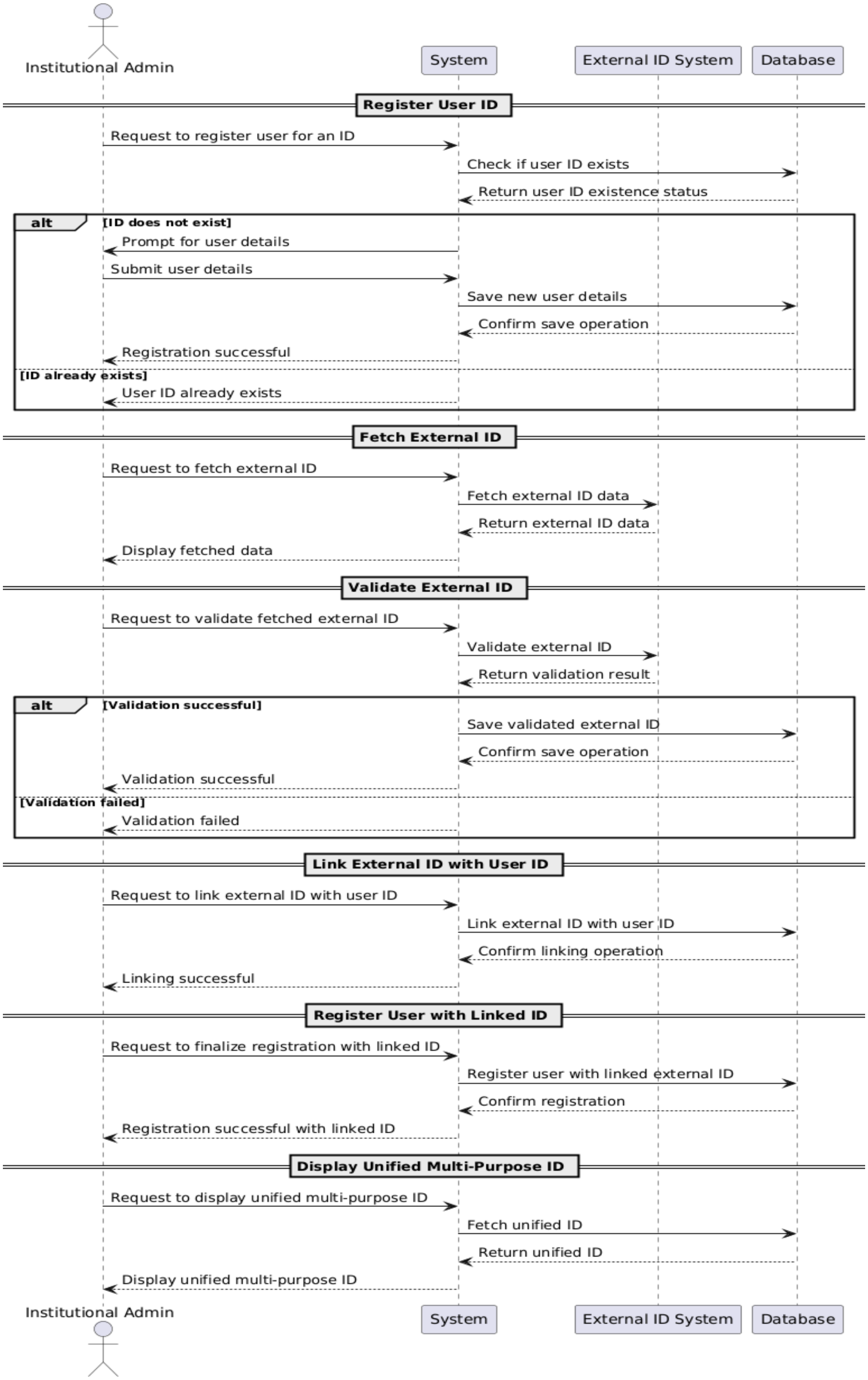

Fig 3.6 External Data Sequence Diagram

3.3.3.2 Activity Diagram

Register User

The activity diagram for the registration process illustrates the flow from user registration to the final ID display. It starts with the user submitting registration details, followed by the system fetching external ID data. The fetched data undergoes validation to ensure accuracy and authenticity. Once validated, the external ID is linked to the user's profile. Finally, the system consolidates and displays the linked final ID, completing the registration process.

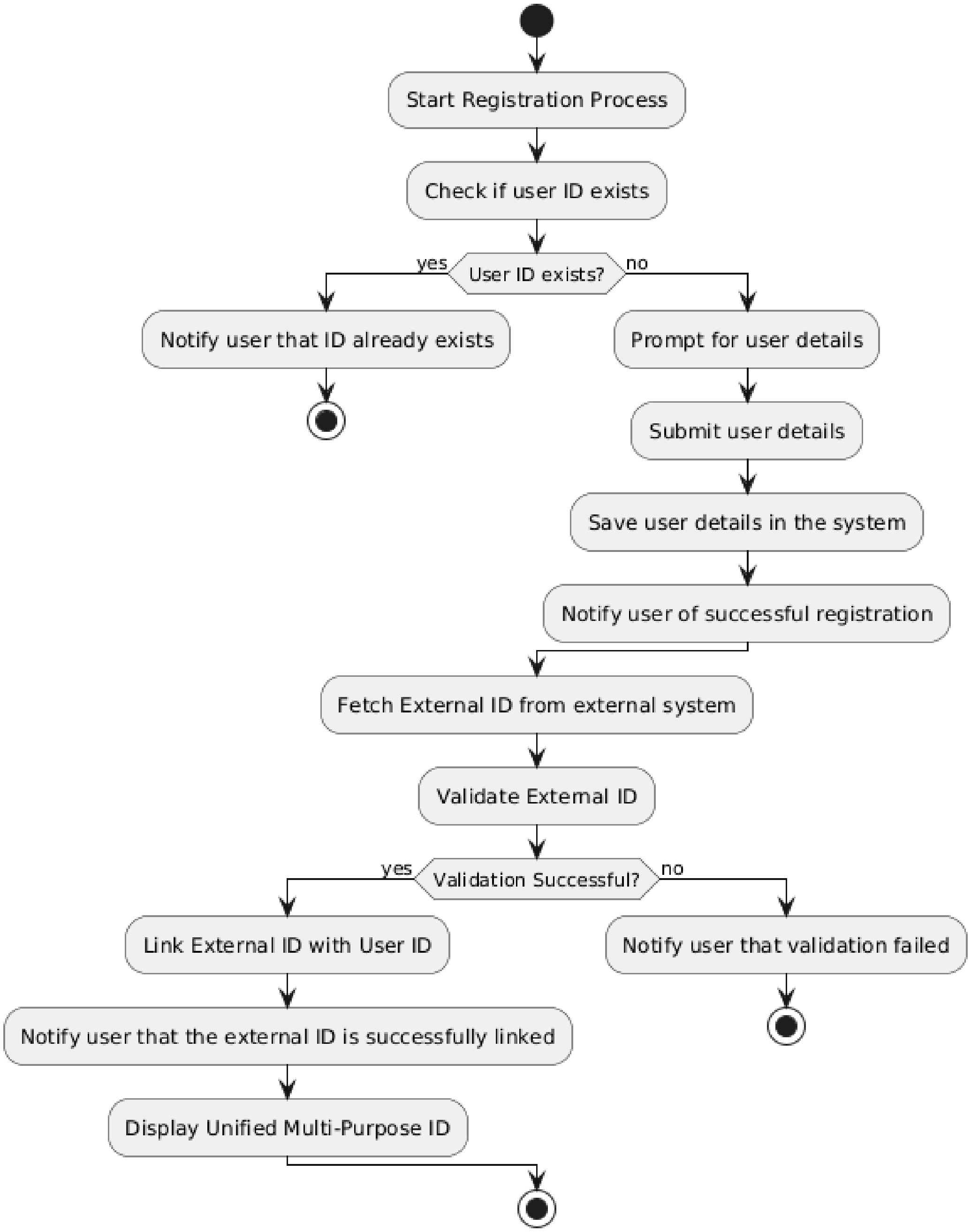
Start Registration Process
Check if user ID exists
User ID exists?
yes
no
Notify user that ID already exists
Prompt for user details
Submit user details
Save user details in the system
Notify user of successful registration
Fetch External ID from external system
Validate External ID
Validation Successful?
yes
no
Link External ID with User ID
Notify user that validation failed
Notify user that the external ID is successfully linked
Display Unified Multi-Purpose ID

Fig 3.7 Register User Activity Diagram

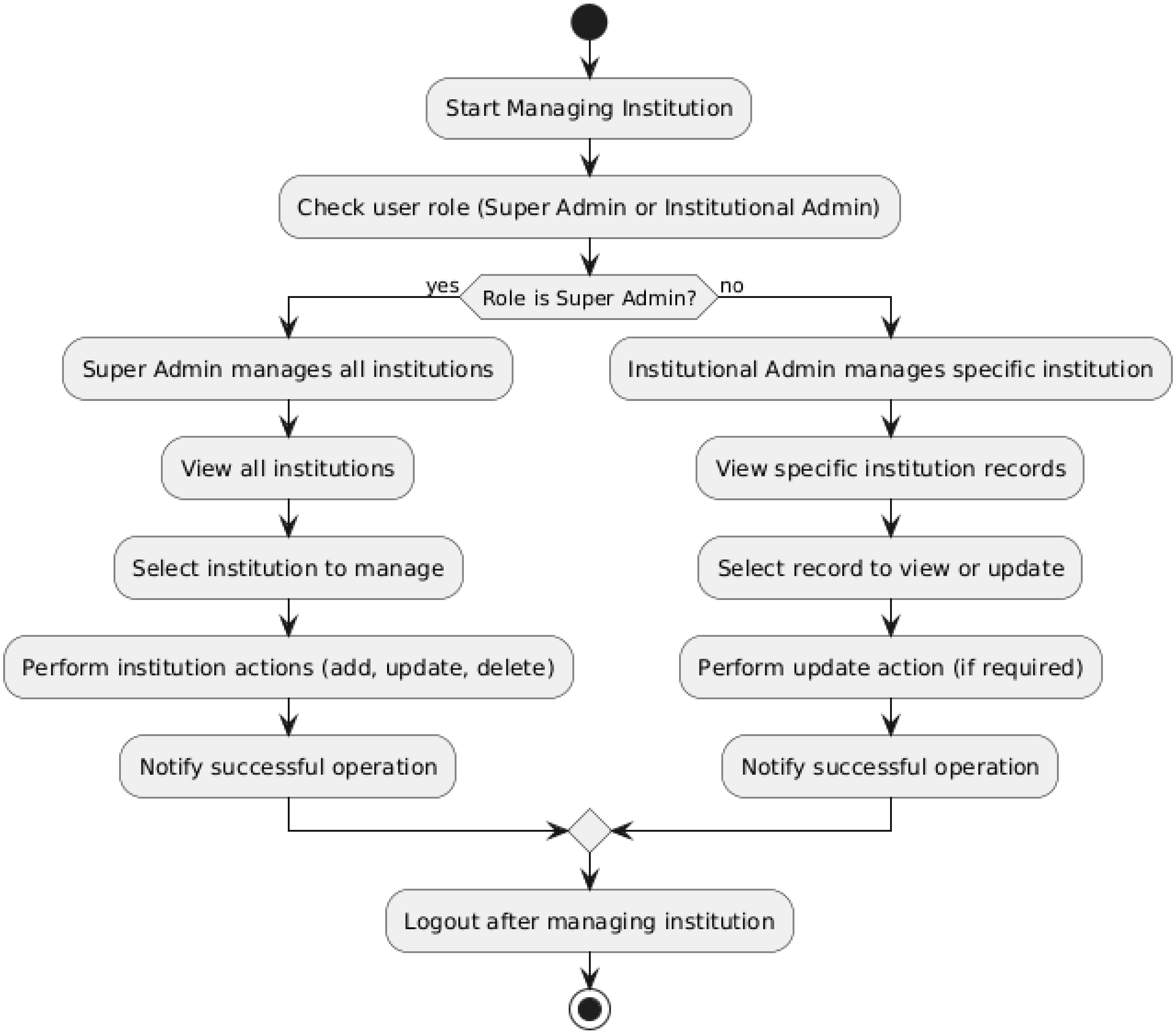
Start Managing Institution
Check user role (Super Admin or Institutional Admin)
yes
Role is Super Admin?
no
Super Admin manages all institutions
Institutional Admin manages specific institution
View all institutions
View specific institution records
Select institution to manage
Select record to view or update
Perform institution actions (add, update, delete)
Perform update action (if required)
Notify successful operation
Notify successful operation
Logout after managing institution

Fig 3.8 Manage Institutions Activity Diagram

3.3.3.3 State Diagram

The state diagram illustrates the system's behavior as it transitions between states during key processes like user login, ID registration, validation, and institution management. Starting from an idle state, actions like login lead to authentication, followed by processes such as registering, fetching, and validating IDs, ultimately finalizing and linking them. For administrators, states include managing institutions, sending notifications, and approving updates. The system returns to idle after logout or task completion, showcasing a seamless flow of interactions.

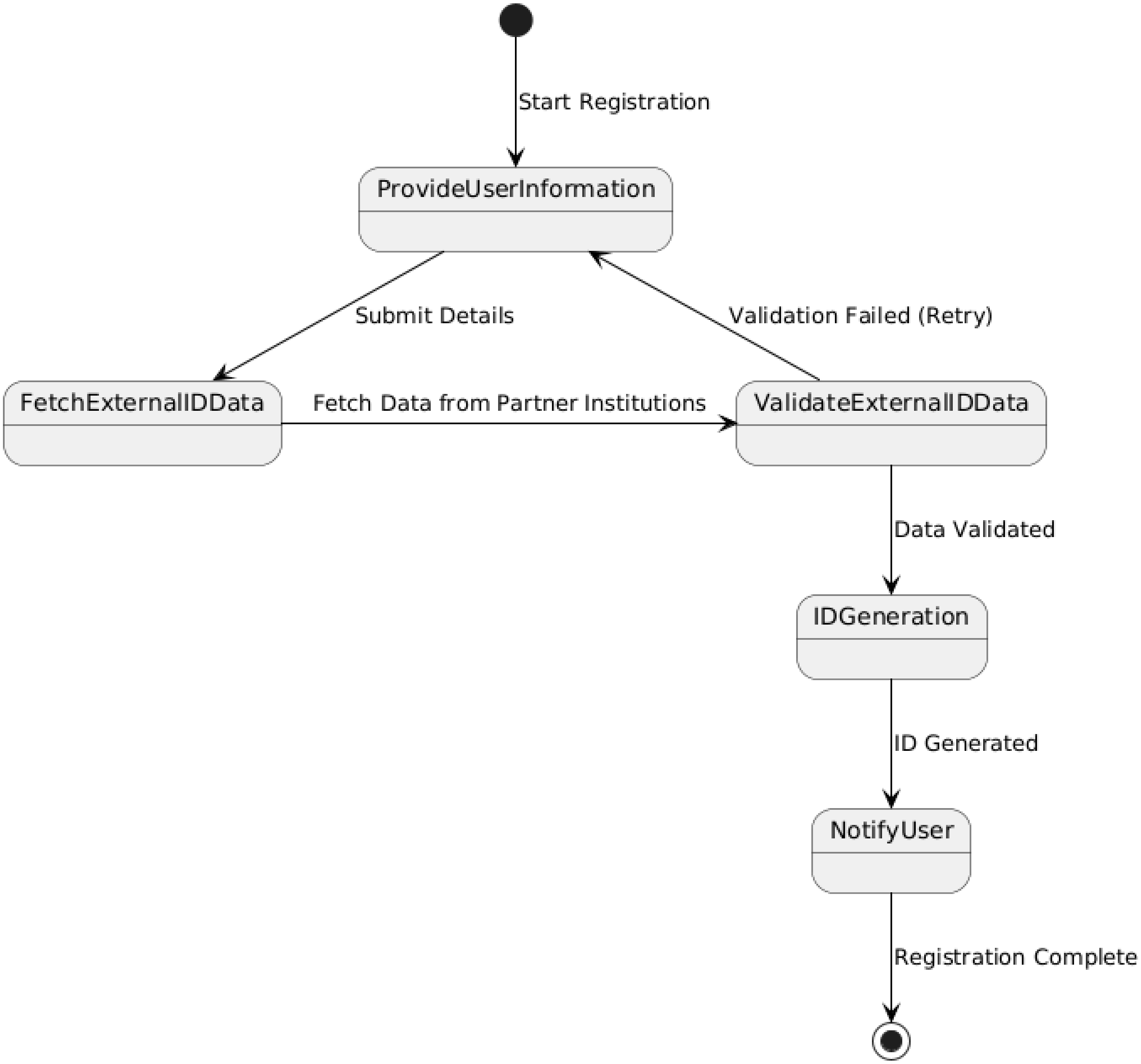

Fig 3.9 Register User StateDiagram

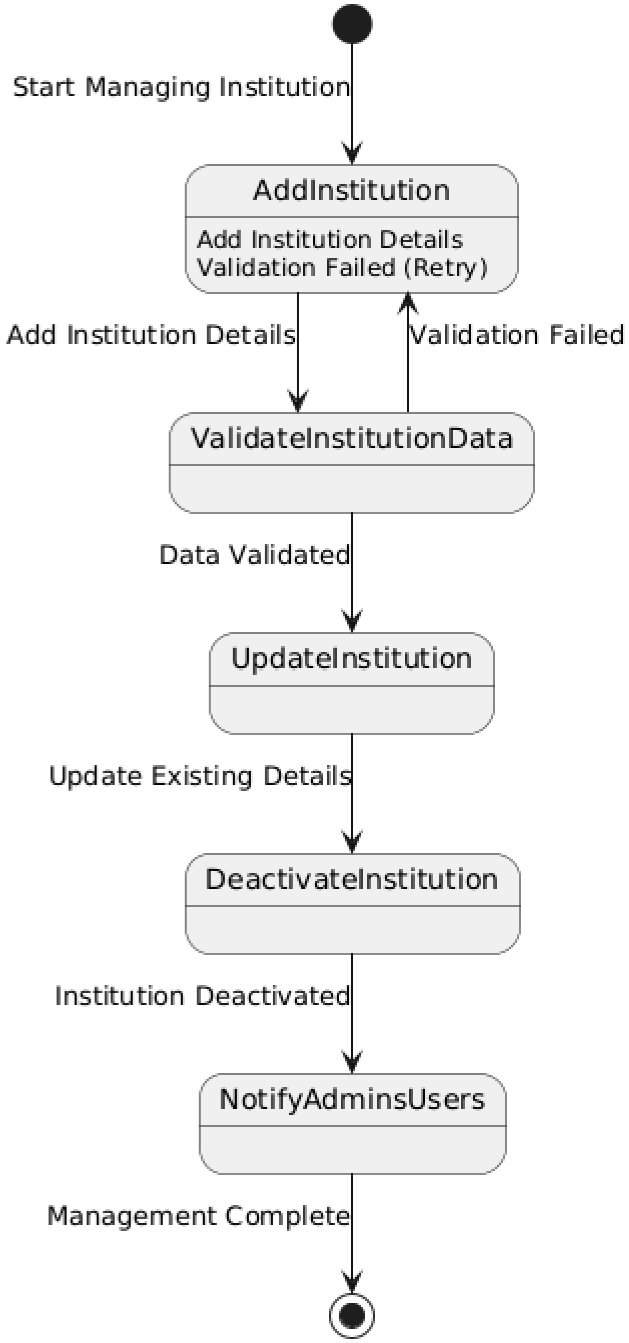

Fig 3.10 Manage Institutions State Diagram

3.3.4 Class-Based Modeling

Table 3.23. Class Description

Class Name	Description	Relevant Tasks
User	Manages data related to users, including personal details, credentials, and linked IDs.	Login, Logout, Register for ID, Request ID Update, Schedule ID Renewal
Institution	Represents organizations participating in the system, storing institutional data and managing associated users	Manage Institution Records, Assign Roles
Super Admin	Handles administrative tasks for managing institutions, and system configurations.	Manage Institutions, Add Institutions, Delete institutions
Institutional Admin	Handles administrative tasks for managing users, institution, and system configurations.	Manage Institutions, Approve/Reject ID Updates, Notify Users for Renewal
ID	Stores and tracks ID-related data, including linked external IDs and renewal details.	Register ID, Validate External ID, Link External ID, Schedule Renewal
Report	Generates and stores analytical and performance data related to system usage and institutional activities.	View System Analytics, Generate Reports
ExternalID	Manages data integration and validation for external IDs from partner systems.	Fetch External ID, Validate External ID, Link External ID
Notification	Handles sending reminders and updates to users regarding ID renewals and other system alerts.	Notify User for ID Renewal
Session	Tracks user sessions, including login/logout history and active session management.	Login, Logout

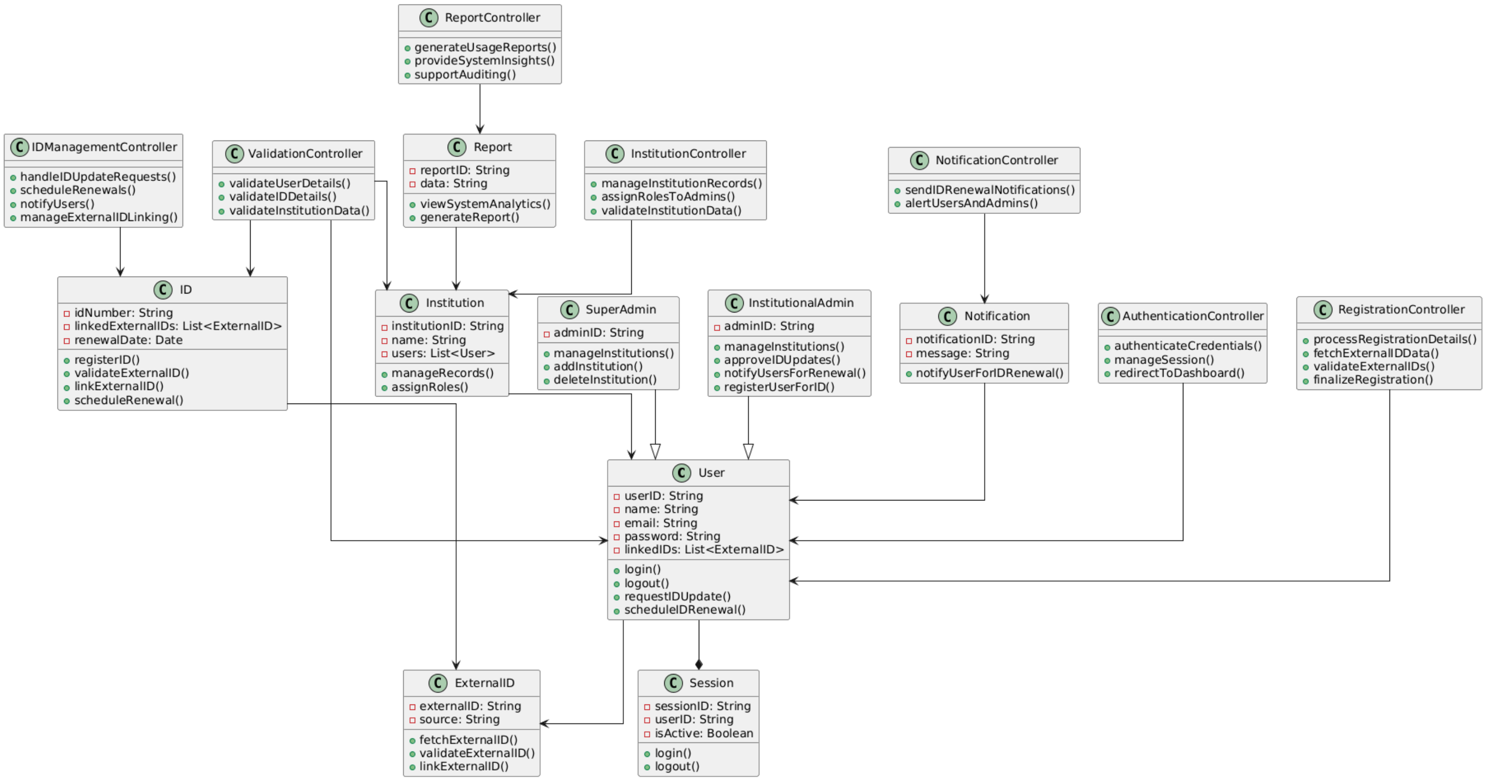

Fig 3.11 Class Diagram

References

[1] “Website.” [Online]. Available: https://nbe.gov.et/wp-content/uploads/2023/04/SBB-59-2014.pdf

[2] “Website.” [Online]. Available: https://nbe.gov.et/files/annual-report-2019-2020-2/

[3] “Technical Difficulties.” Accessed: Jan. 24, 2025. [Online]. Available: https://www.state.gov/executive-order-13224/

[4] J. Daugman, “Biometric decision landscapes,” *Pattern Recognit.*, vol. 34, no. 2, pp. 272–284, 2001.

[5] A. Ross and A. Jain, “Biometric sensor interoperability: A case study in fingerprints,” in *Biometrics: Theory, Applications, and Systems (BTAS)*, 2008, pp. 1–8.

[6] K. Patton, *Qualitative Evaluation Methods*, 3rd ed. Thousand Oaks, CA: Sage Publications, 2002.

[7] G. E. P. Box, J. S. Hunter, and W. G. Hunter, *Statistics for Experimenters: Design, Innovation, and Discovery*, 2nd ed. Wiley, 2005.

[8] E. Windmill, *Flutter for Mobile Developers: An Introduction*, 1st ed. Birmingham, England: Packt Publishing, 2019.

[9] K. Bowyer, P. Flynn, and P. Phillips, “Introduction to the special issue on biometrics,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 389–393, 2007.

[10] “Quick Start.” Accessed: Jan. 24, 2025. [Online]. Available: https://react.dev/learn

[11] “Getting started with Django,” Django Project. Accessed: Jan. 24, 2025. [Online]. Available: https://www.djangoproject.com/start/

[12] “Documentation.” Accessed: Jan. 24, 2025. [Online]. Available: https://www.postgresql.org/docs/

[13] A. Smith, “The cost of fraud in digital identification systems,” *J. Econ. Perspect.*, vol. 28, no. 3, pp. 75–90, 2018.

[14] Unique Identification Authority of India, “Aadhaar overview.”

[15] M. Nilekani and R. Shah, *Rebooting India: Realizing a Billion Aspirations*. Harlow, England: Penguin Books, 2015.

[16] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Springer Science & Business Media, 2007. [Online]. Available: https://books.google.com/books/about/Handbook_of_Biometrics.html?hl=&id=WfCowMOvpiC

[17] “Addressing Its Lack of an ID System, India Registers 1.2 Billion in a Decade,” UCLA Anderson Review. Accessed: Jan. 24, 2025. [Online]. Available: https://anderson-review.ucla.edu/addressing-its-lack-of-an-id-system-india-registers-1-2-billion-i n-a-decade/

[18] e-Estonia, “e-Residency overview.”

[19] Government of Kenya, “Huduma Namba implementation report,” Nairobi, Kenya, 2019.

[20] P. Ghosh, “India’s Aadhaar: Big data and governance,” *Econ. Polit. Wkly.*, vol. 50, no. 15, pp.

42–49, Apr. 2015.

[21] D. Kotka, “The making of e-Estonia,” *IEEE Internet Comput.*, vol. 21, no. 4, pp. 78–81, Jul. 2017.

[22] K. P. Mohanty, “Bridging silos: Challenges of interoperability in e-governance systems,” *Journal of Digital Transformation*, vol. 10, no. 3, pp. 115–132, 2020.