Software Requirement Specifications

for

S.M.A.R.T.E.X

Version 2.0

Prepared by

Group: 16 **Group Name: BitEngine**

Danish Mehmood	210297	danishm21@iitk.ac.in
Rikesh Sharma	180606	rikesh@iitk.ac.in
Ajeet Meena	210078	ajeetm21@iitk.ac.in
Kumar Gourav Songara	170353	songara@iitk.ac.in
Anuj Kumar	200164	kanuj20@iik.ac.in
Avinash Saini	200232	avinashs20@iitk.ac.in
Pratiksha Dawane	210760	ppdawane21@iitk.ac.in
Lohit P Talavar	210564	lohitp21@iitk.ac.in

Course: CS253

Mentor TA: Rumit

Date: 22/04/23

`

Revisions

Version	Primary Author(s)	Description of Version	Date Completed
Version 2.0	Danish Mehmood	Final Draft	14/04/2023

1 Introduction

1.1 Product Scope

An Automated Entry Exit System (AEES) is a software solution used to track and manage the movement of people in and out of an area. The purpose of the software is to provide real-time monitoring and control of access to a facility, while also collecting data on the comings and goings of individuals.
Many times, movement inside the campus and constant movement outside the campus necessitates the campus community making an entry into the register-book, which takes a long time and wastes paper. We want to create an automated entry exit system for the campus community to streamline the process.

Some benefits of an AEES include increased security and safety by ensuring that only authorized individuals have access to a facility, improved efficiency by automating the process of checking in and out, and the ability to collect data on who is entering and exiting a facility and when.

Product scope is limited to college but can also be used for organization that need to keep the data of employee's entry and exit and their time of entry and exit. Of Course, it can be modified to attendance system as well. But mostly due to the current manual system of entry and exit which is tedious and tiresome, this system is most suitable for the college entry exit as it is clean, fast and easy.

The main objectives of an AEES are to:

- Control access to a facility by managing the flow of people in and out.
- Monitor the comings and goings of individuals in real-time.
- Collect data on who and when is he/she entering and exiting the facility.
- Increase security and safety of the facility.

The project's goal would be to develop an efficient and secure system for regulating movement on and off campus while also keeping the necessary records for future access by authorised users.

1.2 Intended Audience and Document Overview

This document represents the finalized version of the Software Requirements Document, encompassing all features and requirements that have been addressed during the development process. Throughout the development cycle, this document has undergone revisions and updates, ensuring that it accurately represents the current state of the software. As such, this document now serves as a comprehensive reference for the software's specifications and future maintenance. Please note that any further changes or enhancements to the software will necessitate updates to this document to maintain alignment with the implemented system.

The document is intended for requirements engineer, domain expert, developer and project manager, testers, and documentation writers. The rest of the SRS document contains information about product overview, design, implementation and convention, constraints, and Assumptions. This document also contains detailed information about functional and non-functional requirements for the software and the External Interface details.
The document is best read top-to-down but each section is written in a way that they are self contained so the intended readers can directly refer to the concerned section.

1.3 Definitions, Acronyms and Abbreviations

- **Secure**: System must allow only the authorised user to make entry or exit from the area.
- **Automated**: The system must update entry exit detail with minimum interaction from user. Like by just reading the student ID-card, system should make all the necessary entry in the table and allow access to move in or out of the campus.
- **AEES**: Automated Entry Exit System.
- **SMARTEX**: Smart Automated Entry Exit System.
- **Access control device**: We are using bar-code reader or a mobile phone for now.

1.4 Document Conventions

In general, this document follows the IEEE formatting requirements. Use Arial font size 11, or 12 throughout the document for text. Use italics for comments. Document text should be single spaced and maintain the 1" margins found in this template. For Section and Subsection titles please follow the template.

1.5 References and Acknowledgments

1. IEEE 830 Template

We would like to appreciate to each individual who have helped and supported us during the project .We are thankful to Mr.Indranil Saha our professor who is our support during our project . We would like to thank our TA Mr.Rumit who is there for us at each step of our project and guidingus throughout each step.

We will also like to acknowledge Mr. Filippo Tortomasi for the app Barcode to PC

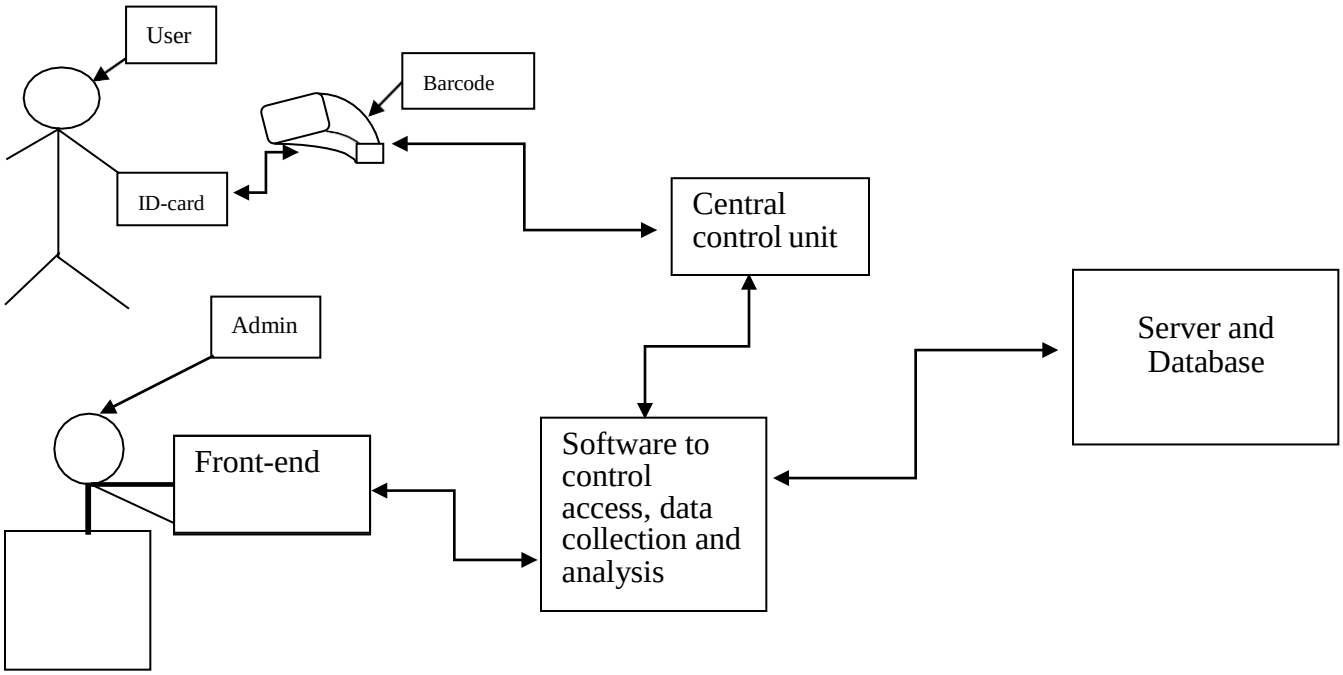
App website: https://barcodetopc.com/
Github: https://github.com/fttx/barcode-to-pc-app

At the end we are thankful towards our group members for being motivated during the project andsharing and understanding each other's opinion and applying it to get the best project.

2 Overall Description

2.1 Product Overview

From a product perspective, an Automated Entry Exit System (AEES) is designed to provide secure and efficient access control for a facility. The system typically consists of a variety of components, including access control devices such as barcode readers or biometric scanners, a central control unit for managing access, and software for collecting and analyzing data.
The system interacts with the environment in several ways. At the point of entry, individuals present their credentials, such as an ID card or biometric data, to the access control device. The device then communicates with the central control unit to verify the individual's identity and authorize or deny access. Once access is granted, the individual can enter the facility. The system also keeps track of the time of entry and exit of individuals.
This system will act as a replacement for the existing manual register entry for movement in and out of the campus. This will help reduce the time and wastage of paper. It will also simplify the process and make the process efficient, secure and less error prone.



2.2 Product Functionality

1. **Access Control**: The system must be able to manage facility access by managing the movement of students into and out of the facility. This includes the ability to authenticate the identification of persons and permit or prohibit their access based on predetermined criteria.
2. **Real-time Monitoring**: The system must offer real-time monitoring of persons' entry and exit from a facility. This includes the ability to monitor who enters and exits the facility and at what time.

3. **Data Collection**: The system must gather information on who enters and exits the facility, as well as the time of their entry and leave. This information may then be used for analysis and reporting.

4. **Security**: The system must ensure that only authorised persons have access to a database about the in and out records, hence enhancing security and safety.

5. **Efficiency**: The system must automate the process of checking in and out, which may assist to increase efficiency and decrease the burden of security employees and reduce the hassle for entering details into the register-book while in and out.

6. **User-friendly**: Both end-users and administrators must be able to utilise and navigate the system without difficulty.

2.3 Design and Implementation Constraints

The main hardware constraint here would be availability of a scanner and a device (most preferably a tablet) at different gates of the campus so that cards can be scanned, and info can be stored on the server. Another constraint is security, the system will contain basic info about the users, we will have to take measures to ensure that the info doesn't get leaked, for that we will have to make sure the system works on the campus intranet only.

2.4 Assumptions and Dependencies

Hardware dependencies

1. Barcode scanner.
2. Mobile/PC device at every check post.

3 Specific Requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

The user interface of the system will include both a physical component and a software component.
The physical component of the user interface includes the access control devices that individuals interact with when entering or exiting the facility. The access control devices will be located at the point of entry and exit and are used to verify the identity of individuals and authorize or deny access.
The software component of the user interface is typically accessed by the system administrator and other authorized users. The software provides a dashboard or control panel that allows guard/admin to manage the system settings, such as creating guard/admin accounts, setting access levels and permissions, and generating reports.

One interface will be for student for filling the data automatically or physically (in case scanner doesn't work).
The UI will have to be as user-friendly as possible by providing descriptive labels, icons, and step-by-step directions for doing common activities.

3.1.2 Hardware Interfaces

For Hardware interface for backend there will be computer for guard, so that person can do his job and for student we will have scanner and computer both for registry of that gate.

For accessing the admin page by the authorized users, the hardware required will be internet enabled desktop.

A barcode scanner or a mobile device may be used for scanning the barcode on student's ID.

At the backend a database is needed to store the information.

3.1.3 Software Interfaces

We aim to include the following elements in our software interface.

An administrative page to access different sections of the system, create manage user accounts, setup different access levels.

A minimal end-user interface for the entering an exit with ideally just scanning the student's ID card.

3.2 Functional Requirements

3.2.1 Authentication: The system must be able to authenticate the identity of individuals using their student's ID card.

3.2.2 A navigation menu: Allows users to access different sections of the system, such as Scan Page, Manual Entry, Daily Statistics, Logout.

3.2.3 An Admin Dashboard: Provide an overview of Daily Statistics status, changing passwords or adding new admin or guard.

3.2.4 Guard management by Admin: Allows admin to create and manage guard and admin accounts

3.2.5 Scanning/Manual entry: Allows guard/admin to help facilitate automatic entry/exit for student/non-students.

3.2.6 Status Check: Guard/Admin should be able to see the status of a student/non-student if he/she is inside or outside the campus.

3.2.7 Daily Statistics: Allows admin to get info on entry and exit daily statistics

3.2.8 Settings: Allows admin to change admin/guard login credentials or add new admin/guard.

3.2.9 Scanning screen: Provide the end-user to ideally scan and enter or exit with minimum other interaction.

3.2.10 Time Recording: The system should be able to record time of entry and exit just after scanning i-card.

3.2.11 Non-Student Registration: People who are not students or don't already have their data in the database should be able to register for the first time so that their data can be stored and their entry/exit can be easier.

3.2.12 History: Admin/Guard must be able to know complete information about entry/exit of any student by putting his details like roll number or user-id.

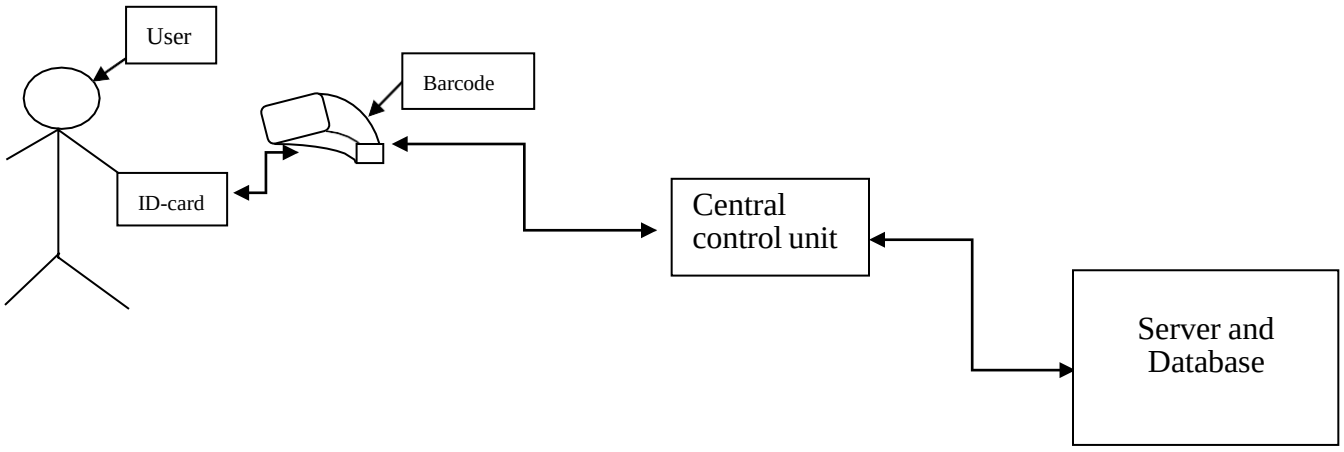
3.2.13 Editing Records: Admin/Guard should be able to edit or delete any entry from the history table in case of wrong information.

3.2.14 Logout: Admin/Guard should be able to logout of the system.

3.3 Use Case Model

In this diagram, a student the access control device, such as a barcode reader, which communicates with the central control unit to verify the individual's identity and authorize or deny access.
The central control unit then communicates with the software for data collection and analysis, which keeps track of the time of entry and exit, and other relevant data.
In context, the system is used in where access to certain area is permitted only after authentication.
The admin front-end to access different sections of the system, create manage user accounts, setup different access levels.

3.3.1 Use Case: UN1



Author – Rikesh Sharma

Purpose – Mimicking regular entry and exit from the campus

Requirements Traceability – Scanning with access control device. Retrieving the data from the barcode of the ID card and generating the date time, name, roll no, entry exit information and sending to central control unit to add it to the database.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

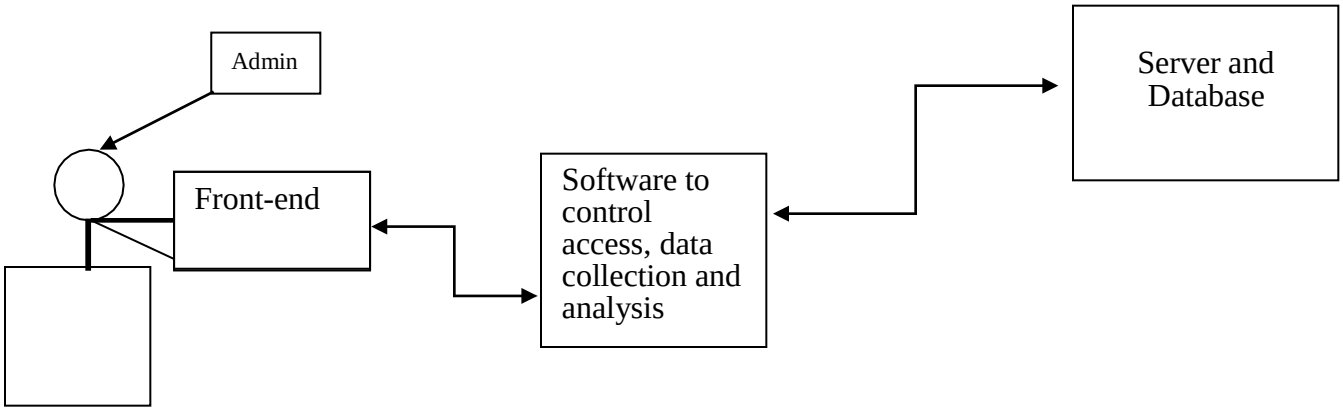
Actors – Human, Scanner, Database

Exceptions – ID card not available, Scanner not working, Scanner unable to read, Bad Internet connection, Database offline.

Includes None

Notes/Issues - None

3.3.2 Use Case: UN2



Author – Rikesh Sharma

Purpose – Normal admin-dashboard access.

Requirements Traceability – Login to the admin dashboard. Accessing the different sections of the system, such as Users, Access Control, Reports, and Settings.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues - None

3.3.3 Use Case : UN3

Author – Avinash Saini

Purpose – Bar code scanning Failed

Requirements Traceability – Login to the admin dashboard. It will show fail.
Preconditions - None

Post conditions – Normal viable product ready

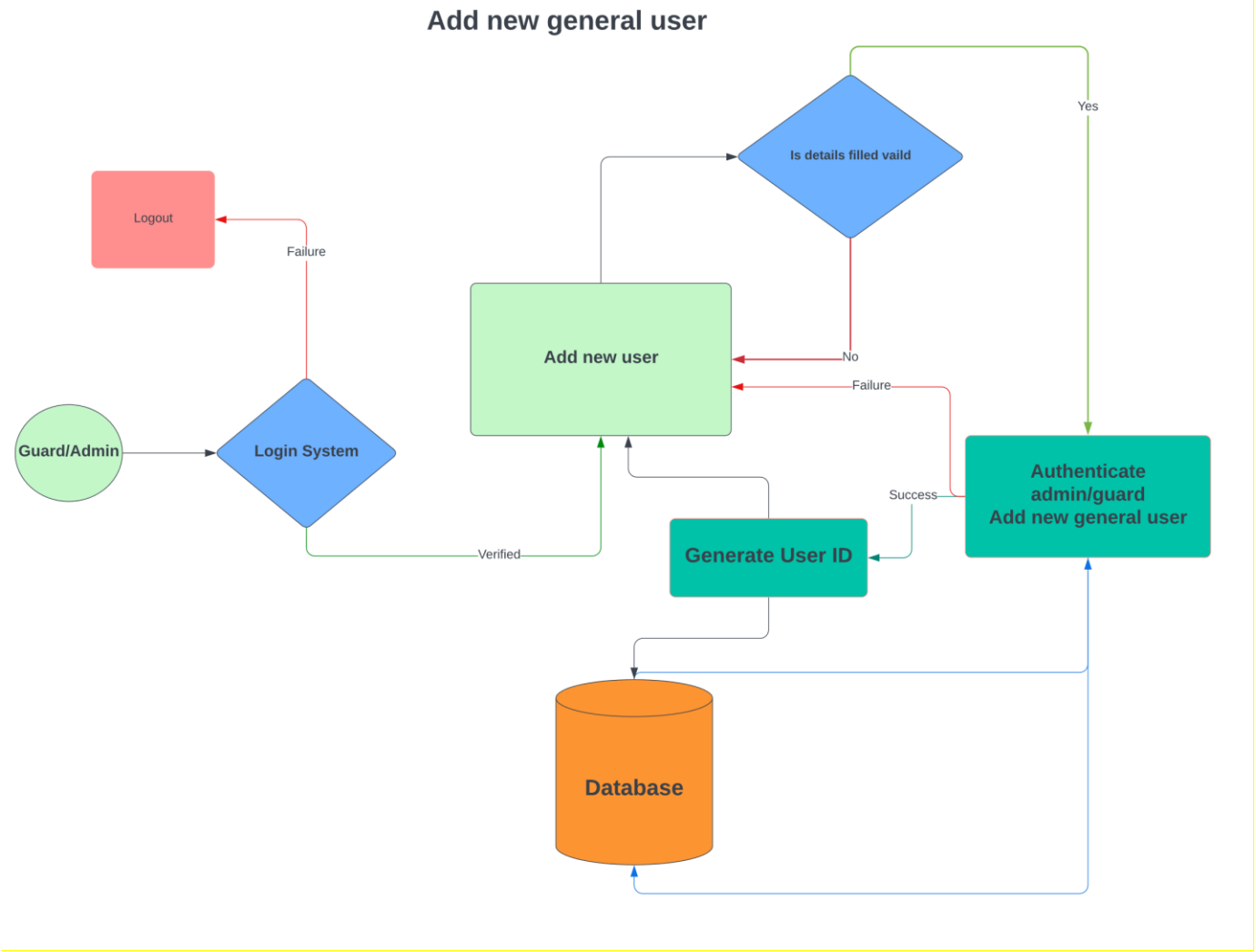
Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues – None

3.3.4 Use Case: UN4



Author – Rikesh Sharma

Purpose – Add new general user.

Requirements Traceability – Login to the homepage dashboard. Add new general user.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

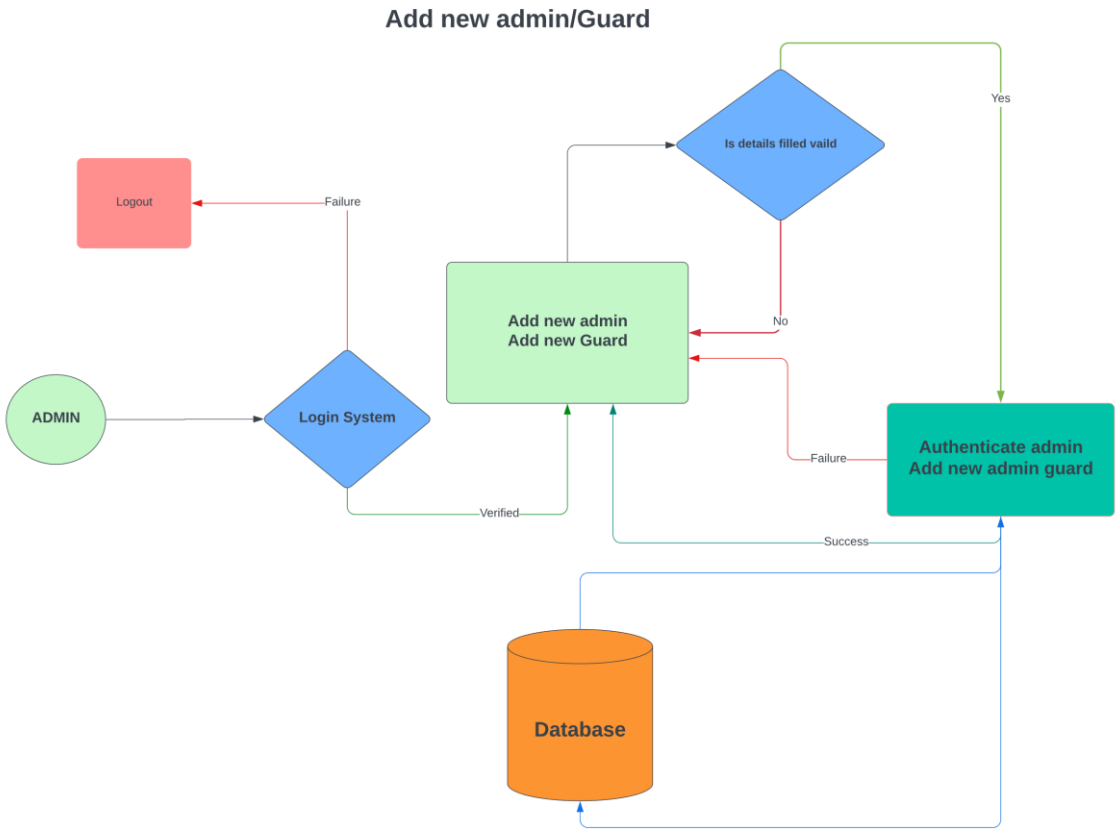
Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues - None

3.3.5 Use Case: UN5



Author – Rikesh Sharma

Purpose – Add new admin and guard.

Requirements Traceability – Login to the admin dashboard. Add new admin / guard.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

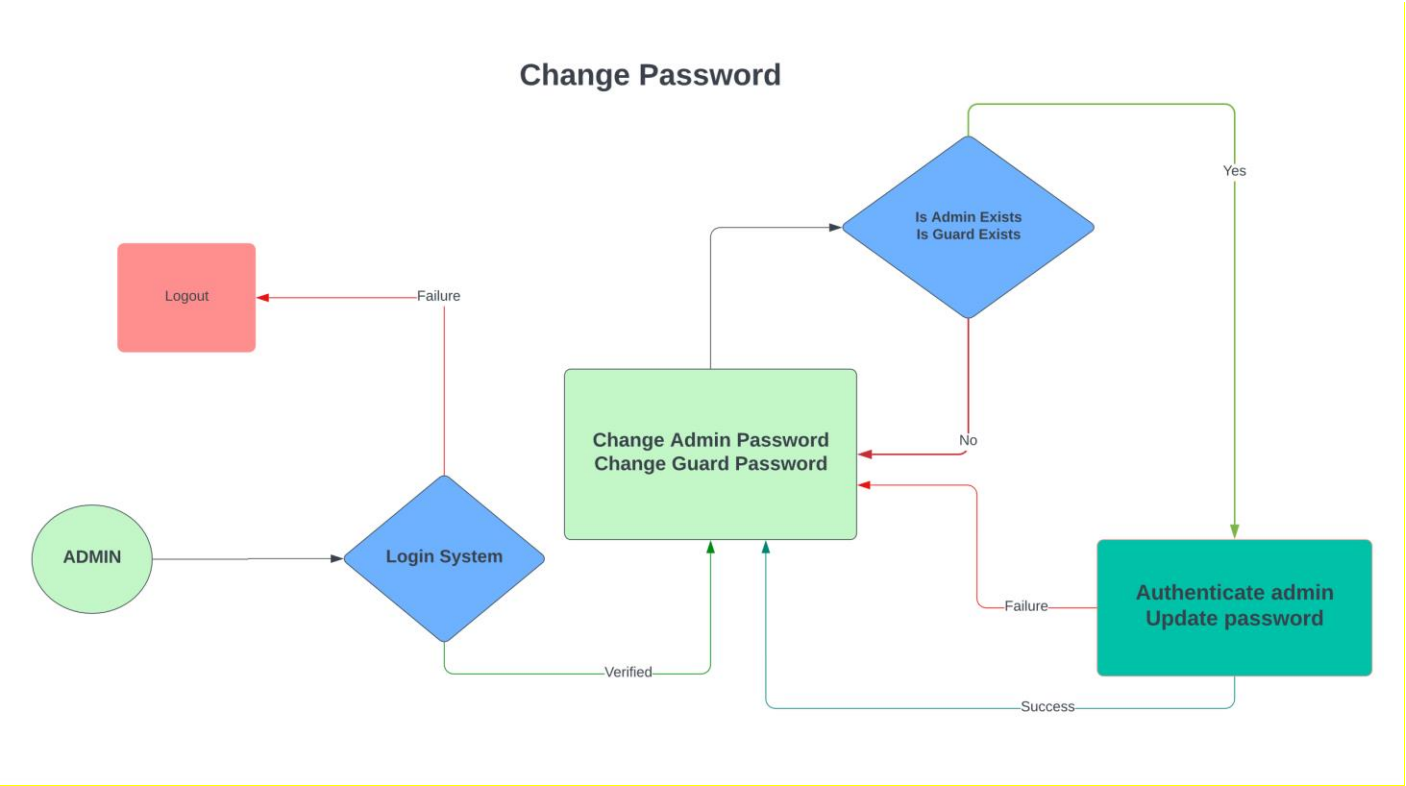
Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues - None

3.3.6 Use Case: UN6



Author – Rikesh Sharma

Purpose – Change Password.

Requirements Traceability – Login to the admin dashboard. Change admin and guard password.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

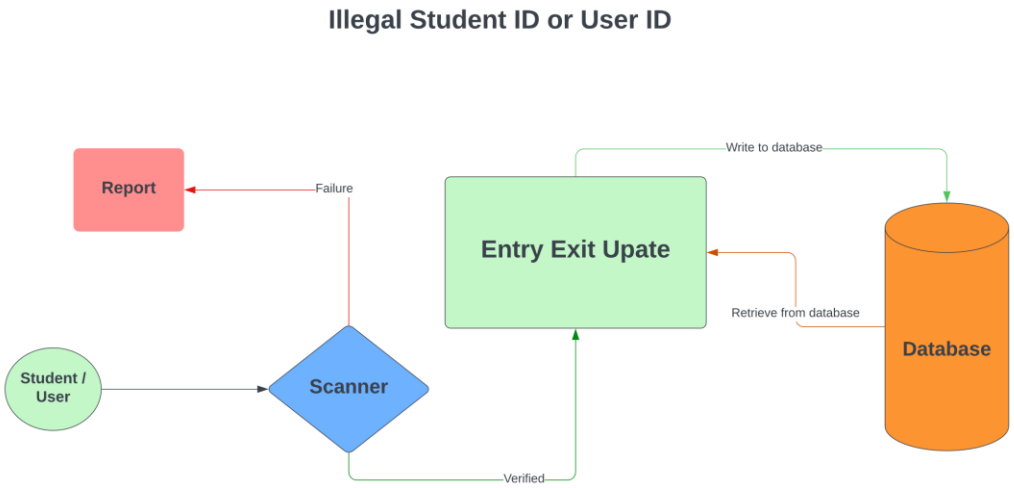
Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues – None

3.3.7 Use Case: UN7



Author – Rikesh Sharma

Purpose – Detection of illegal ID card.

Requirements Traceability – Login to the Homepage. Scanner.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

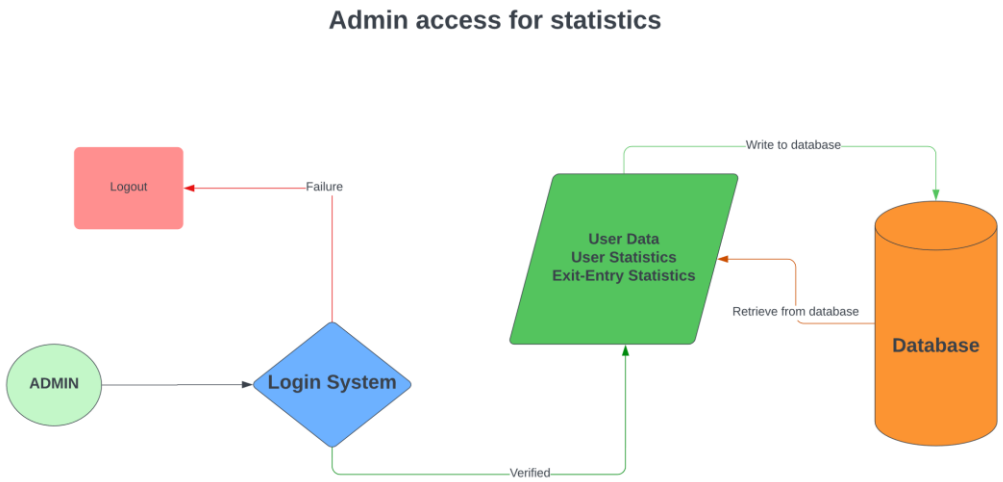
Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues – None

3.3.8 Use Case: UN8



Author – Rikesh Sharma

Purpose – Access daily statistics.

Requirements Traceability – Login to the admin dashboard. Daily entry exit statistics.

Priority – Very Important. High.

Preconditions - None

Post conditions – Normal viable product ready

Actors – Human, Desktop, Database

Exceptions – Hardware Desktop error, Bad Internet connection, Database offline.

Includes None

Notes/Issues – None

4 Other Non-functional Requirements

4.1 Performance Requirements

Correctness: The system must be able to process many transactions and users in real-time, with minimal delays and errors.

Response time: The system should work with a few milliseconds of response-time and there should be not much variation in duration of authenticating multiple authentications subsequentially.

Reliability: The system must be reliable and have minimal downtime.

4.2 Safety and Security Requirements

Security: The system must be secure and protect against unauthorized access, data breaches, and other security threats.system should not be vulnerable to sql injection attacks.

Safety:
Use static code analysis tools.
Use of popular and well mainatained libraries and frameworks.
All data should be encrypted in transit and at rest.

4.3 Software Quality Attributes

4.3.1 Usability

Usability: The system must be easy to use and navigate for both end-users and administrators.

The system will be user-friendly means any user(new or infrequent) will be able to use product very easily and new users will be able to learn all the functions of product within few minutes.

4.3.2 Maintainability

Maintainability: The system must be easy to maintain and upgrade, with minimal disruption to operations.

Even after the completion of this system, if project member wants some required changes in the system then they can do. They can add some new additional features at any time.

To avoid problems in future we have to achieve, writing efficient and bug-free code with proper tests to cover all the cases or by improving the quality attributes such as high availability, maintainability and reliability.