

**DEPARTMENT OF INFORMATION AND COMMUNICATION
TECHNOLOGY**

OPTION: INFORMATION TECHNOLOGY

YEAR: Level 7 year 3 IT

**TOPIC: FACIAL ENTRY AND EXIT SECURITY APP.
Securing Belongings, Streamlining Access**

*A project report submitted in partial fulfillment of the requirements for the award of an
Advanced Diploma in Information and Communication Technology Department, Option of
Information Technology*

Academic Year: 2023 - 2024

Prepared by:

Elisa KWIZERA

21RP00159

Under the Guidance of Jean Claude SEBUHORO.

DECLARATION

I declare that this project work entitled “**Facial Entry and Exit Security App**“, is original work and has not previously been submitted to any University/College or other Institution of Higher Learning for the award of any degree.

It is my own research, in which other scholars' writings were cited and references provided. I thus declare this work is mine and was completed successfully under the supervision of **Jean Claude SEBUHORO**

Elisa KWIZERA

Signature:

APPROVAL

This is to certify that the project work “**Facial Entry and Exit Security App**” was written and compiled by **Elisa KWIZERA** under the supervision of

Jean Claude SEBUHORO for the award of

ADVANCED DIPLOMA

IN

INFORMATION TECHNOLOGY.

.....

Name of Supervisor

.....

Date & Signature

.....

Name of Head of Department

.....

Date & Signature

DEDICATION

I dedicate this report to Almighty God whose blessing, guidance, and strength have sustained me through this journey. With His grace, none of this would have been possible

I also dedicate myself to my family, whose unwavering support and encouragement have been a constant source of motivation.

To my mentors and colleagues, who guided me with their knowledge and expertise, I am truly grateful for the learning opportunities provided. Your insights and patience helped me grow both professionally and personally

TABLE OF CONTENTS

DECLARATION.....	i
APPROVAL	ii
DEDICATION.....	iii
TABLE OF CONTENTS	iv
LIST OF FIGURES	vi
ACRONYMS AND EXPANSIONS	vii
1 CHAPTER 1: GENERAL INTRODUCTION.....	1
1.1 Background.....	1
1.2 Problem Statement.....	2
1.3 Objectives.....	2
1.3.1 General Objective.	2
1.3.2 Specific Objective.....	2
1.4 Project Scope	3
1.5 Project Limitation	3
1.6 Research Questions	4
1.7 Hypothesis.....	4
1.8 Significance of study.....	4
1.9 Methods and Techniques	5
1.9.1 Methods.....	5
1.9.2 Techniques	6
2 CHAPTER 2: LITERATURE REVIEW	8
2.1 Introduction to Access Control Systems	8
2.2 Facial Recognition Technology in Security Application.....	8
2.3 Face Recognition: Some of the Problems Encountered	8
2.4 Facial recognition in Access control Systems	9
2.5 Conclusion.....	9
3 CHAPTER 3: SYSTEM ANALYSIS AND DESIGN.....	10
3.1 System Analysis	10

3.1.1	Requirements Analysis	10
3.1.2	Feasibility Study	13
3.2	System Design	13
3.2.1	System Architecture	13
3.2.2	Database Design	14
3.2.3	User Interface Design	16
3.2.4	Workflow Design	21
3.3	Future Extension	22
4	CHAPTER 4: IMPLEMENTATION	23
4.1	Technology Stack	23
4.2	Frontend Implementation	24
4.2.1	Sign Up and Login	24
4.2.2	Entry and Exit Forms	25
4.3	Backend Implementation	25
4.4	Facial Recognition Integration	26
4.5	Testing	27
4.6	Challenges and Solutions	28
4.7	Summary	28
5	CHAPTER 5: CONCLUSION AND RECOMMENDATION.	29
5.1	Conclusion	29
5.2	Recommendations	29
6	REFERENCES	31

LIST OF FIGURES

Figure 1 Waterfall model	6
Figure 2 Use Case	12
Figure 3 Database Security correction.....	15
Figure 4 database checkin correction	16
Figure 5 Security Login	17
Figure 6 Security create account	18
Figure 7 checking in (entering)	19
Figure 8 checking out	20
Figure 9 history of people checked.....	21

ACRONYMS AND EXPANSIONS

PWA: Progressive Web Application

JS: JavaScript

HTTP: Hyper Text Transfer Protocol

API: Application Programming Interface

HTML: Hyper Text Markup Language

CSS: Cascading Style Sheet

ID: Identity

1 CHAPTER 1: GENERAL INTRODUCTION

1.1 Background

The Facial Entry and Exit App represents the latest innovation in access control, addressing the limitations of traditional methods. The app uses advanced facial recognition technology to manage entry and exit points, ensuring that individuals leave with the items they bring in.

In today's schools and workplaces, and other organizations there's a frequent issue. Most workers and students are complaining several times about their properties being taken by people who don't belong to them. Due to several times of their properties being stolen, they become discouraged and slow down their performance in the organization they are working in.

Traditional entry and exit systems, such as manual checks and ID cards, are often inefficient and prone to errors. These systems fail to prevent unauthorized access and misplacement of belongings. However, advancements in facial recognition technology offer promising solutions. Facial recognition uses cameras and algorithms to identify individuals based on their unique facial features, providing a more secure and efficient alternative to traditional methods.

Life changes and becomes hard for students and employees. These students and employees whose things are stolen meet difficulties in getting substitutes for those stolen ones. Most of the time things are expensive which is difficult to afford and makes life hard due to the burden of buying stolen things, like computers.

Nowadays people are taking each other's belongings. It may include telephones, bags, laptops, and others. Imagine a student leaving with a laptop they didn't bring or a worker grabbing the wrong bag. These mix-ups cause a lot of confusion and frustration.

Efficient and secure entry and exit systems are essential in today's fast-paced environments like schools, workplaces, and public venues. Traditional methods, such as manual checks and ID cards, often suffer from errors and inefficiencies. This can lead to unauthorized access and misplaced belongings.

1.2 Problem Statement

In NGOMA COLLEGE and workplaces, people often accidentally take items that don't belong to them, causing disruptions and security risks. Common items like laptops, phones, bags, umbrellas, and others get mixed up, leading to confusion and frustration. This also poses a significant security concern as valuable items can be lost or stolen.

Current methods like manual checks and basic security measures are not effective in preventing these mix-ups. These methods rely on visual inspection and manual verification, which are prone to human error and inefficiency. As a result, they fail to provide a reliable solution to this widespread issue.

To address this problem, we need an advanced solution that manages entry and exit points while ensuring accountability and security. The proposed Facial Entry and Exit App aims to fill this gap by using facial recognition technology to streamline the identification of individuals and their belongings.

1.3 Objectives

1.3.1 General Objective.

First of all, the general objective of the **Facial Entry and Exit Security App** is to develop a system that will facilitate maintaining security at Ngoma College when Entering and leaving the gate.

The general objective of the "**Facial Entry and Exit Security App**" project is to boost the security of individual materials and ensure individuals materials are well maintained and not taken by someone which doesn't belongs and has no permission to take them.

1.3.2 Specific Objective.

- I. To Recognize the Face while entering
- II. To Record materials/ tools of a person during entering
- III. To Recognize the face during exiting
- IV. To Display materials that belong to a recognized person
- V. To Check if materials meet with the recorded ones
- VI. To Remove materials of a person during exit

1.4 Project Scope

The “**Facial Entry and Exit Security app’s**” Scope is to emphasize developing a progressive web app that will allow students or employees to register. During the time of entering an organization, the application will record and recognize the face of the person and record his/ her materials, like Telephones, Bags, laptops, and others. During the time of leaving the organization, the application will recognize the face of the person and display the materials he/ she enters with, and security guards check if it matches the materials exits with.

For example: if the person enters with one (1) telephone and leaves with more than one telephone, the guards will ask where they got the other telephone yet they don’t come with it.

The system will not stop someone from moving but the guards on the Gates are the ones who will not allow persons with things which are not belong to them to move.

The project will be limited only to recognizing the face during entering and recording the tools you entered and recognizing the face during exiting and displaying tools that you exit.

1.5 Project Limitation

It is very crucial to jot down “**Facial Entry and Exit Security App’s**” limitations, below are the limitations listed:

- I. Internet Access: Users of the system must have access to the Internet to utilize the project, which may limit participation in areas with limited connectivity.
- II. Face recognition: The success of the system relies on recognizing the face of a person when exiting and entering.
- III. Displaying Materials: While the system can assist in identifying taken materials, it may not guarantee their recovery, as recovery efforts depend on the law of organization.
- IV. Legal Considerations: The project must adhere to legal and privacy regulations regarding the collection and storage of user data, which may vary by jurisdiction.
- V. The project will not enforce some to return the tool/ material it will only show the security guards the material taken and they do their responsibility

1.6 Research Questions

The main purpose of this study is to eradicate the following research questions

1. How effective is facial recognition technology in enhancing the security of personal belongings in schools?
2. What are the user perceptions and acceptance levels of the Facial Entry and Exit Security App?
3. What challenges do security personnel face in implementing and using the app?
4. How does the app impact the efficiency of entry and exit processes in the selected environments?

1.7 Hypothesis

The implementation of the **Facial Entry and Exit Security App** at NGOMA COLLEGE using advanced facial recognition technology will significantly reduce the incidents of theft and misplacement of personal belongings in NGOMA COLLEGE. Only authorized individuals enter and exit with the items they originally brought in, the app addresses the limitation of traditional access control methods, such as manual checks and ID cards, which are often error-prone and inefficient. This innovation is expected to enhance security measures and improve the overall safety and satisfaction of students and employees.

The use of facial recognition technology in entry and exit management system will contribute to creating a more secure environment, leading to increased trust and confidence among users. By minimizing the risk of theft and confusion caused by the mix-up of personal belongings, the app is hypothesized to improve the productivity and morale of individuals within NGOMA COLLEGE. This is because they will no longer be preoccupied with the fear of losing their valuable items, enabling them to focus better on their tasks and activities.

1.8 Significance of study

1. Enhanced security: Provides a secure method to control access and prevent theft by using facial recognition technology
2. Improved Accountability: Ensure individuals leave with the items they brought, reducing access to unauthorized possession

3. Operational Efficiency: Replace error-prone traditional methods like manual checks and ID cards, making entry and exit processes more efficient
4. Increased Trust and satisfaction: reduces fear of theft, boosting morale and productivity among students and employees
5. Practical Application: Provides a real-world solution to a common problem in various organizations, benefiting schools, and workplaces.

1.9 Methods and Techniques

The methodology for developing the **Facial entry and exit app** at NGOMA COLLEGE focuses on utilizing a combination of software development practices, testing, and evaluation methods to create a reliable and efficient facial recognition-based access control system.

1.9.1 Methods

Research design

1. The qualitative method was employed, which involves interviews, surveys, and observation to gather user experiences and perceptions

Data collection methods

1. Survey and questionnaires: Designed to collect data on current security issues, user experience, and expectations from the system
2. Interviews: conducted with key stakeholders, including students, and security guards to gather in-depth qualitative data
3. Observation: Direct observation at entry and exit points to monitor system app performance and user interaction

Sample selection

1. Purposive sampling: this is used to select a diverse group of participants, including students and security personnel, for comprehensive data collection

Testing and evaluation

1. Usability Testing: conducted with a small group to identify usability issues and areas of improvement
2. Performance Testing: Evaluating the app under various conditions to ensure reliable operation.

3. Security Testing: Assessing the app's capability to prevent unauthorized access and theft through simulation

Ethical Consideration

1. Ensuring participant privacy, obtaining informed consent, and complying with data protection regulations are essential components of those study

1.9.2 Techniques

Software Development Techniques

1. Agile Methodology: An iterative approach to developing the app, allowing for continuous feedback and rapid adaptation to user needs.
2. Progressive Web App (PWA) Development: Using JavaScript, HTML, and CSS for a responsive and user-friendly interface.

Waterfall model: The best method to be used in developing software, which use the algorithm of moving to next step when the current step in done.

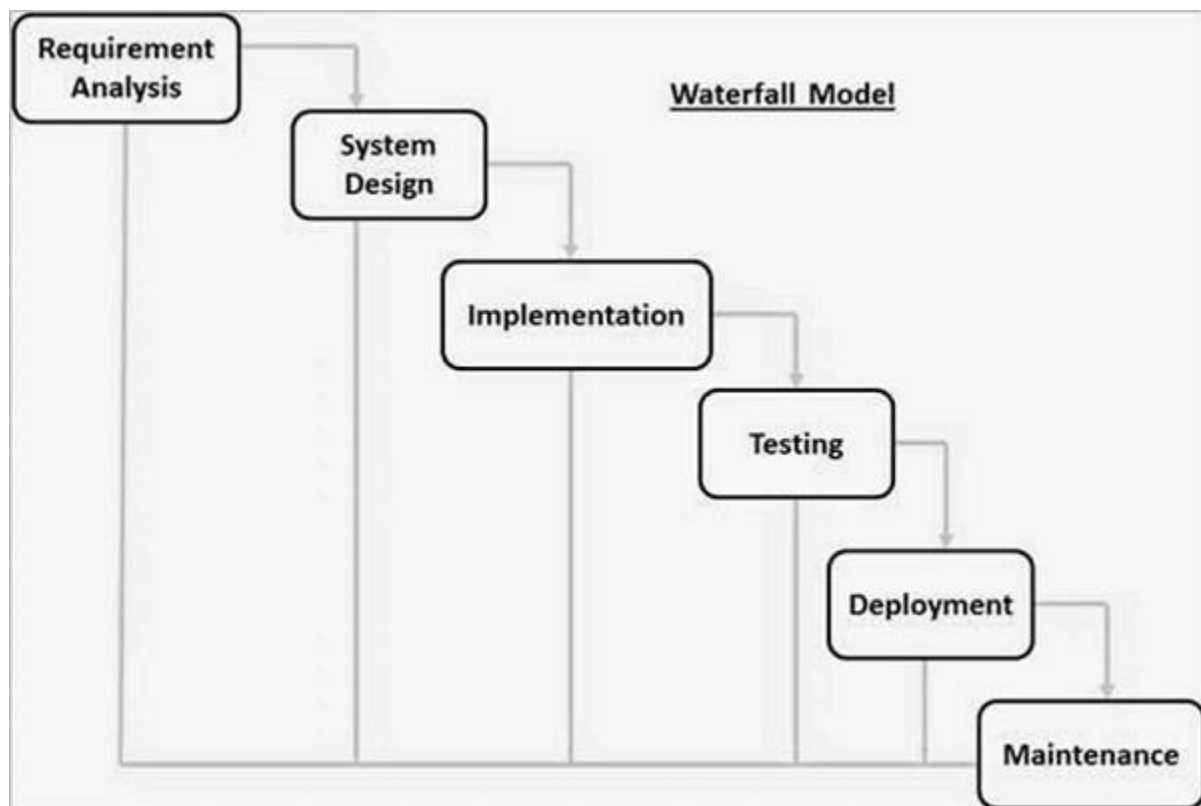


Figure 1 Waterfall model

Technology Stack

1. Frontend Development: JavaScript, HTML, and CSS for building a Progressive Web App (PWA).
2. Backend Development: Node.js and Express.js for server-side operations and API development.
3. Facial Recognition Libraries: Implementing facial recognition technology using libraries like OpenCV or Face-api.js for accurate recognition.
4. Database Management: Using MongoDB to manage user data, entry and exit logs, and records of belongings.

Data Collection Techniques

1. Digital Surveys and Questionnaires: Online forms to collect quantitative data from participants.
2. Structured Interviews: Pre-defined questions to guide conversations with stakeholders.
3. Direct Observation: On-site observation of user interaction and system performance.

2 CHAPTER 2: LITERATURE REVIEW

2.1 Introduction to Access Control Systems

Over time, the methods of controlling access have revolutionized from simple methods of using keys and ID cards to using biometrics. The necessity of access control has become essential in different fields such as schools, offices, or related public areas in which the preservation of security is vital. Some of the conventional measures that are used including checkpointing and ID card systems have been found to be ineffective in the prevention of unauthorized entry and or loss of property hence the need to embrace other methods. These include biometric access control systems, especially facial recognition which has proven to provide better security and reduce operation costs (Chen, 2022).

2.2 Facial Recognition Technology in Security Application

Facial recognition technology has received significant importance in the current security solutions to work as a fast and efficient identification method. The technology uses geometry analysis to map features of one's face making it easy to compare with the records that are stored in the system (Jain & Li, 2023). Facial recognition has been used in several security protocols in some precincts, companies, etc. Showing it is a very effective program. Current research also highlights its usefulness in curbing crime incidences and unlawful intrusions in secure zones (Singh et al., 2022).

2.3 Face Recognition: Some of the Problems Encountered

Despite the advantages of facial recognition technology, there are certain challenges associated with this facial recognition technology though it comes along with lots of benefits. The second challenge regards privacy, as the biometric data are collected and stored, which has to be done legally and ethically (Smith & Miller, 2022). Furthermore, facial recognition systems can be imprecise due to drawbacks such as low lighting, low-quality photographs, or a subject's changed appearance (Zhou et al., 2018). It has been found that algorithms may bring in ethnicity, age, and or gender discrimination which may lead to unequal treatment the clients (Ferrara, 2023).

2.4 Facial recognition in Access control Systems

Many people believe that the application of facial recognition in access control systems is a plus to security management. It also enables automatic operations of entry and exit and helps save time and boost efficiency since few manual checks are required (Mingtsung et al., 2020). It has been proven that the application of facial recognition in conjunction with other methods of physical security such as RFID and motion detectors can enhance the accuracy of access control systems (Siau & Wang, 2020). In addition, the level of acceptance by the users in regards to the application of facial recognition in the control of access is relatively positive especially when privacy is addressed appropriately (Almeida et al., 2022).

2.5 Conclusion

Concisely, the deployment of facial recognition technology in access control systems solves the problem encountered with the traditional method. However, as many would note, there is privacy invasion and possible accuracy problems existing within the tradition; however, with the consistent progression of technology and ethical motivation, these problems are not irreversible. Such a solution can be seen together with the Facial Entry and Exit App that has been proposed to become a secure and efficient solution for controlling entry and exit points in schools, workplaces, and other institutions.

3 CHAPTER 3: SYSTEM ANALYSIS AND DESIGN.

This chapter discusses the development and design of the ‘**Facial Entry and Exit Security App.**’ This intention is to show how the proposed solution came into being to solve the problem postulated in the earlier chapters. The last revelation is that the system analysis and design plays a role in establishing the soundness, scalability, and extensibility of the solution. This step also has a rather profound impact on the quality of the produced software and its further development.

3.1 System Analysis

System analysis is a process of defining and defining the characteristic features and capabilities that the **Facial Entry and Exit Security App** should perform. Facial recognition will help the system in controlling entry and exit points and also the recording of material that the individual accompanies. It will be able to recognize these materials at this exit point so that those on the list will only be allowed to take the items they came with.

3.1.1 Requirements Analysis

The first phase of the initial phase of system analysis is the collection of requirements for the identification of functionalities and features of an app that is to be developed. These are classified into two categories: as well as functional and non-functional requirements.

Functional Requirements:

User Registration: The app must enable the students and employees to provide their profiles and materials on entry to the premises.

Facial Recognition for Entry: While entering the system, it must identify an individual’s face and also capture any other material that is/are relevant.

Materials Management: There should exist a record to show what was put into the system in a bid to compare with what is leaving the system.

Facial Recognition for Exit: The system requires the recognition of a person and then, as an exit, the system should recognize the material which the person takes with him.

Material Verification: The app should give a message to the guards in case of any inconsistency in the material.

Audit Trail: For the purpose of security auditing all the entry and exit events should be recorded in the system.

Non-Functional Requirements:

Performance: It should be able to identify faces and validate materials within a few seconds in order to enhance flow in/out of the premises.

Security: Facial data and material records have to be kept secure to ensure that few people have access to it.

Scalability: The system should be scalable to cater to a larger number of users and materials with the growing organization.

Usability: It has to be easy to operate because the introduction of the system has to be done in a way that will help both the end users as well as the security personnel.

Use case Diagram:

This diagram is the representation of user's interactions with the system and showing the specification of a use case. This diagram will show the privileges of a user and what they are allowed to do according to their roles.

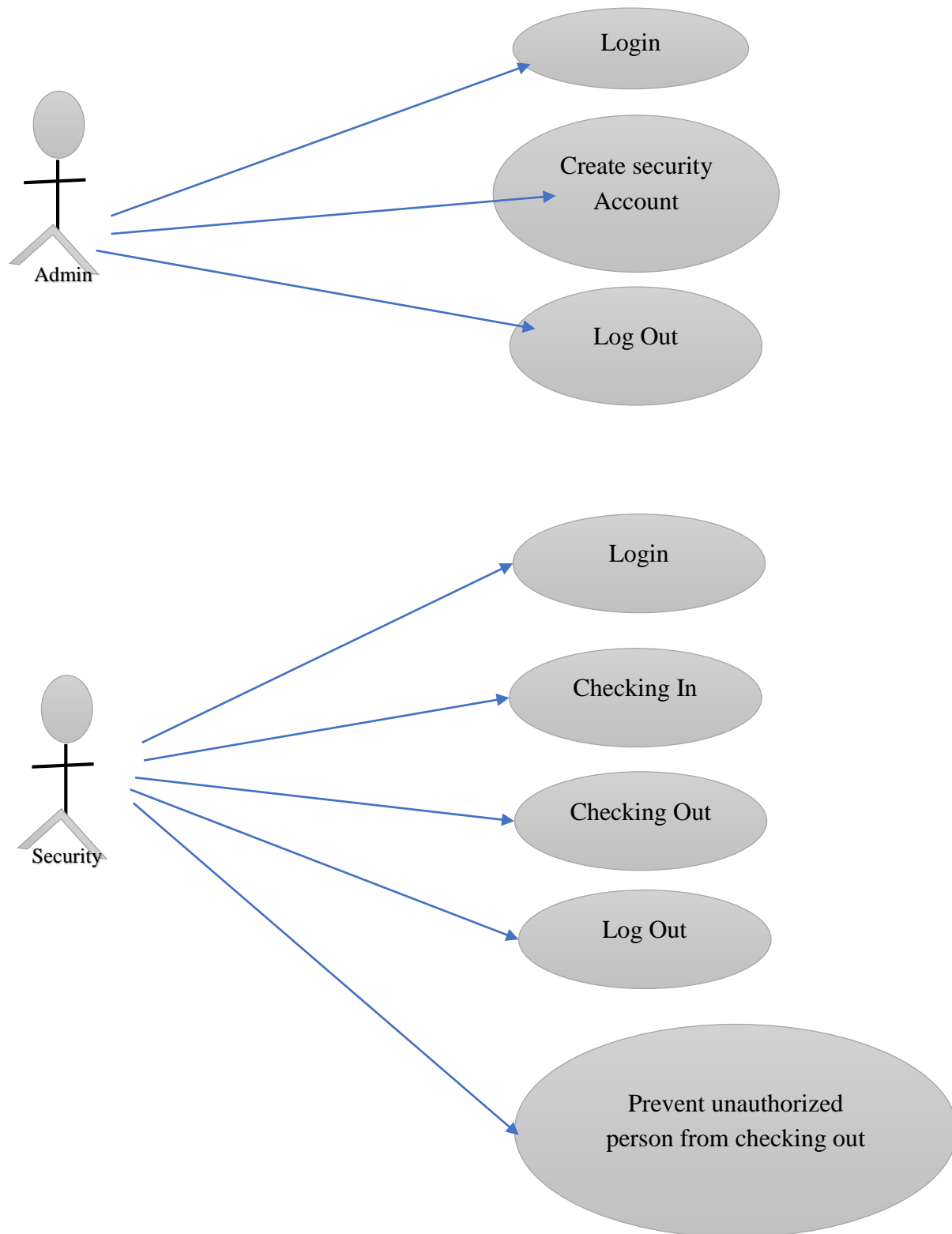


Figure 2 Use Case

3.1.2 Feasibility Study

The feasibility study evaluates the extent to which the proposed system can be implemented taking into consideration time, resource, and technological availability.

Technical Feasibility: Since there exist facial recognition libraries such as OpenCV and Face-api.js, the technology needed for the undertaking is available. The app can also be made to run as a Progressive Web App hence it can be accessed in the browser without creating a native mobile application.

Operational Feasibility: The app has the potential to improve the security and operations of those buildings in a large way. It can easily be incorporated into the day-to-day activities of organizations such as schools and workplaces making it secure without complicating it.

Economic Feasibility: The major costs that have been incurred for the development of this application relate to the facial recognition and security features which shall be offset by the gains that this app will generate in cases of theft or loss of the items.

3.2 System Design

System design for the solution requires the development of a concept map, such as the decision of the system structure, database format, and the design of the Graphical User Interface.

3.2.1 System Architecture

The system is divided into three main components: These are divided into Frontend, Backend, and Database. Every single part plays a certain part in the general design.

Frontend: PWA is the key to the application interface. Users can register, log in, and keep into practice the material that they use in the web browser. PWA is designed using HTML, CSS, and JS for optimal responsiveness and good usability.

Backend: The backend which has been created by using Node.js and Express.js, is responsible for the management of the application flow. It addresses the requests related to face recognition, management and handling of materials, and communication with the database. This layer also

provides safe and effective communication between the user and the system as well as identifying and authenticating the user of the system.

Database: MongoDB is used for storing users' data and entry/exit logs, as well as material records. That is why the methodology of creating the database is supposed to be scalable and adapted to the increasing number of users.

3.2.2 Database Design

The last system imposes several basic needs in the system in how such data as the user's data, face data, and material records are to be stored and retrieved in databases. The following collections will be created in MongoDB: The following collections will be created in MongoDB:

Users: This collection holds information about users including ID, registered materials, and further; their facial information.

Fields: It is composed of `_id`, `regNumber`, and `Materials` which were all described above.

Entry Logs: This collection records each record created in the system with information linking the users with their materials.

Fields: `_id`, `sId`, `materials`, `status`

Exit Logs: This collection informs the user that he or she is leaving while checking out the items the user is removing from the collection.

Fields: `_id`, `sId`, `materials`, `status`

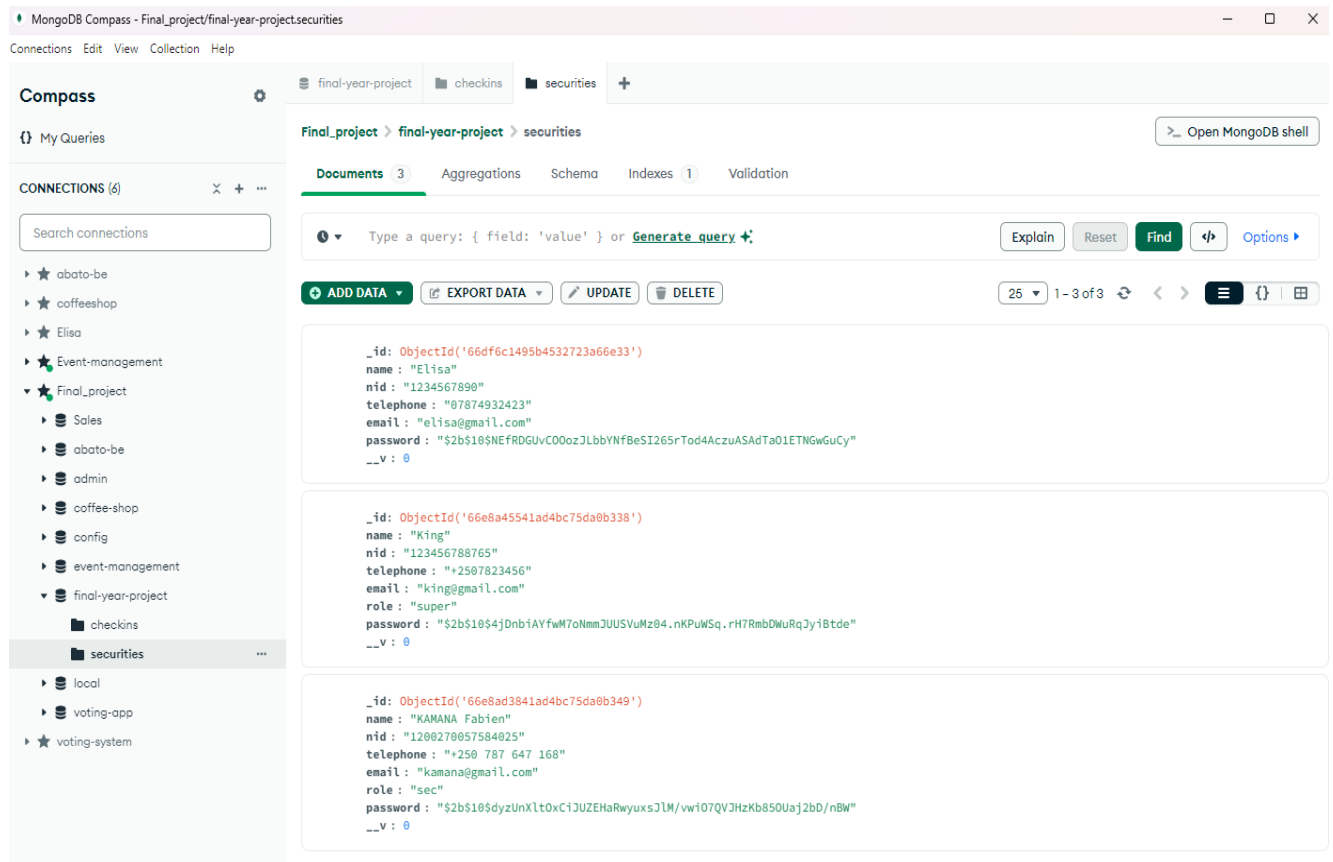


Figure 3 Database Security correction

Database design in the Checkins correction: This shows how the information of person checked-In or moved out the school.

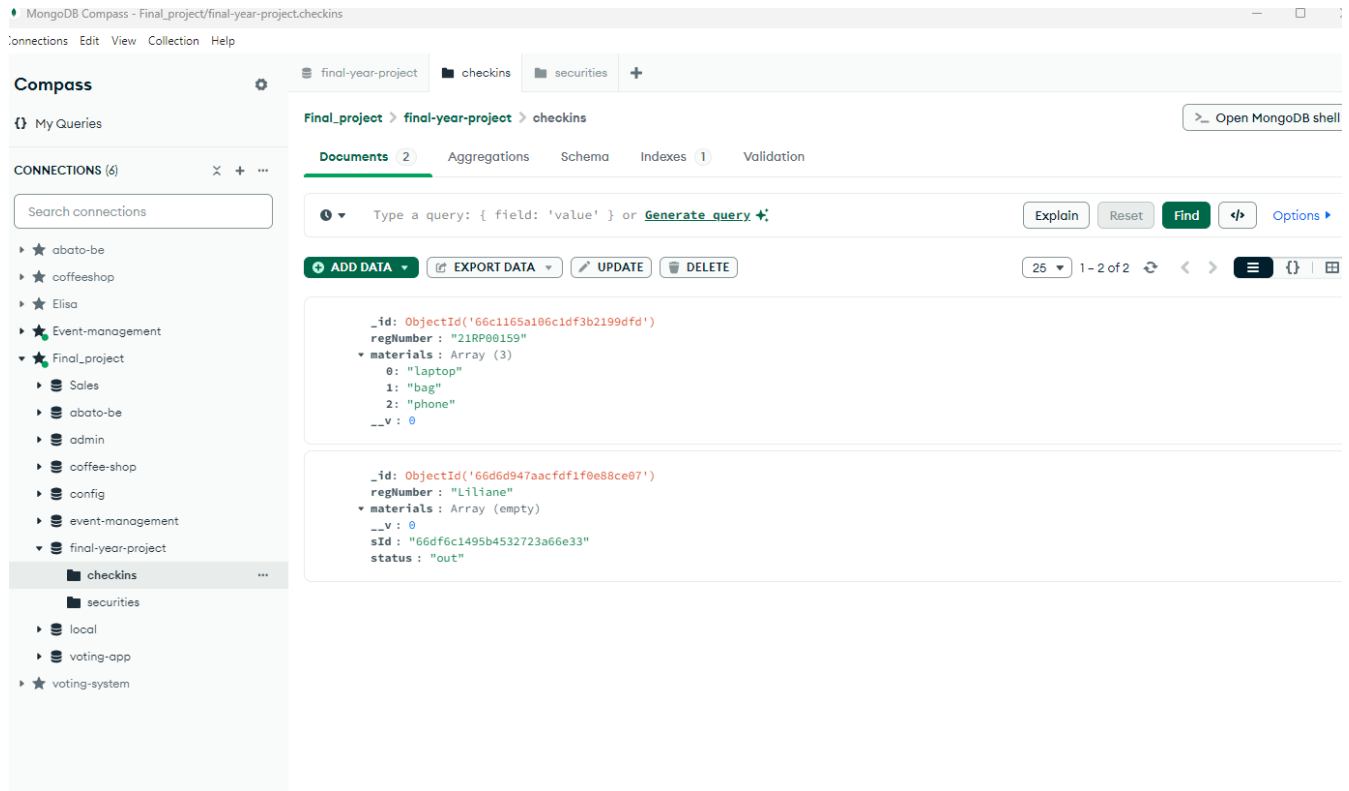


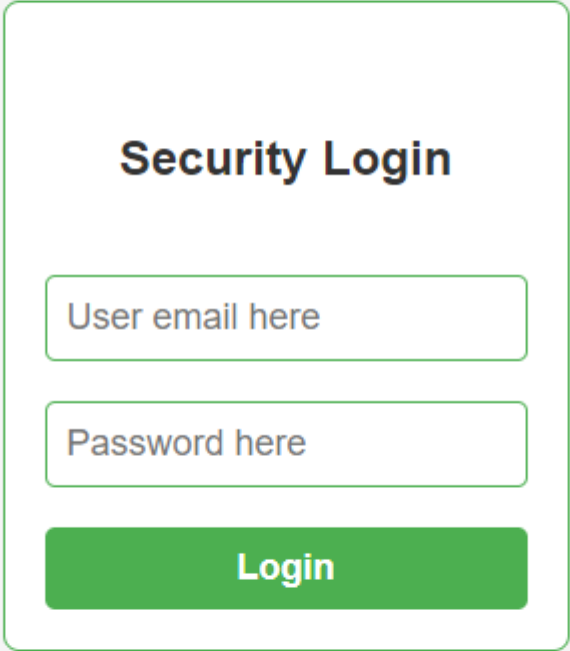
Figure 4 database checkin correction

3.2.3 User Interface Design

It is however important for the average users as well as security personnel who will be operating the UI to find it easy to work on. The following pages are designed: The following pages are designed:

Login and Registration Page: When first using the application, it permits the users to sign up for their profile and materials.

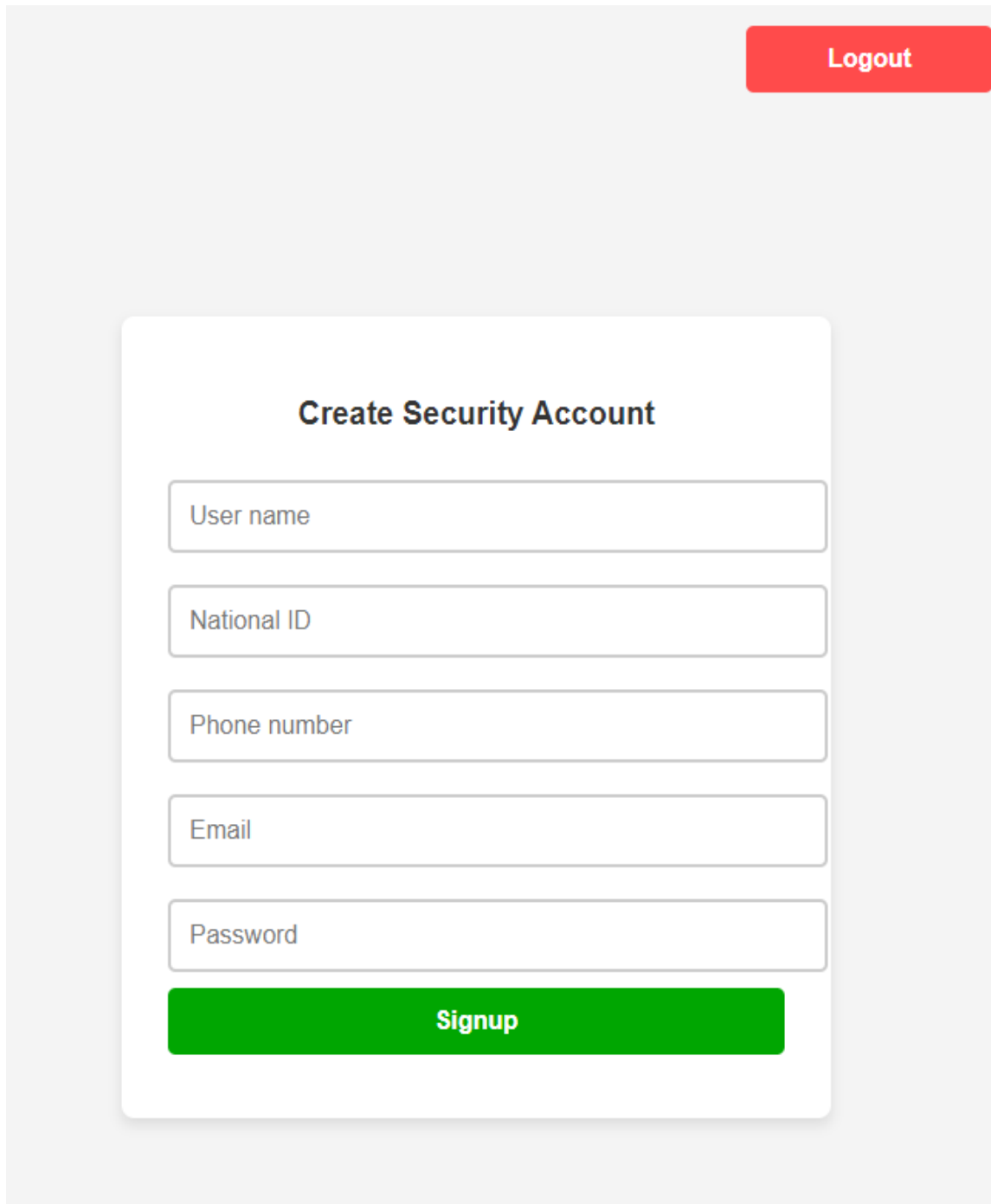
Security Login Page: The page where the security logs in before they do anything either checking in or checking out



The image shows a 'Security Login' form centered on a light gray background. The form is a white rectangle with rounded corners and a thin green border. At the top, the text 'Security Login' is displayed in a bold, black, sans-serif font. Below this, there are two input fields, each with a green border and rounded corners. The first field contains the placeholder text 'User email here' in a gray font. The second field contains the placeholder text 'Password here' in a gray font. At the bottom of the form is a solid green rectangular button with the word 'Login' written in white, bold, sans-serif font.

Figure 5 Security Login

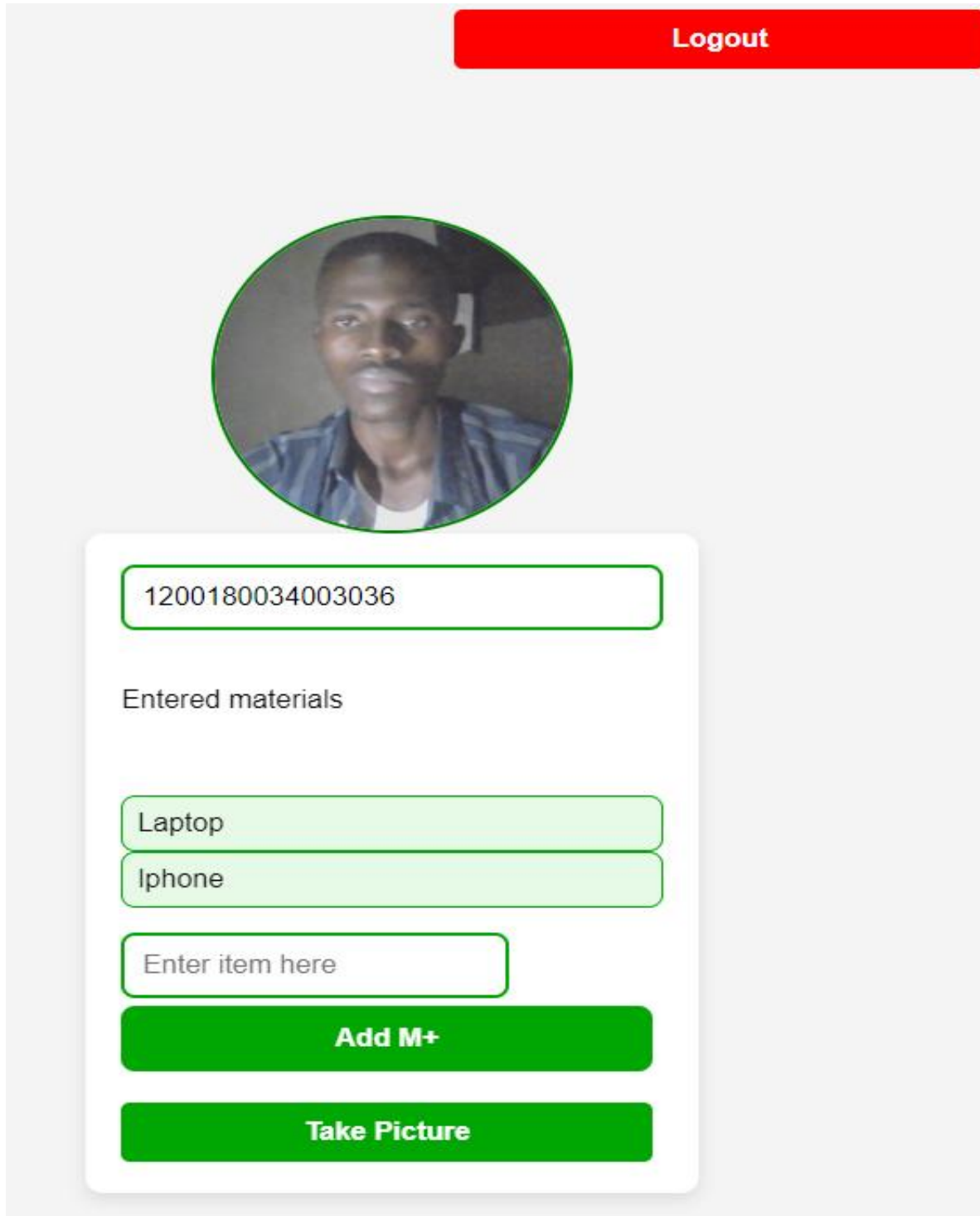
Registration Page: The page where Security admin creates the account of the other security guards



The image shows a web interface for creating a security account. At the top right, there is a red button labeled "Logout". In the center, there is a white rounded rectangle containing the title "Create Security Account". Below the title are five input fields: "User name", "National ID", "Phone number", "Email", and "Password". At the bottom of this rectangle is a green button labeled "Signup".

Figure 6 Security create account

Entry Page: Shows the interface for taking and identifying the user's face through the camera. Having successfully verified his/her identity, the user is required to inform the system of the items he/she is carrying.



The image shows a mobile application interface for an entry system. At the top right, there is a red button labeled "Logout". Below this, on the left, is a circular profile picture of a man with a mustache wearing a blue and white striped shirt. To the right of the profile picture is a white rounded rectangle containing a text input field with the number "1200180034003036". Below the input field is the text "Entered materials". Underneath this text are two stacked light green rounded rectangles containing the text "Laptop" and "Iphone". Below these is another light green rounded rectangle with the placeholder text "Enter item here". At the bottom of the white rounded rectangle are two green buttons: "Add M+" and "Take Picture".

Figure 7 checking in (entering)

Exit Page: This looks like the entry page but also shows the registered materials for cross-checking.



Capture

Back

Loaded

Figure 8 checking out

View History of Entered: For better performance the security guard can see person he/ she checks, either in or out. Below is the image that shows it:

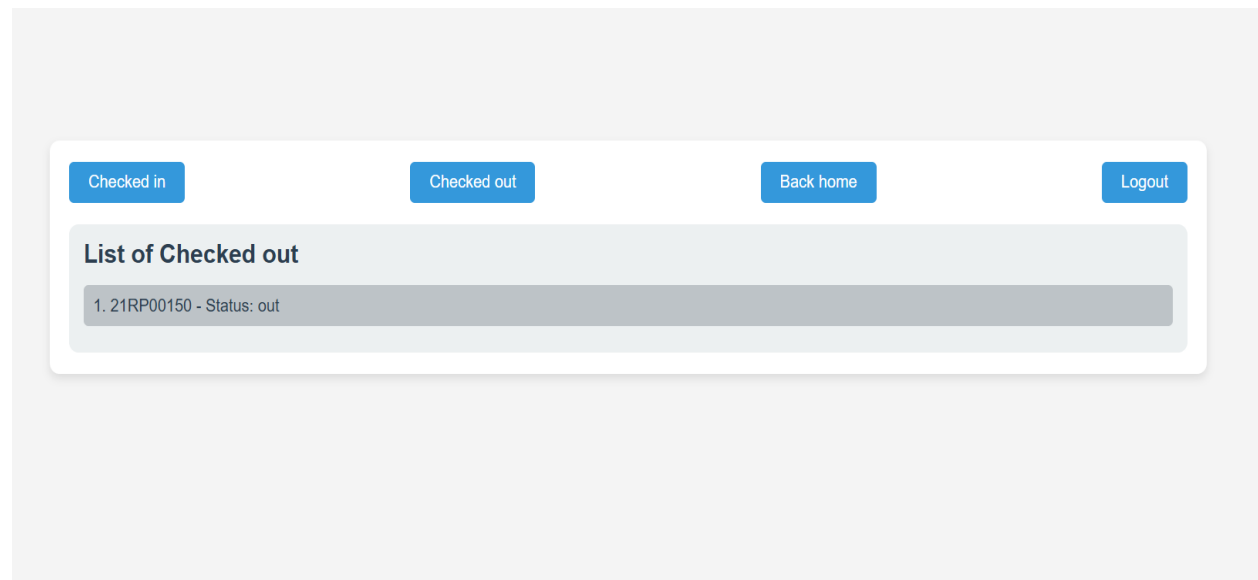


Figure 9 history of people checked

Admin Panel: In order for security personnel to check logs, produce reports, and prevent persons from exiting if any unauthorized materials are found.

3.2.4 Workflow Design

This implies that the flow of the system work is designed in such a way that it will have easy entry and easy exits. Below are the key steps: Below are the key steps:

User Entry:

The user goes to the entry point, the facial image of which is recorded by the camera.

Face identification is done and the user's account is retrieved.

The user logs in with the materials he or she is carrying.

The material is stored in the system and the entry is logged.

User Exit:

The user moves closer to the exit point and the system takes his/her face once more.

Biometric systems such as facial recognition scans the user.

The system shows the records of the entered materials during entry as shown next.

In this step, the security personnel compares the registered items with the ones the user is having.

This means that any mismatch results in denying to exit.

3.3 Future Extension

The future expansion of the system is also addressed in the system design. They can later incorporate other features such as the incorporation of RFID tags for material tracking, ensuring that the system recognizes multiple forms of biometric data for authentication, and the use of AI to detect abnormal activities in the system. Furthermore, the development of a mobile application for native Android and cross-over I OS platforms can be considered for better reachability.

4 CHAPTER 4: IMPLEMENTATION

The life cycle of the “Facial Entry and Exit Security App” can be categorized under the implementation phase, in that it gives a practical solution to the system design phase. In this chapter, the authors describe how the application was constructed, the design steps demonstrated with key forms, features, and functionalities used to address objectives defined in the previous stages. The chapter focuses on the technologies applied, the frontend and the backend application and establishment of the database as well as the incorporation of the facial recognition technology.

4.1 Technology Stack

The development of the application involved the following technology stack: The development of the application involved the following technology stack:

Frontend:

Designing a true Progressive Web App (PWA) while coding the site in HTML, JavaScript, and CSS to guarantee the usage of responsive interfaces.

The use of the Tailwind CSS to achieve near-instant styling and a high level of adjustability to work with on projects.

Backend:

Node.js and Express.js to manage the API or to handle all the server-side functionality.

Facial Recognition Libraries: Face-api.js for identifying people’s faces in real-time.

MongoDB for logs such as belongings logs, entry/ exit history as well as storing users’ data.

Security Measures:

JWT (JSON Web Token) for security issues of the user credentials and permissions.

Data Encryption to protect the users’ information they input into the different services.

Tools:

Visual Studio Code with R and Python languages for programming and testing.

GitHub for version control.

Postman for testing APIs.

AWS services, such as MongoDB Atlas for organizations' cloud-based databases.

4.2 Frontend Implementation

The frontend interface was also designed as a PWA to make sure the users can use the application on both, desktop and mobile. Key UI components include:

4.2.1 Sign Up and Login

Registration Form:

It is the collection of user data in a form like full name, email, and form used to capture facial photo. The face data is captured through the device camera with the help of the Face-API as shown below. Load it by the js library, then, pass it to the backend to proceed with the registration process.

The form also enables users to provide information on their assets to be checked in (e.g., phones, laptops, and bags) on entry.

Login Form:

Customers use facial recognition to log in to the system when the system scans the stored face data and allows users to log in.

Users are provided content on registered materials and entry logs within the system.

Dashboard

The current users who have accessed the premises and their respective registered materials are well captured on the dashboard.

They can view a list of people and what is similar to the materials that they had on entry and the materials that they take out.

4.2.2 Entry and Exit Forms

Entry Form:

When the face is scanned to capture it, the required materials are registered and the information thus obtained is stored in the database.

The entry logs by date and time are provided and recorded and are available for access by security guards' examination.

Exit Form:

When exiting the facial recognition system analyzes the face comparing it with the data that was taken at entry.

All the materials that are entered are shown to the user and security guards where they are supposed to be.

Entries can also be checked by guards by a physical comparison with the materials being taken.

Material Management System

After registration, the users can then upload new materials onto it or even modify materials already existing in the profile or delete them.

Security can, for instance, have the records of all the materials registered to be taken out to verify this list.

4.3 Backend Implementation

The backend was done using Node.js and Express.js, masterful for the control of user login, face recognition, and over the data.

User Authentication:

JWT (JSON Web Token) was implemented for the purpose of securing API.

After facial recognition, the user is allowed to log into the system and is given a JWT token that allows him or her to access the dashboard and material management.

API Endpoints

User Management:

The following endpoints were developed for the registration of users, facial recognition for login, and getting the user details respectively.

Material Management:

AMS enables the user to enter materials while registering and modify or remove them as required.

Entry/Exit Logs:

In addition to the time, the system records details of entry and exit, materials entered, and the user identification number among others. The logs are displayed in the admin dashboard for monitoring.

4.4 Facial Recognition Integration

The Face-api.js library was implemented in the frontend as well as the backend part.

The backend captures image data from the front and pre-processes it for feature extraction of the face and then compares this data set with a master data set for the user.

If the user is successfully recognized the system will show the list of materials entered and registered for entry verification.

Database Configuration

The database configuration was set up using MongoDB: The database configuration was set up using MongoDB:

Users Collection:

It stores the personal details of users, facial recognition data that are hashed to enhance security, and materials that registered users upload.

Entry Logs Collection:

Contains information about the time the user entered the store, the list of registered materials, and facial data for entry recognition.

Exit Logs Collection:

Records the exit of the user, the materials that the user has checked in as well as those which the system has checked out on his/her behalf. These discrepancies are brought out, especially for security personnel.

4.5 Testing

Unit Testing: Each part and activity of the product were verified in order to make sure all functions work according to their conception.

Integration Testing: Interacted between the front-end forms and the back-end API calls.

Performance Testing: Tested the application's functionality under numerous circumstances such as many users using the app at once.

Usability Testing: Completed with the focus group to see whether there are any UX problems **and to ensure a smooth interaction between the user and the interface.**

4.6 Challenges and Solutions

Facial Recognition Accuracy: There are some issues found with the identification of faces in the context of developing the system with different lighting conditions. This was done by improving the image preprocessing and refining the facial recognition algorithm.

Data Privacy: This brought much focus to making sure that there was proper collection, storage, and management of facial data. It is also as mentioned earlier secured through encryption for storing any data and it also complies with privacy rules and regulations.

Offline Functionality: Since the app was in the cloud, it was still a challenge to ensure that ‘entry and exit’ data would always be available in case the internet went down. To optimize the data access a temporary caching system was introduced where data was cached locally for recent requests.

4.7 Summary

To ensure that the “Facial Entry and Exit Security App” was effectively developed and implemented the following iterative development process was followed using modern technologies including React.js, Node.js, MongoDB, and Face-api.js. The app also handles entry and exit management in a secure manner with face recognition ability to track the belongings of the users thus eliminating security issues compared with those of traditional systems. The last application has gone through usability and security testing to provide an effective solution for handling personal Southeast belongings at school and the workplace as required.

5 CHAPTER 5: CONCLUSION AND RECOMMENDATION.

5.1 Conclusion

The Facial Entry and Exit Security Application is one of the newest and innovative software aimed at simplifying the ways of using face recognition algorithms for tracking the movements of personnel. Overall, the application makes security and convenience much better as compared with traditional practices like ID cards or manual sign-in. The system by employing AI's facial recognition logs entrants and exits effectively hence suitable in business establishments, schools, etc.

The development process entailed the consideration of various technologies including HTML, CSS, JS, Node.js for computing and processing back-end results, and MongoDB for storing data. The use of face-api.js helped in the process of adopting facial recognition functionality into the work, and other functions such as session management, role access control, and data-free features were included to add to the security of the system.

It can, therefore, be said that this application has succeeded in achieving the aims of developing an effective software that would capacitate easy and secure logging of entries and exits. This openness allows the system to report in real-time as well as its data analysis for better management, thus improving operational performance.

5.2 Recommendations

Enhancing Security Measures: As for facial recognition, it is suggested to apply more secure layers that will enhance security of the sensitive areas such as Multi-Factor Authentication.

Continuous Model Training: Whenever the number of users registered in the system increases, it becomes useful to retrain the system so as to ensure that the facial recognition model has high precision especially when dealing with different types of individuals and climatic conditions.

Scalability: Designing the system, it has to be in a way that would allow for its further expansion, especially when an organization is huge encompassing numerous employees or students. It can be done through the optimization of the backend support and integration of cloud solutions.

Integration with Other Systems: Also, there should be syncing of the facial log system with other security systems, attendance management, or HRM systems to come up with a single hub to contain all the data and make the organizational processes easier.

Mobile Application Improvements: In order to improve the ergonomics and usability of the users of the platform, more improvements should be distinguished in the mobile design. These can include increasing efficiency of performance on various devices, incorporating today's 'offline mode', and increasing the interaction speed of the function using facial recognition algorithms in different lights.

6 REFERENCES

- Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377–387. <https://doi.org/10.1007/s43681-021-00077-w>
- Chen, D. M. H. (2022). Issues and Strategies of Localising Sensitive Audiovisual Elements in Game Streaming: A Case Study on Overwatch League (OWL) Chinese Streaming. *British Journal of Chinese Studies*, 12(2), 154–179. <https://doi.org/10.51661/bjocs.v12i2.191>
- Ferrara, E. (2023). *Fairness And Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, And Mitigation Strategies*. <https://doi.org/10.3390/sci6010003>
- Jain & Li, 2019. (2023). Correction to: Genomic analyses in African populations identify novel risk loci for cleft palate. *Human Molecular Genetics*, 32(12), 2117–2117. <https://doi.org/10.1093/hmg/ddad027>
- Mingtsung, C., Wei, Q., Jiaqi, H., & zhuomin, Z. (2020). Research on the application of face recognition system. *Journal of Physics: Conference Series*, 1684(1), 012126. <https://doi.org/10.1088/1742-6596/1684/1/012126>
- Siau, K., & Wang, W. (2020). Artificial Intelligence (AI) Ethics. *Journal of Database Management*, 31(2), 74–87. <https://doi.org/10.4018/JDM.2020040105>
- Singh, B., Korstad, J., Guldhe, A., & Kothari, R. (2022). Corrigendum: Editorial: Emerging Feedstocks & Clean Technologies for Lignocellulosic Biofuel. *Frontiers in Energy Research*, 10. <https://doi.org/10.3389/fenrg.2022.972074>
- Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & SOCIETY*, 37(1), 167–175. <https://doi.org/10.1007/s00146-021-01199-9>
- Zhou, Y., Liu, D., & Huang, T. (2018). Survey of Face Detection on Low-Quality Images. *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*, 769–773. <https://doi.org/10.1109/FG.2018.00121>