DESIGN AND IMPLEMENTATION OF SMART CONTROL ACCESS SYSTEM IN INSTITUTIONS: CASE OF EXAM ROOMS AT ULK

BY: CITO MATABA ARMAND

ROLL NUMBER: 202150372

Research project submitted in partial fulfillment of the requirement for award of advanced diploma in Electronics and Telecommunication Technology

Supervised by: Eng. ISAAC Tumwine

September 2024

DECLARATION

I, CITO MATABA Armand, declare that this research study is my original work and has not been presented for a degree or any other academic award in any University or Institution of Learning". No part of this research should be reproduced without the author’s consent or that of ULK Polytechnic Institute.

Supervisor name:

Sign: Date:

APPROVAL

This research project entitled " **Design and implementation of Smart control access system in institutions: Case of exam's rooms at ULK"** prepared and submitted by CITO MATABA Armand in partial fulfillment of the requirement for award of advanced diploma (A1) in Electronics and Telecommunication Technology has been examined and approved by the panel on oral examination.

Name and Sig. of Chairperson:

Date of Comprehensive Examination:

DEDICATION

This research project is dedicated to my family and friends for their financial and moral support and encouragement throughout my academic journey. To my professors and institutors, whose guidance and wisdom have been invaluable.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to everyone who has supported me throughout the process of completing this research project.

First and foremost, I extend my sincere thanks to my institutors and faculty members at ULK Polytechnic for their encouragement and for providing a favorable learning environment.

A special thanks to my family for their constant love, patience, and encouragement, which have been my source of strength. To my classmates, thank you for your companionship, advice, and moral support.

Lastly, I would like to acknowledge specially my friends and roommates for their assistance and contributions.

ABSTRACT

This project presents the design and implementation of a smart access control system for exam rooms using NodeMCU, RFID technology, LCD display, and Wi-Fi connectivity integrated with a Django-based backend. The primary objective is to enhance security, rapidity and streamline the management of student access during examination periods.

The system utilizes RFID cards for student identification, where each card is registered in a database hosted on a Django server. When a student scans their RFID card at the entrance, the NodeMCU retrieves the card data and sends a request to the Django server to verify the student's identity and access permissions. Based on the response, the system displays an appropriate message on the LCD screen, indicating whether access is granted or denied. Additionally, visual indicators such as green and red lamps provide immediate feedback on the access status.

A website with "ulkcontrolservice.onrender.com" as domain name is deployed to ensure every student can see his/her personal details and a messaging system where he/she can claim or request access to administrators of school who manage access and individual details on their interface of the same website. This project addresses the need for a secure, fast, reliable, and user-friendly access control solution in educational institutions, aiming to prevent unauthorized entry and enhance the rapidity in accessing examination rooms.

The implementation details, system architecture, and potential applications of the proposed solution are discussed, highlighting its effectiveness and scalability for broader use in similar scenarios.

Keywords: Smart access control system, RFID Technology.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACCRONYMS AND ABBREVIATIONS

ICT: Information and Communication Technologies

IoT: Internet of Things

LCD: Liquid Crystal Display

NodeMCU: Node MicroController Unit

RFID: Radio Frequency Identification

ULK: Kigali Independent University

UPI: ULK Polytechnic Institute

CHAPTER ONE: GENERAL INTRODUCTION

1.0 Introduction

Nowadays, multiple information and communication technologies (ICT) have the potential to develop society and directed towards several domains such as health, industry, and social life. In recent time, their use progresses considerably to cover education field, and have significant impact on the learning outcomes. In the context of the development of traditional practices towards modern education, ICT have become tools which characterize a whole generation henceforth defined as 'digital natives', who have gone far from textbooks and similar traditional tools. A number of digital tools, mobile devices and platforms are now available to education fields. It can therefore rethink education and assessment practices, methods and educational environments. Therefore, technology should be fully integrated not only in learning but in classes and examination rooms as well (Mrabet & Abdelaziz, 2020).

This project uses the advancements in RFID technology and the Internet of Things (IoT) to develop a smart access control system for examination rooms. The system integrates a NodeMCU (ESP8266) microcontroller or ESP32, an RFID reader, an LCD display, and Wi-Fi connectivity with a Django-based backend. Each student is assigned an RFID card with unique identification data stored in a centralized database. Upon scanning their RFID card at the entrance, the NodeMCU reads the card data and communicates with the Django server to verify the student's identity and access privileges in real-time.

The system provides immediate feedback through an LCD display, indicating whether the student is granted or denied access based on the server's response. Additionally, visual indicators such as green and red lamps enhance the user experience by providing clear access status.

In this chapter, we provide an overview of the issues associated with the current methods at ULK and potential applications of the proposed solution are discussed, highlighting its effectiveness and scalability for broader use in similar scenarios.

1.1 Background of the study

Access control systems play a crucial role in securing sensitive areas and ensuring that only authorized individuals can gain entry. Traditionally, educational institutions have relied on manual methods. However, this method is labor-intensive, prone to human error, and can be easily compromised as the number of students increases while the personal assigned to control remain the same.

Despite the advancements that technology has made, many institutions continue to face challenges in managing access leading to cheating, theft, other security breaches and lateness. There is a clear need for a more reliable and efficient access control system that can address these challenges. By integrating RFID technology with microcontrollers and web-based applications, it is possible to create a system that provides real-time monitoring and data management, further improving security and efficiency and rapidity.

By exploiting the capabilities of modern technologies, this project seeks to offer a scalable and reliable solution for institutions and especially educational institutions, ensuring that only authorized individuals can access examination rooms.

1.2 Statement of the problem

Ensuring the security and integrity of examination rooms is a critical concern for educational institutions. Traditional access control methods, such as manual checks: verifying student names on a list, signing present by hands and as proof a shit of paper, are often insufficient in preventing unauthorized access and extremely slow in processing. The fact is students get stressed as the waiting line take time to end.

The primary problem is the lack of a robust, efficient, and reliable access control system that can ensure only authorized individuals gain entry to examination rooms causing frustration on behalf of students and personnel. Slowness and unauthorized access can lead to cheating, theft, case of missing exams ultimately undermining the credibility of the examination process and the institution as a whole.

Given these challenges, there is a clear need for an advanced access control solution that leverages modern technologies to enhance security and efficiency. This research project aims to address the identified problems by providing real-time verification of student identities and access privileges, reducing administrative workload and avoiding stress and miss of exams for students.

1.3 Purpose of the study

By analyzing the issues that many institutions observe with controlling access and especially difficulties students face to access examination rooms, the successful implementation of this access control system is set to significantly improve the security of examination rooms by ensuring that only authorized individuals can gain entry and rapidly. This will help in maintaining the integrity of the examinations, procuring satisfaction to the stressed queue. Also, the use of a similar system in other institutions will streamline the process of managing access, reducing the administrative burden on staff and improving overall operational efficiency.

1.4. Research Objectives

This system aims to enhance security, rapidity, efficiency, and reliability in managing student access examination rooms. To achieve this objective, the following specific objectives are outlined:

1. To design a database well structured.
2. To design and develop interfaces.
3. To integrate a Real-Time Verification System.

1.5 Research questions

These research questions are aligned with our research objectives and will help ensure that our study is comprehensive and covers the necessary aspects:

1. How to design a database well structured?
2. How to design and develop interfaces?
3. How to integrate a Real-Time Verification System?

1.6 Scope

This study focuses on developing and implementing a smart access control system for examination rooms at ULK. The theoretical scope includes analyzing current access control challenges, developing a real-time RFID-based verification system, and integrating visual indicators and a user-friendly interface. The content scope encompasses the use of NodeMCU RFID technology, an LCD display, Wi-Fi connectivity, and a Django-based backend, along with a website for students to verify their access status. This research will not address policy-making or administrative decisions related to access control.

1.7 Significance of the study

This study aims to revolutionize access control systems in educational institutions by developing a smart system using NodeMCU, RFID technology, and a Django-based backend.

To the researcher that I am, the realization of this project will prove the capacity of linking converting the theoretical lessons we learn to practices by solving society problems.

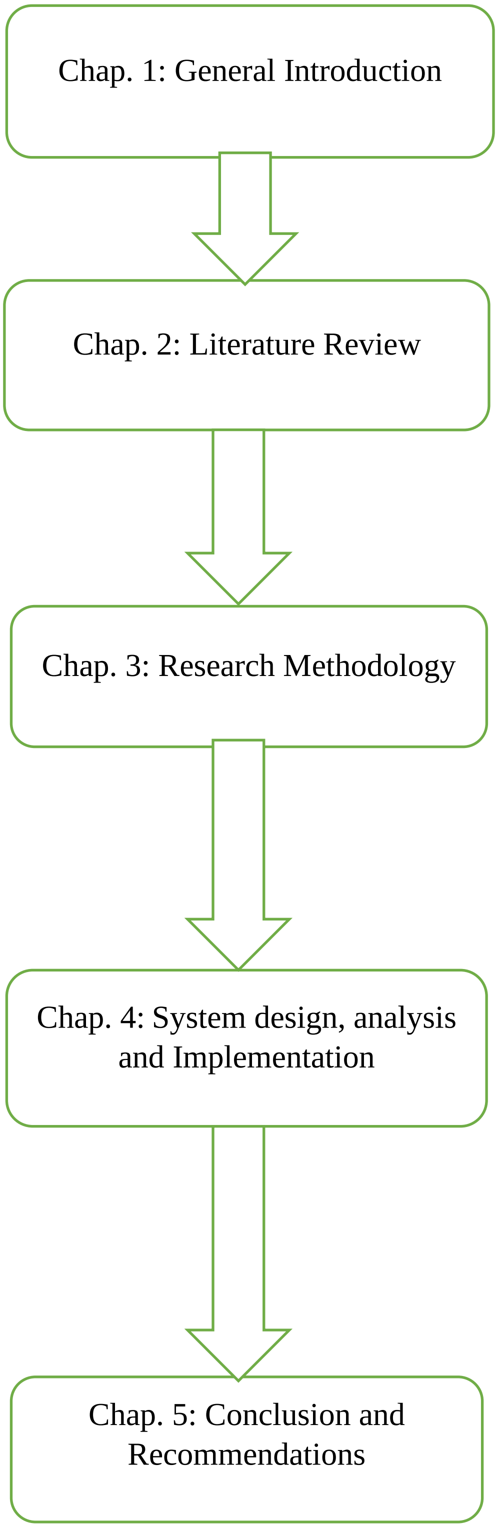
This innovative solution seeks to enhance rapidity, security, efficiency, and reliability in managing student access to examination rooms, significantly. Students will benefit from a smoother, more reliable access process, reducing stress and delays before exams, while an online verification system will offer them the convenience of checking their access status and requesting assistance when needed.

Staff and administrators will experience reduced administrative burdens, as the system will streamline the process of monitoring and managing student access. The automated verification and real-time feedback mechanisms will ensure more accurate and efficient record-keeping, freeing up valuable time for other critical tasks. Additionally, this study contributes to the field of IoT and access control systems by demonstrating an innovative application of modern technologies. The scalability and versatility of the system suggest it could be adapted for use in other institutions, such as corporate offices or healthcare facilities, highlighting its broader impact and significance.

1.8 Organization of Study

This study is composed by 5 chapters as Figure 1 can show:

Figure 1.1. Organization of the Study


Chap. 1: General Introduction
Chap. 2: Literature Review
Chap. 3: Research Methodology
Chap. 4: System design, analysis and Implementation
Chap. 5: Conclusion and Recommendations

The chapter One gave an introduction and defines the topic with its objectives, research questions, the background of the study to guide us to achieve its purpose.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter provides a comprehensive review of the existing literature relevant to the development and implementation of smart access control systems in educational institutions. It explores key concepts, opinions, and ideas from experts, discusses the theoretical frameworks underpinning the study, and examines related empirical studies. The review aims to identify gaps in the literature and establish a foundation for the current research.

2.1 Concepts, Opinions, Ideas from Authors/Experts

Efficiency and Reliability:

The integration of RFID technology and IoT in access control systems has been extensively studied in recent years. According to Alhelaly (2023), RFID technology offers a reliable and efficient method for managing access control in various settings, including educational institutions. Akpinar and Hakan (2010) highlight the benefits of using IoT to enhance real-time monitoring and data management, which significantly improves security and operational efficiency. Administration systems for automatically managing routine have-to-do works of school staff and students with the aid of computers are one of them (Akpınar & Hakan, 2010). The reliability of these systems is also a major advantage, as they provide real-time verification and immediate feedback to users, thereby reducing the likelihood of human error and administrative burden (Akpınar & Hakan, 2010).

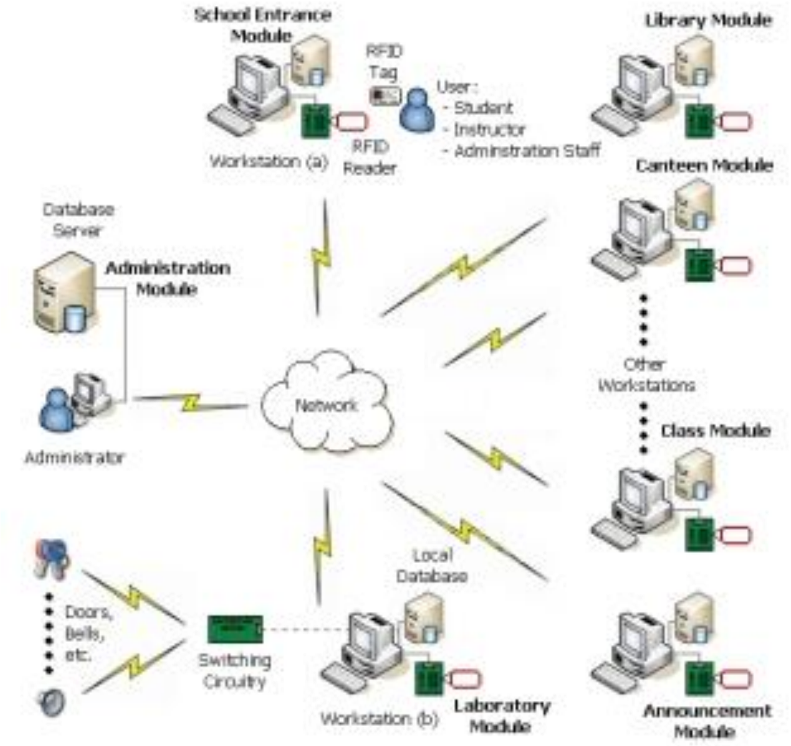
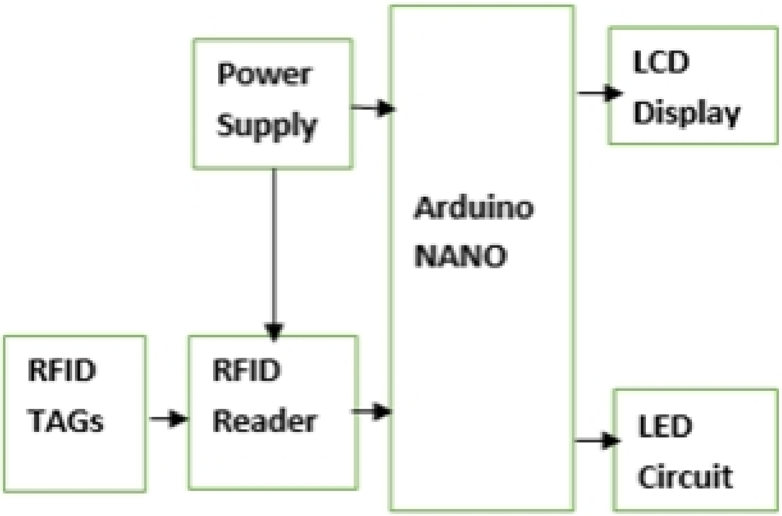


Figure 2.1: System design (2010)

Security in Access Control Systems:

Several studies have demonstrated the effectiveness of RFID-based access control systems in reducing unauthorized access and enhancing security. For instance, University of Oklahoma conducted a study on the implementation of an RFID-based access control system for their students, which resulted in a significant decrease in security breaches and unauthorized entries. These technologies offer a more reliable and efficient means of managing access, ensuring only authorized individuals can enter examination rooms (Vandana, Kumar, Sivani, Devanand, & Venkatanarayana, 2018). Their proposed system is shown in figure 2.2.



` *Figure 2.2: Proposed System without IoT(2018)*

IoT and RFID Technologies:

The application of IoT and RFID technologies in access control systems has been a focus of recent research. These technologies enable automated data collection and processing, allowing for seamless integration with other systems and enhanced data security (D, Kundu , & Kaur, 2012). Case studies in various institutions have demonstrated the effectiveness of these technologies in improving operational efficiency and security. The implementation of similar systems has also proved the advantages they present. The figure 4 shows how large applications of RFID with IoT are.

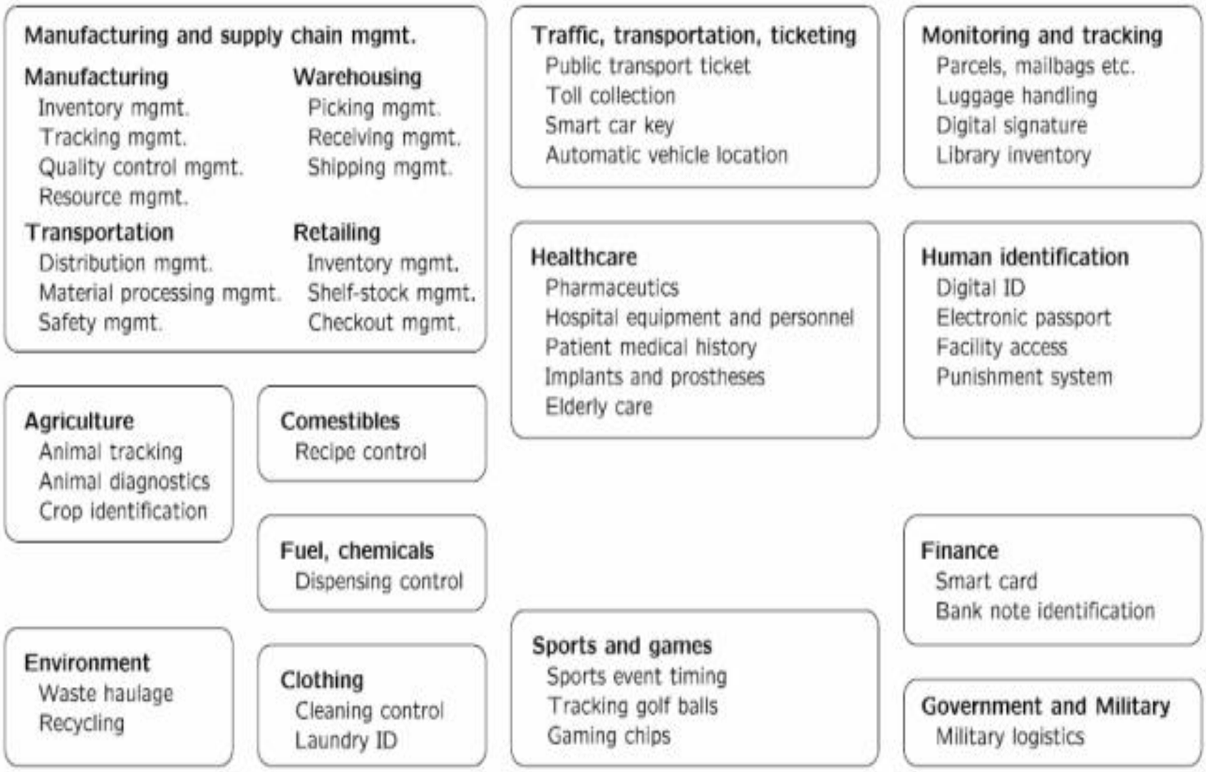


Figure 2.3 Applications of RFID technologies

2.2 Theoretical perspectives

The theoretical foundation of this project is based on the principles of universal computing and the Internet of Things (IoT). Universal computing, as described by Steve Jobs (1997), refers to the seamless integration of technology into everyday environments, enabling real-time data collection and processing. The IoT framework, as outlined by Samuel Greengard, involves the interconnection of devices and systems to facilitate communication and data exchange.

The use of RFID technology in access control systems aligns with these theoretical perspectives by enabling real-time monitoring and data management. This approach enhances security and operational efficiency.

2.3 Related studies

RFID and IoT systems enhance security and convenience on campus, making it easier for students to access facilities and services

The Axia Institute at Michigan State University has conducted extensive research on the use of RFID in healthcare, exploring its benefits and costs. Similarly, The University of Texas at

Arlington conducted research on the use of IoT in smart campus solutions, demonstrating the potential for real-time monitoring and data management to enhance security and operational efficiency.

Another relevant study by Samantha H. and Golui K. (2019) focused on the application of RFID technology in library management systems. The findings indicated that RFID-based systems improved inventory management and reduced instances of lost or misplaced items, highlighting the versatility and effectiveness of RFID technology in various contexts.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

In this chapter, i discuss the research methodology employed in investigating the control of access to examination rooms. This includes the overall research design, the population of interest, the sample size, and the methods used to gather and analyze data. These components are crucial in ensuring the reliability and validity of the research findings.

3.1 Research Design

The research design provides a framework for the study and helps in planning the entire research process. For this project, which focuses on controlling access to examination rooms, an **action design research** is employed. As it is a dynamic approach aimed at both understanding and improving a specific situation or system. It involves actively implementing changes and monitoring the effects to refine and improve the approach continuously. Given that my project involves the implementation of a prototype for controlling access to examination rooms, Action Research is indeed an appropriate choice.

3.2 Research Population

The research population consists of all individuals and systems involved in the examination process within our institution. This includes:

- **Students**: All students registered at ULK.
- **Examination Supervisors and Invigilators**: Personnel responsible for monitoring and enforcing examination regulations.

The **target population** is specifically the students and staff of the institution's examination departments, as the findings aim to generalize to this group. The study will collect data from these groups to assess how well the access control measures function and identify any challenges or areas for improvement.

3.3 Sample Size

Determining the appropriate sample size is essential for the reliability of the study's findings. The sample size must be large enough to represent the target population accurately but manageable within the constraints of the study. For this research, the sample includes:

- A representative number of students from different faculties and years of study, selected using random sampling to ensure diversity in the sample.
- Some available examination supervisors involved with access control of examination rooms.

3.4 Research Instrument

3.4.1 Choice of the Research Instrument

For this study on controlling access to examination rooms, these research instruments are utilized:

- **Interview Guide**: Semi-structured interviews conducted with key stakeholders, such as administrators and technical staff, to gain deeper insights into the challenges and advantages of the current and proposed access control systems.
- **Observations**: I observe all participants and try to identify their feelings with the actual system (this has started since our first year of study at ULK and has motivated our need to improve and develop a smart control system which is the topic of this research)

3.4.2 Validity and Reliability of the Instrument

To ensure the validity and reliability of the research instruments:

- **Validity**: Content validity is established by ensuring that the instruments cover all relevant aspects identified in the literature review. Experts in the field will review the instruments to confirm their appropriateness and comprehensiveness.
- **Reliability**: The reliability of the instruments is tested using a pilot study, where the instruments will be administered to a sample similar to the study population.

3.5 Data Gathering Procedures

The data gathering process were conducted in three phases:

1. **Pre-implementation**:
   - Obtain ethical clearance from relevant bodies.
   - Pre-test the instruments with a small sample.
2. **Implementation**:
   - Conduct semi-structured interviews with key stakeholders.
   - Use the observations to analyze problems faced
3. **Post-implementation**:
   - Collect and secure all data.
   - Follow up with participants if additional information is needed.
   - Thank all participants and provide feedback where appropriate.

3.6 Data Analysis and Interpretation

Data analysis will involve both qualitative and quantitative methods:

1. **Quantitative Data**: Data from observations will help to analyze how often students and staff get issues with the actual system of controlling access. For example, Count the number of students who think they are allowed to participate but find their names not on the lists, or for staff, count the number of problems faced by not recognizing the examination room where each class is assigned to sit for exams, …
2. **Qualitative Data**: Data from interviews and observations will be analyzed using thematic analysis. This involves coding the data to identify key themes and patterns, which will be interpreted in the context of the study's objectives. This will be crucial for ameliorating the new system and help all users to adopt it.

Interpretation of findings

The interpretation of the analyzed data focused on addressing the research objectives and questions. Key points for interpretation include:

1. **Effectiveness of the Access Control System**:

   The data has been interpreted to determine the system's effectiveness in restricting access to authorized individuals only. The results indicated that the system successfully can prevent unauthorized access and whether the measures taken are perceived as adequate by the stakeholders for the following reasons:

      1. The database's ability to store and retrieve data accurately and efficiently, which is crucial for real-time verification.
      2. The database design supports the system's functionality, including the organization of data related to student identities, access permissions, and logs of access attempts.

2. **Challenges and Users Perceptions and Satisfaction**:

   Analysis of the qualitative data has highlighted challenges or issues encountered with the actual system. On the other hand, if objectives reached, the system will offer ease of use for all users, accuracy and rapidity enhanced. The reason is that the user-interfaces facilitate easy interaction for students and staff

3. **Comparative Analysis**:

   Comparing the two systems (the actual and the proposed) helped us to understand the advantages that offers the new system. From users that we've observed to the administrators and staffs to whom we've asked questions, the impacts that the implementation of the new system is huge:

   1. The performance of the real-time verification system, including its accuracy in identifying authorized users and preventing unauthorized access and the effectiveness of the RFID system are unbelievable compared to the actual system with papers, signature and paper as proof.
   2. The integration process's effectiveness, including how well the new system performs in real-time scenarios. With the actual system, for example, if a student pays in the morning, he/she got to bring a photocopy of his/her card with the signature of finance office. This is subjects to human errors, fraud and the process time is long. For the new system, intervenants loved the facts that as

soon as the finance office recognizes that you’ve paid, your card is assigned an access authorized.

3. Also the management of derogation and requests is online, rapid and efficient with the new system compared to the actual where waiting line is long and can’t finish in delay of starting time for exams days.

Overall, the interpretation aimed to provide a comprehensive understanding of the system's performance, the problem faced with actual system and areas for improvement par rapport au system actual. The conclusions drawn from the interpretation will inform recommendations for policy and practice regarding the control of access to examination rooms.

3.7 Ethical Considerations

The study adheres to ethical principles to ensure the safety, social, and psychological well-being of participants. The following measures have been taken:

- **Informed Consent**: Participants were informed about the study's purpose, procedures, potential risks, and benefits.
- **Confidentiality**: All personal data are anonymized, and only aggregate data are reported.
- **Right to Withdraw**: Participants were informed of their right to withdraw from the study at any time.

Ethical clearance will be sought from the relevant ethics committee, and all procedures will be in line with ethical standards.

3.8 Limitations of the Study

The study encountered several limitations, including:

- **Sample Size and Diversity**: The study's findings may be limited by the sample size and diversity. ULK counts more than thousand students. While efforts have been made to ensure a representative sample, logistical constraints limited participation from certain groups.

- **Response Bias**: Participants may not provide accurate responses due to confidentiality, social desirability bias or misunderstanding of the questions. The critical aspect of the topic is the main cause.
- **Technical Issues**: Technical challenges during the implementation and testing of the access control system prototype affected analysis and improvements, costs of components for example.

These limitations were acknowledged, and efforts were made to minimize their impact. For instance, the use of multiple data sources reduced biases and enhanced the reliability of the findings.

CHAPTER FOUR: SYSTEM DESIGN, ANALYSIS, AND IMPLEMENTATION

4.0 Introduction

In this chapter, i delve into the technical aspects of the access control system for examination rooms. The chapter covers the design, analysis, and implementation phases, including the necessary calculations, drawings, specifications, and cost estimation. These components are crucial in ensuring the system's functionality, efficiency, and feasibility.

4.1 Drawings

This section provides visual representations of the system's design through various types of diagrams. These drawings are essential for understanding the physical layout, electronic connections, and logical flow of operations within the system. They serve as a blueprint for both the implementation and troubleshooting processes.

The system architecture diagram gives an overview of the entire setup, while the circuit diagrams focus on the electrical connections and flowcharts illustrate the process flow of user authentication and system operations.

a) **System Architecture Diagram:**

This diagram (fig. 4.1) offers a high-level overview of the system's components and their interactions. It illustrates how different modules, our kit, server, and the central database, are connected and communicate with each other. The diagram helps in visualizing the overall structure and flow of data within the system, providing a clear understanding of the system's architecture.

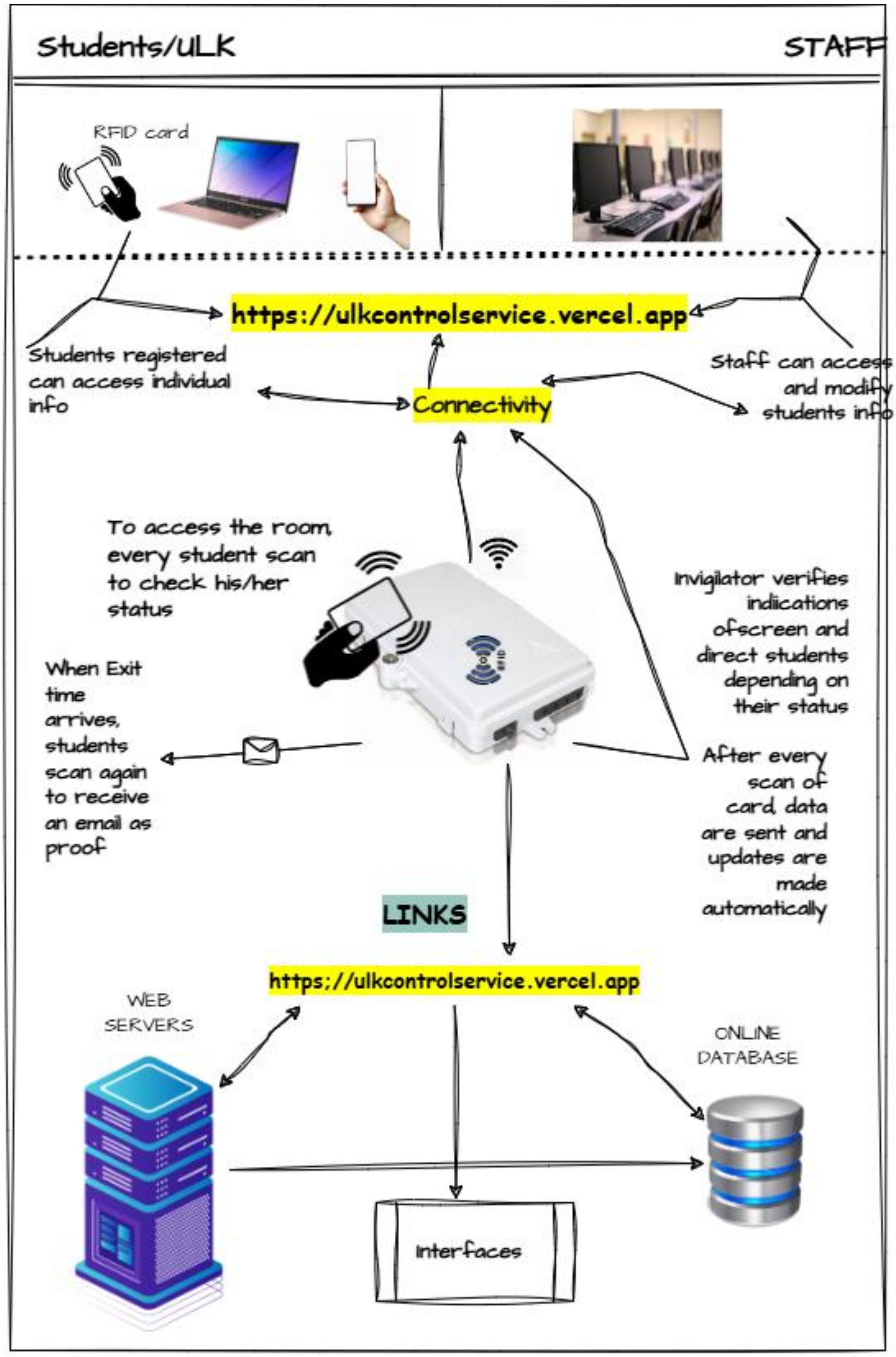

Students/uLK
STAFF
RFID card
https://ulkcontrolservice.vercel.app
Students registered can access individual info
Connectivity
Staff can access and modify students info
To access the room, every student scan to check his/her status
Invigilator verifies indications ofscreen and direct students depending on their status
When Exit time arrives, students scan again to receive an email as proof
After every scan of card, data are sent and updates are made automatically
LINKS
https://ulkcontrolservice.vercel.app
WEB SERVERS
ONLINE DATABASE
Interfaces

Figure 4.1: System Architecture Diagram

]

b) **Circuit Diagrams:**

This diagram presents detailed schematics of the electronic components involved in the system. It includes connections for the RFID readers, LCD screen, microcontroller, and power supply circuit. The circuit diagram shows how the various components are electrically connected, including the wiring, power sources, and data lines. This circuit is crucial for the accurate assembly of the system's hardware and for identifying the specific electronic requirements (Figure 4.2).

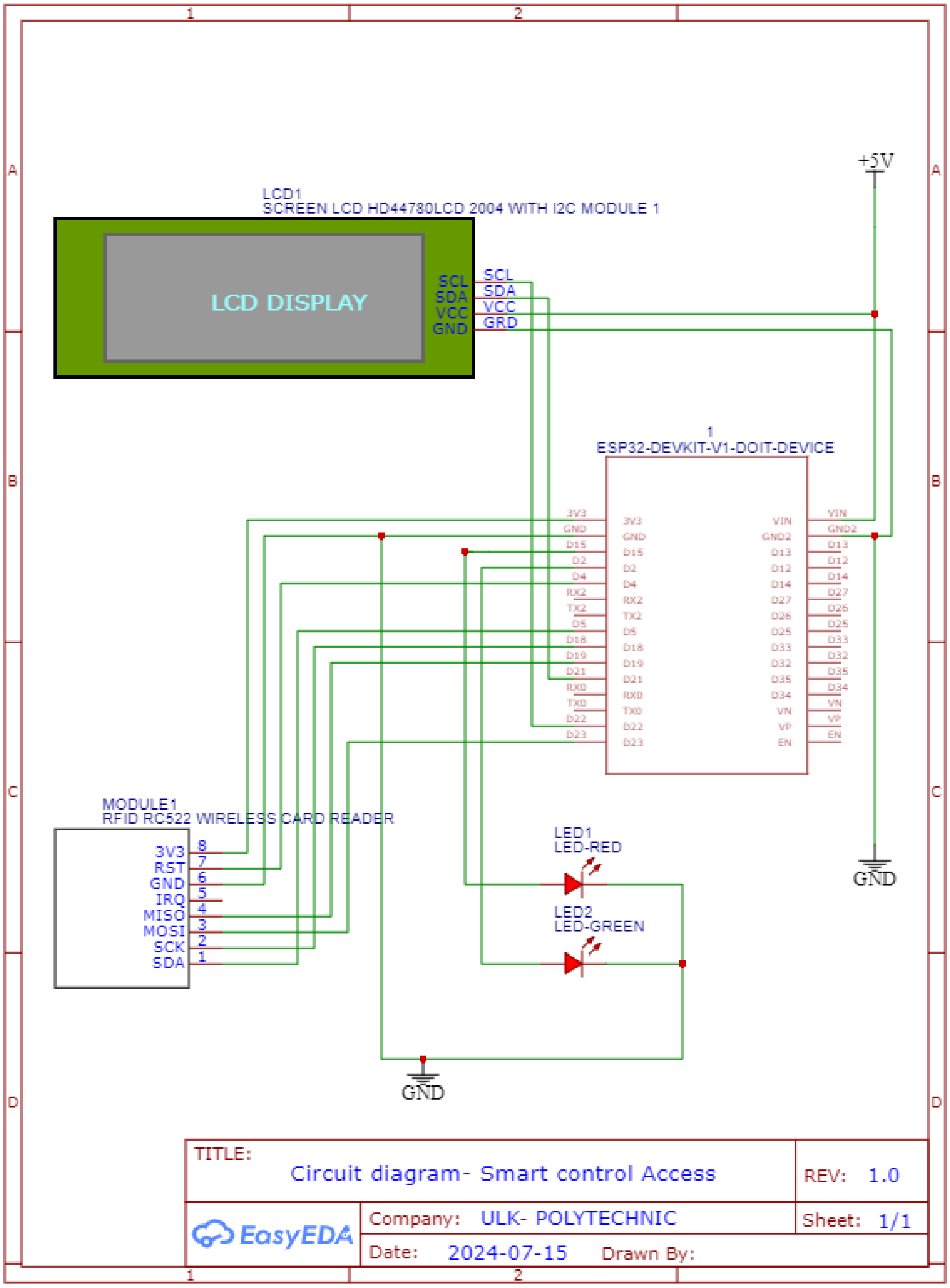


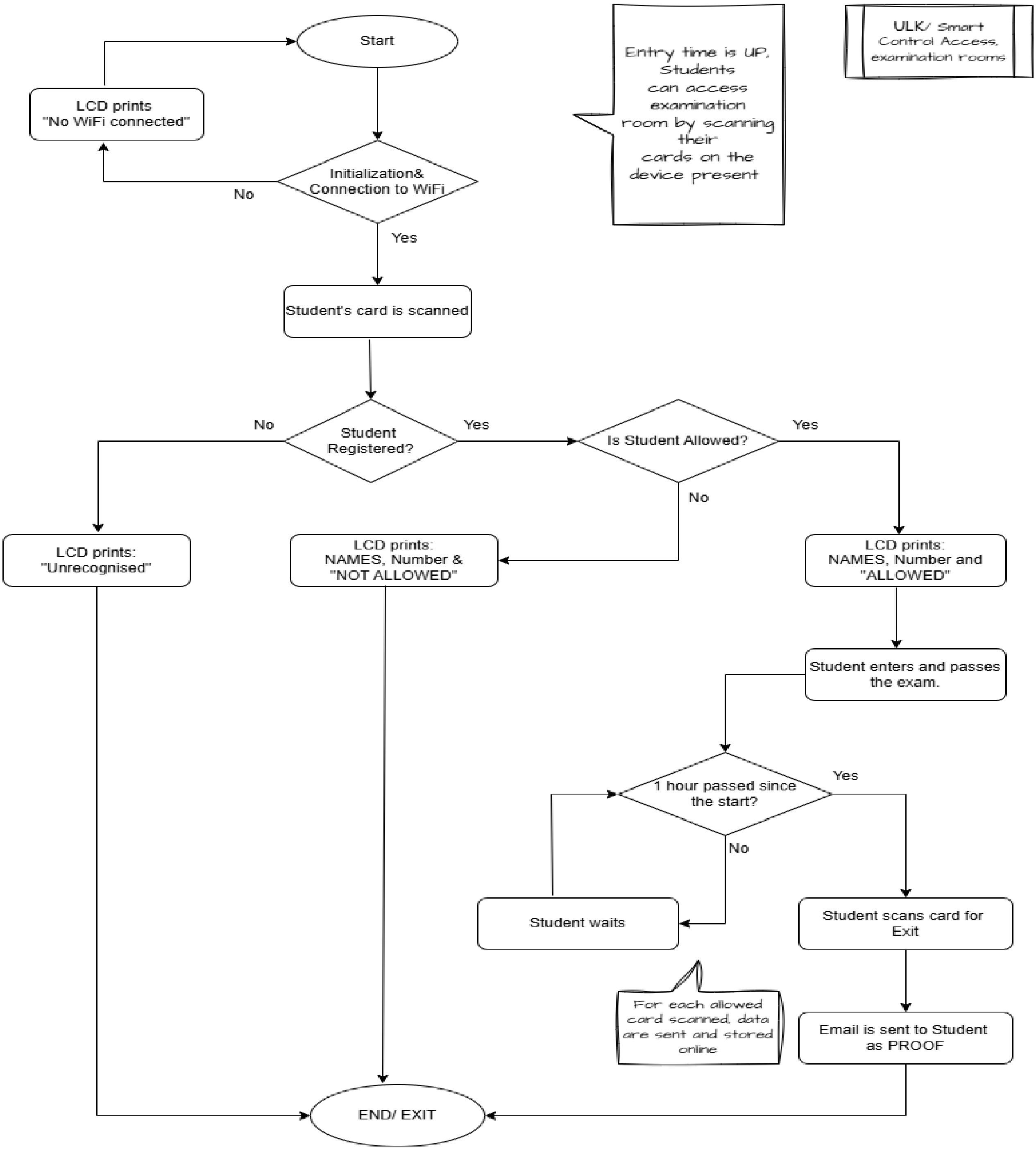
Figure 4.2: Circuit Diagram of the system

c) Flowcharts:

Flowcharts are used to depict the system's workflow, detailing the processes for user authentication, database queries, and system responses. They illustrate the sequence of operations, decision points, and data flow within the system.

- **Access Process (Examination rooms):**

Figure 4.3 Control Access Process


Start
LCD prints "No WiFi connected"
Initialization& Connection to WiFi
No
Yes
Entry time is UP, Students can access examination room by scanning their cards on the device present
ULK/ Smart Control Access, examination rooms
Student's card is scanned
Student Registered?
No
Yes
Is Student Allowed?
Yes
No
LCD prints: "Unrecognised"
LCD prints: NAMES, Number & "NOT ALLOWED"
LCD prints: NAMES, Number and "ALLOWED"
Student enters and passes the exam.
1 hour passed since the start?
Yes
No
Student waits
Student scans card for Exit
For each allowed card scanned, data are sent and stored online
Email is sent to Student as PROOF
END/ EXIT

- **User authentication (Website):**

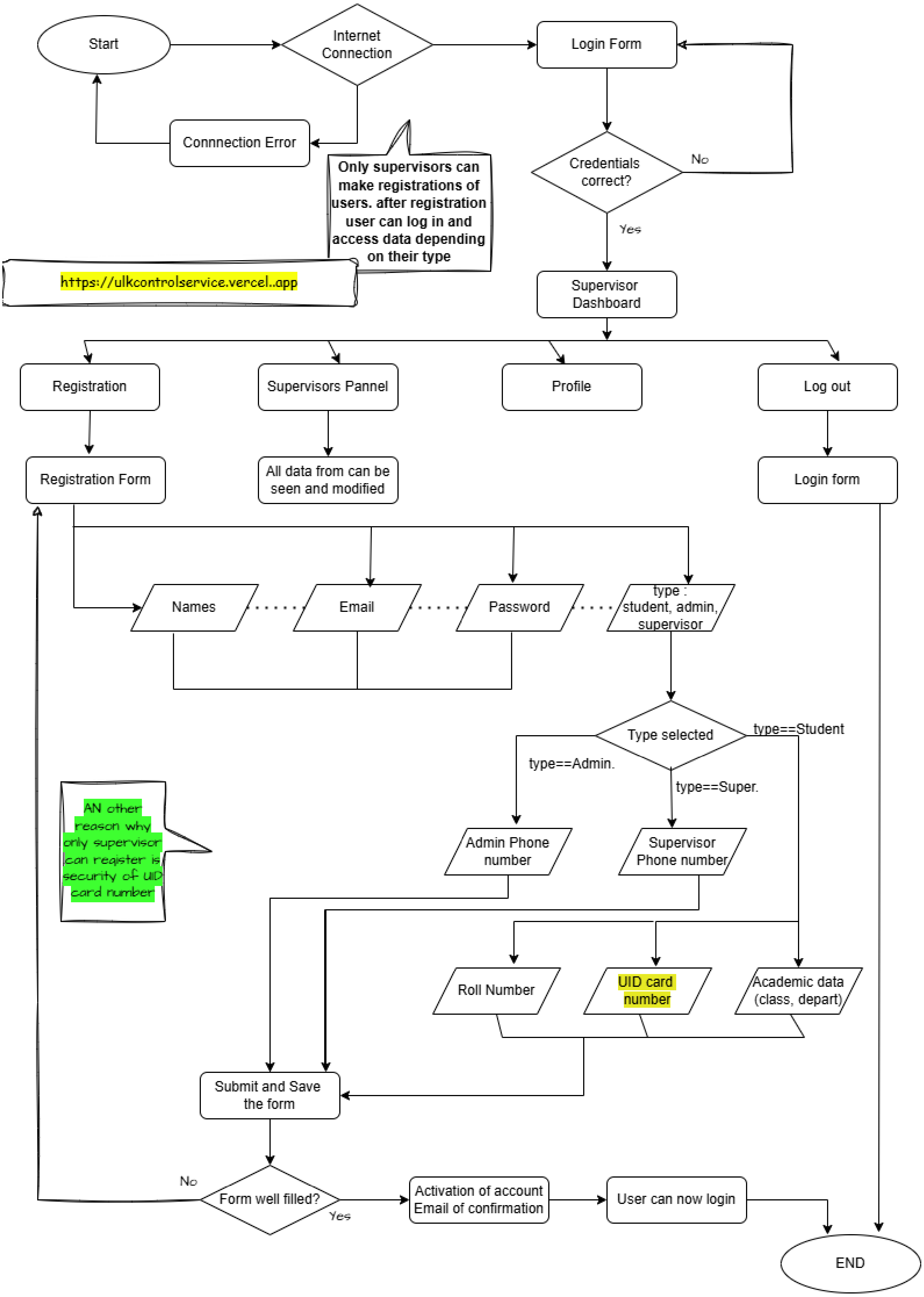
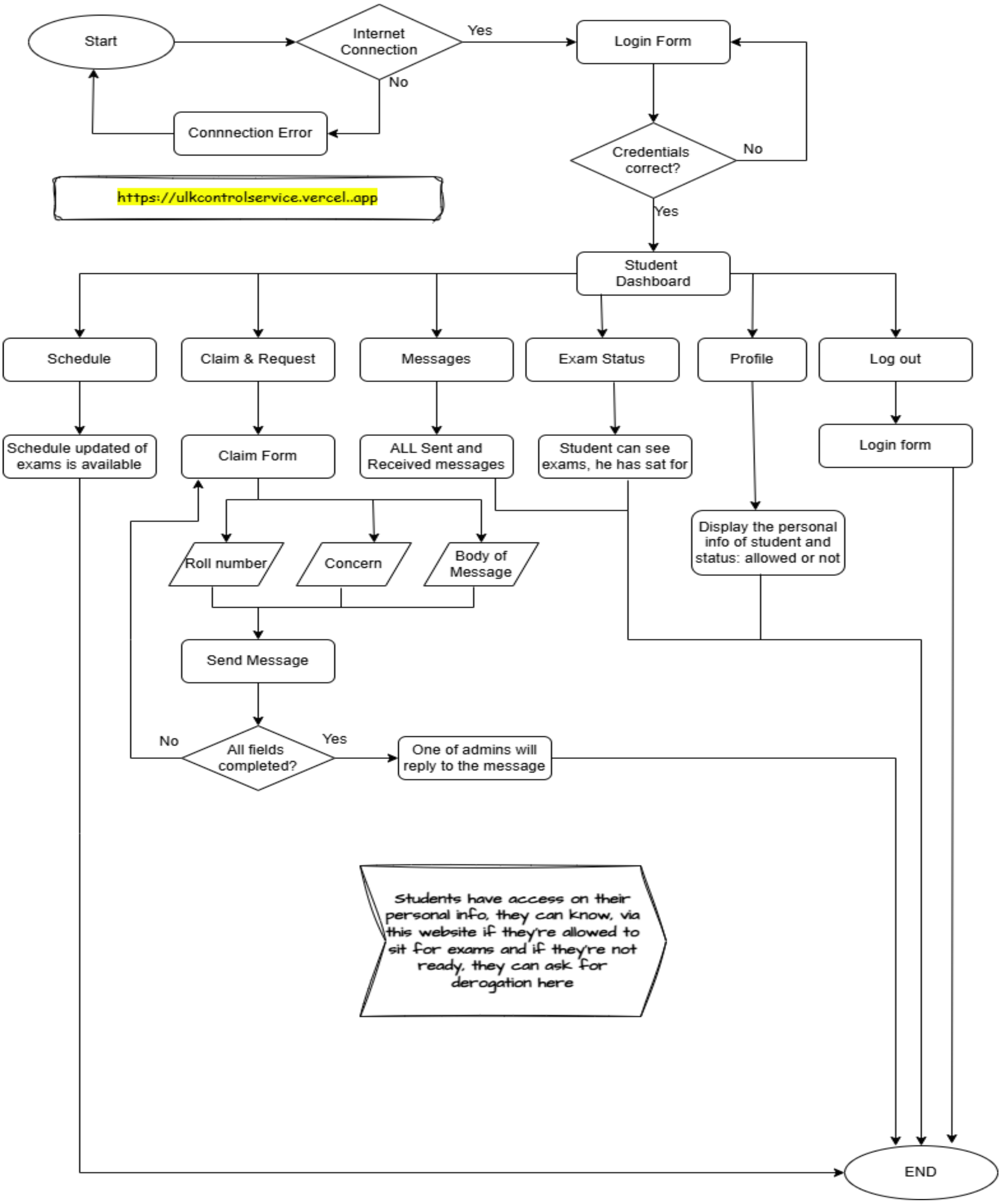

Start
Internet Connection
Login Form
Connnection Error
Credentials correct?
No
Yes
Only supervisors can make registrations of users. after registration user can log in and access data depending on their type
https://ulkcontrolservice.vercel..app
Supervisor Dashboard
Registration
Supervisors Pannel
Profile
Log out
Registration Form
All data from can be seen and modified
Login form
Names
Email
Password
type : student, admin, supervisor
Type selected
type==Student
type==Admin.
type==Super.
AN other reason why only supervisor can register is security of UID card number
Admin Phone number
Supervisor Phone number
Roll Number
UID card number
Academic data (class, depart)
Submit and Save the form
No
Form well filled?
Yes
Activation of account Email of confirmation
User can now login
END

Figure 4.4 Authentication

- **Dashboards (Website):**

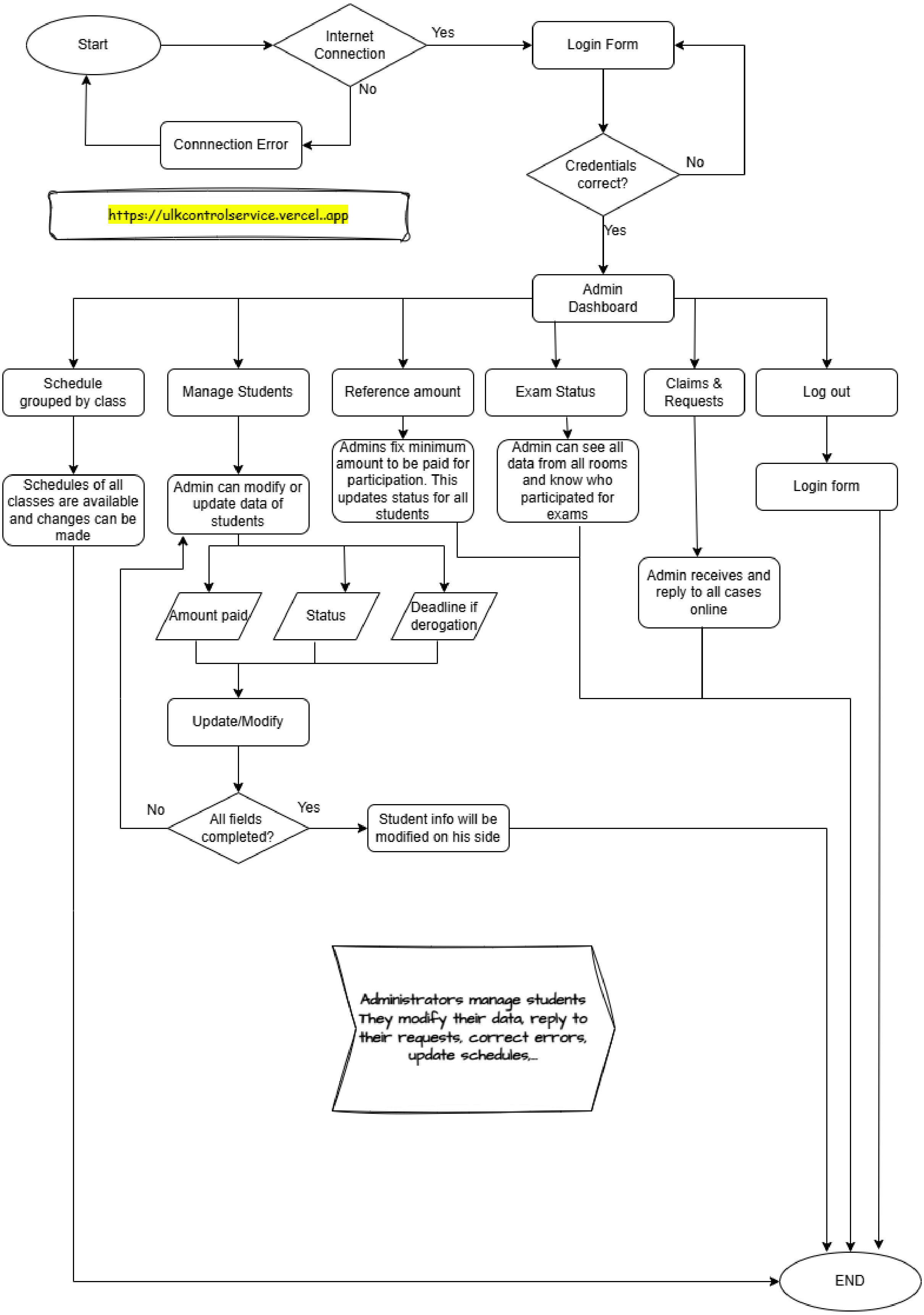
Students and admins do not share the same dashboard, Students have possibilities to access personal information, send request or claim. Admins have the possibilities to access all info of students, make changes and reply to their claims and their requests.

Figure 4.5 Student dashboard



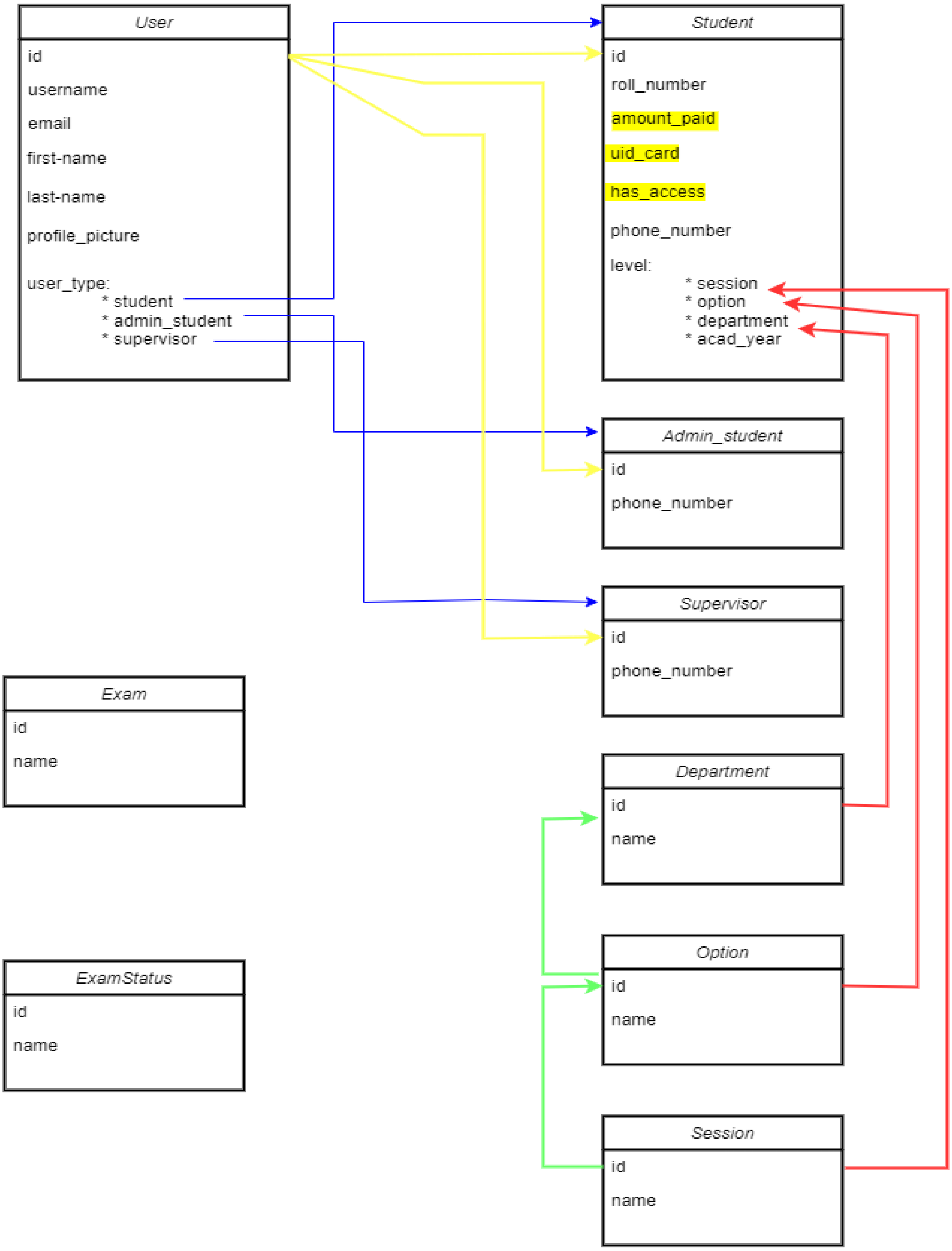
Start
Internet Connection
Yes
No
Login Form
Connnection Error
Credentials correct?
No
Yes
https://ulkcontrolservice.vercel..app
Student Dashboard
Schedule
Claim & Request
Messages
Exam Status
Profile
Log out
Schedule updated of exams is available
Claim Form
ALL Sent and Received messages
Student can see exams, he has sat for
Login form
Display the personal info of student and status: allowed or not
Roll number
Concern
Body of Message
Send Message
No
All fields completed?
Yes
One of admins will reply to the message
Students have access on their personal info, they can know, via this website if they're allowed to sit for exams and if they're not ready, they can ask for derogation here
END

Figure 4.6 Admins Dashboard


Start
Internet Connection
Yes
No
Login Form
Connnection Error
Credentials correct?
No
Yes
https://ulkcontrolservice.vercel..app
Admin Dashboard
Schedule grouped by class
Manage Students
Reference amount
Exam Status
Claims & Requests
Log out
Schedules of all classes are available and changes can be made
Admin can modify or update data of students
Admins fix minimum amount to be paid for participation. This updates status for all students
Admin can see all data from all rooms and know who participated for exams
Login form
Admin receives and reply to all cases online
Amount paid
Status
Deadline if derogation
Update/Modify
No
All fields completed?
Yes
Student info will be modified on his side
Administrators manage students They modify their data, reply to their requests, correct errors, update schedules,…
END

d) Database design

Table 4-7 Database structure



→ The arrows represent links that are between tables(classes). Foreign keys

4.2 Calculations

In this section, we perform and present the various calculations that are essential for the design and operation of the access control system. These calculations ensure that the system is designed to meet the required specifications and can handle the expected load. Here are the key calculations you should include:

1. **Power Requirements:**

   Components**:** RFID readers, LCD screens, microcontrollers, and other peripherals.
   Calculations based on recommended use:

   V stands for Voltage and I for Intensity.
   Formula: P= V*I

   - RFID Reader: V=3.3V, I=0.03A
   - LCD Screen: V=5V, I=0.02A
   - Microcontroller: V=3.3V, I=0.15A
   - Total Power: P_{total} = (3.3V×0.03A) + (5V×0.02A) + (3.3V×0.15A) = 0.694W

   The device will consume 0.694W equivalent of 694mW.

2. **Database Capacity:**

   The database used is kept online and possesses 25GB of memory which is high not only for research purpose but even for a project like such.

3. **Time Response**

   Calculate the expected response time for the system to verify access credentials and grant or deny entry.

   Formula: $T_{response} = T_{scan} + T_{transmit} + T_{process} + T_{display}$

   Considering the normal response time for each component, we have:

   RFID Scan Time: 50ms
   Data Transmission Time: 20ms
   Processing Time: 30ms
   Display Time: 50ms
   Total Response Time: Tresponse=50ms+20ms+30ms+50ms=150ms

   Considering WiFi Connection quality, this delay may be long.

4.3 Specifications

4.3.1 Hardware specifications:

Components	Specifications
Microcontroller	Model: ESP32 Processor: 32-bit dual-core Clock Speed: Up to 240 MHz Memory: 520 KB SRAM Connectivity: Wi-Fi, Bluetooth GPIO Pins: 30, with multiple analog and digital inputs
Sensor/ RFID Reader	Model: RC522 Chip Operating frequency:13.56MHz Data transfer rate: maximum 10Mbit/s Module interface: SPI Cards supported: MIFARE
Display: LCD	Model: LCD2004 Protocol: I2C Default address:0*27, 0*3F
LEDs	Units:2 Colors: Red and Green
Power Supply	Voltage: 5V
Wires and additional elements	Material: Copper

Table 4-1 Components specifications

4.3.2 Software Specifications

Types	Elements
Firmware	• Programming language: C/C++ with Arduino IDE • Development environment: Visual Studio Code
Web Interface	• Backend framework: Django-Python • Frontend framework: HTML, CSS, JavaScript • Database: PostgresSQL • Hosting: Vercel • Media storing: Cloudinary
Data Handling	• Cloud-based PostgresSQL hosted on Aiven • Security: SSL/TLS/HTTPS as protocol

Tools and Platforms	• All Electronic circuits design: EasyEDA • Other designs: draw.io • Web hosting& deployment: Vercel • Media Management: Cloudinary • Database management: Aiven

Table 4-2 Software specifications

4.4 Cost Estimation

4.4.1 Hardware costs

Material	**Details**	**Quantity**	**Unit Price(RWf)**	**Total(RWf)**
Microcontroller	Type ESP32/30pins	1	15500	15500
Sensor	RFID Reader	1	6500	6500
	Cards	4	1000	4000
LEDS	-	2	200	400
Display	LCD2004- I2C	1	11500	11500
Power Supply	220VAC-12VDC	1	4000	4000
Enclosure, cables, connectors& accessories	-			20000
			Total	61900

Table 4-3 Hardware Costs

Note: *All the prices mentioned in table 3 and table 4 are the ones available on market. They can vary anytime. However, for future use the estimated cost will vary depending on numbers of examination rooms and other details to be ameliorated such as the design.*

4.4.2 Software Costs

Types	Elements	Prices
Firmware Tools	Arduino IDE	Free
	Visual Studio Code	Free
	PlatformIO	Free
Web development	Django Framework	Free
Hosting	Vercel for Web hosting	Free
	Cloudinary for Media Storage	Free

	Aiven for Database	Free
Design tools	Circuits design(EasyEDA)	Free
	Draw.io	Free

Table 4-4 Software costs

4.5 Implementation

In this section, we describe the step-by-step process of implementing the access control system for examination rooms. This includes the deployment of both hardware and software components, testing, and validation to ensure that the system functions as intended.

4.5.1 Hardware Deployment:

For hardware implementation, we used ARDUINO IDE as firmware and uploaded code to microcontroller. The circuit on Figure 6 shows connections to be made. The code uploaded (APPENDIX A) involves Wi-Fi configuration, Reads and detects new card present and exchanges with database through the Https protocol.

Connections:

ESP32 pins	Other Components
3.3V	VCC 3.3V RC522
GRD	GRD RC522, GRD LEDs, GRD LCD
4	RST RC522
5	SDA RC522
18	SCK RC522
19	MISO RC522
21	SDA LCD DISPLAY
22	SCL LCD DISPLAY
23	MOSI RC522
15	LED GREEN+
2	LED RED +
	LCD/5V---5V
	LCD/GRD ---GRD

Table 4-5 Connections

4.5.2 Software Deployment Process:

- ❖ **Database Configuration:** We have set up a database to store student information, access logs, and system configurations. Figure 11 shows its design.
- ❖ **Interface Design:** A website is deployed online on https://ulkcontrolservice.vercel.app for all users. We have developed user

interfaces for administrators to manage student data, monitor access logs, and configure system settings. The figures 8,9 and 10 illustrates the flow of responses depending on requests.

- **Integration of Real-Time Verification System:** We implemented the logic for real-time verification of student credentials. This includes checking RFID card data against the database and updating access logs (Figure 7).
- **Testing and Validation:** Conduct thorough testing to ensure that the system correctly identifies authorized and unauthorized access attempts. Validate that the messages displayed on the LCD screens are accurate and timely.

All the codes related to my project are available on this GitHub repository by following this link: https://github.com/BONHEUR243/control-service. And it’s public on my account.

4.6 Conclusion

In this chapter, i have detailed the design, analysis, and implementation process for the access control system for examination rooms. The calculations provided a clear understanding of the system's power requirements, network bandwidth, database capacity, response time, and backup power needs. The drawings, including system architecture diagrams, circuit diagrams, and flowcharts, visually represented the system's components and workflows.

I outlined the detailed specifications for both hardware and software components, ensuring that each part of the system is carefully selected and configured to meet the operational demands. The cost estimation provided a comprehensive analysis of the financial requirements, ensuring the project's feasibility and sustainability.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter provides a summary of the research findings, conclusions drawn from the study, and recommendations based on the research outcomes. Additionally, it offers suggestions for further study to enhance and expand upon the current research.

5.1 Conclusions

These conclusions address the research questions and objectives outlined in the study.

- ✓ The study successfully demonstrated the creation of a well-structured database to manage student information and access logs. The database was designed to ensure data integrity, security, and efficient retrieval of information. It incorporated tables for student details, RFID card information, and access logs, facilitating smooth data operations.
- ✓ User-friendly interfaces were designed and developed to enhance the usability and accessibility of the system. The web interfaces allowed administrators to manage student data, monitor access logs, and configure system settings efficiently. The intuitive design ensured that users with varying levels of technical expertise could interact with the system without difficulty.
- ✓ The integration of a real-time verification system was successfully achieved. The RFID-based verification system provided instant feedback on student access attempts, improving the security and efficiency of managing examination room access. The system's real-time response capability ensured that only authorized students could enter the examination rooms, thereby enhancing the reliability of the access control mechanism.

The study met its objectives of enhancing security, rapidity, efficiency, and reliability in managing student access to examination rooms. The implemented system demonstrated significant improvements over traditional access control methods done at ULK.

5.2 Recommendations

Based on the conclusions of this study, the following recommendations are made:

- ➢ **System Expansion:** Expand the system to cover all examination rooms and other critical areas within ULK. This will ensure a comprehensive access control mechanism throughout the campus.

- **Regular Updates and Maintenance:** Implement regular updates and maintenance schedules for both the hardware and software components of the system. This will ensure continued reliability and efficiency, as well as the incorporation of new security features. Example: Wi-Fi code on which the microcontroller is connected to.
- **Integration with Other Systems:** Consider integrating the access control system with other university systems, such as student information systems and campus security systems, to create a unified and more efficient security infrastructure. Example: add Visa control for international students or manage attendance of personnel at ULK.

5.3 Suggestions for further study

To build upon the findings of this research, the following areas are suggested for further study:

1. **Advanced Security Features:** Investigate the integration of advanced security features such as biometric authentication, facial recognition, or multi-factor authentication to further enhance the security of the access control system.
2. **User Feedback and Usability:** Explore the usability of the system from the perspective of both administrators and students. Gather feedback to identify areas for improvement in the user interface and overall system experience.

By addressing these areas, future research can continue to improve the effectiveness, reliability, and security of access control systems in educational institutions.

REFERENCES

Akpınar, S., & Hakan, K. (2010). *Computer aided school administration system using RFID technology.*

Alhelaly, S. (2023). Constructing a Smart School Based on the Internet of Things Using RFID Technology.

D, C., Kundu , T., & Kaur, P. (2012). The RFID technology and its applications: a review.

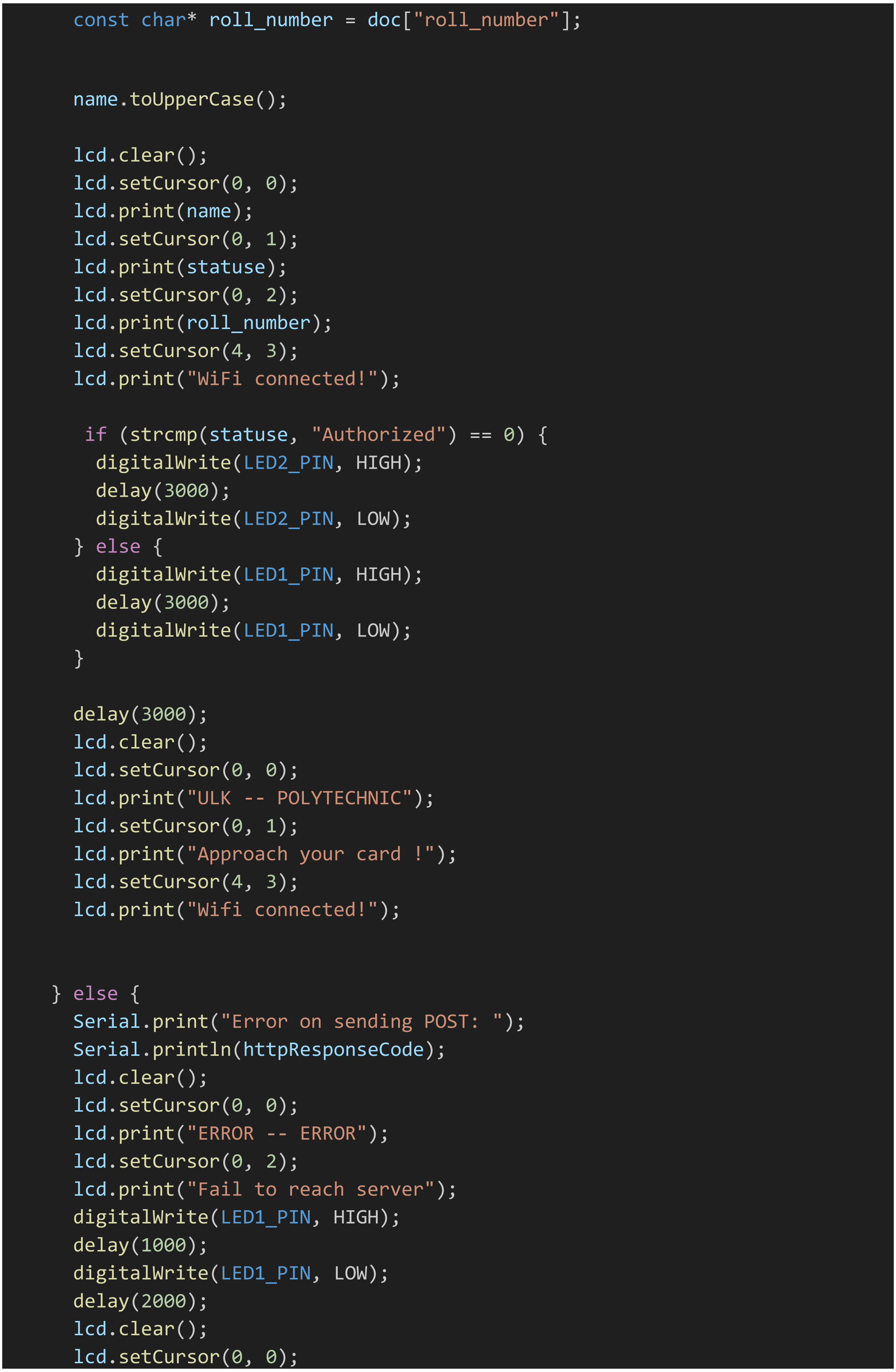
Mrabet, H. E., & Abdelaziz, A. M. (2020). *IoT-School Attendance System Using RFID Technology.*

Vandana, K., Kumar, K., Sivani, G., Devanand, G., & Venkatanarayana, E. (2018). Examination Room Guidance System Using RFID and Arduino. *International Research Journal of Engineering and Technology (IRJET).*

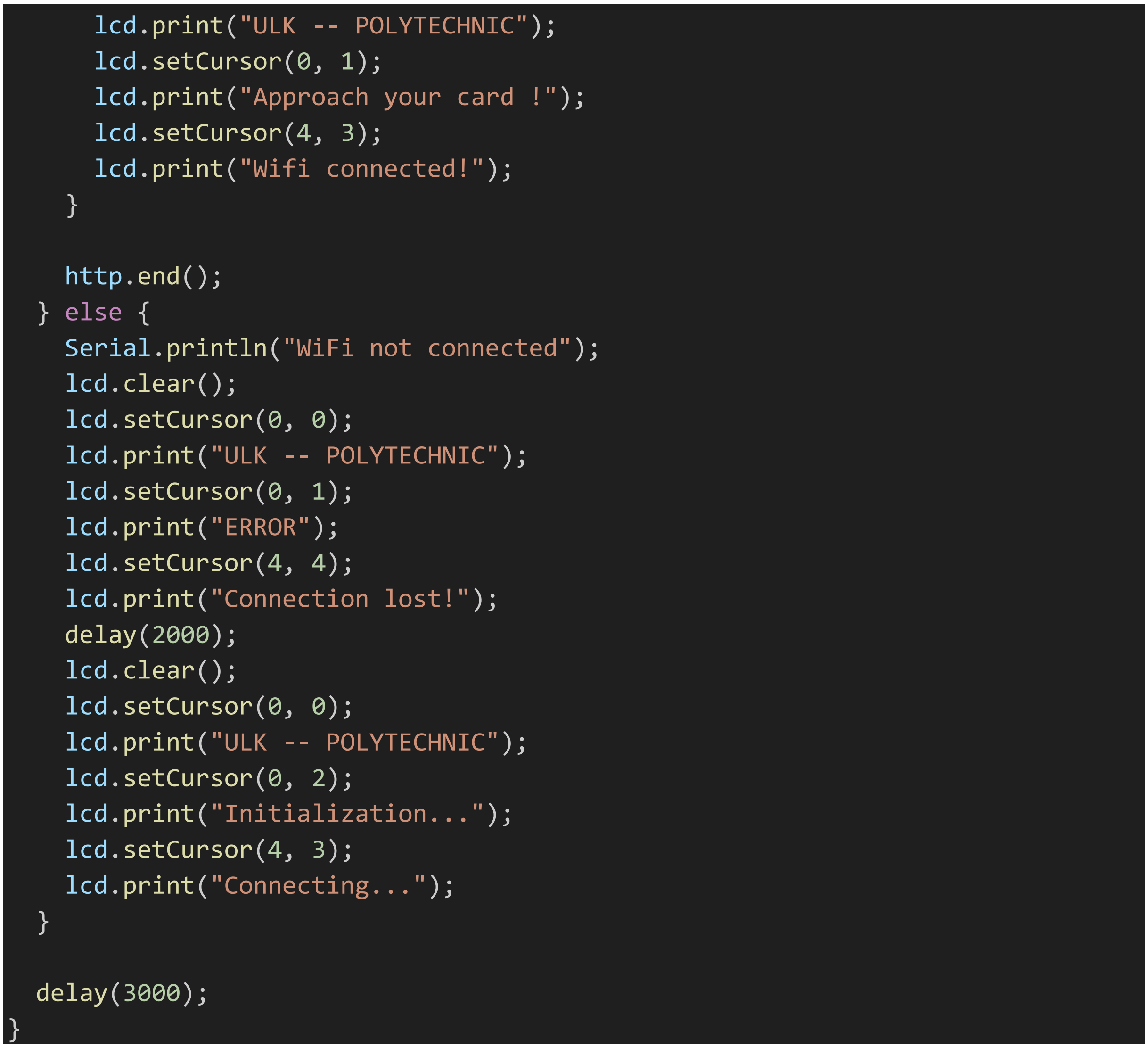
APPENDICES

APPENDIX A: SOFTWARE CODE UPLOADED

```
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <HTTPClient.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <ArduinoJson.h>
#include <MFRC522.h>

#define SS_PIN 5
#define RST_PIN 4
#define LED1_PIN 15 //red led
#define LED2_PIN 2 //green led

MFRC522 rfid(SS_PIN, RST_PIN);
LiquidCrystal_I2C lcd(0x27, 20, 4);
const char* serverName = "https://ulkcontrolservice.vercel.app/check_rfid/";


void setup() {
  Serial.begin(115200);
  SPI.begin();
  rfid.PCD_Init();
  lcd.init();
  lcd.backlight();

  //WiFi.begin("UPI", "poly#2023"); // to use at ULK
 WiFi.begin("CANALBOX-3013-2G", "QqBASw5Z35");
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
    lcd.setCursor(0, 0);
    lcd.print("ULK -- POLYTECHNIC");
    lcd.setCursor(0, 2);
    lcd.print("Initialization...");
    lcd.setCursor(4, 3);
    lcd.print("Connecting...");
  }
  Serial.println("Connected to WiFi");
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("ULK -- POLYTECHNIC");
  lcd.setCursor(0, 1);
  lcd.print("Approach your card !");
  lcd.setCursor(4, 3);
  lcd.print("WiFi connected!");
  pinMode(LED1_PIN, OUTPUT);
  pinMode(LED2_PIN, OUTPUT);
}

void loop() {
  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) {
    delay(50);
    return;
  }

  String cardId = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    cardId += String(rfid.uid.uidByte[i] < 0x10 ? "0" : "");
    cardId += String(rfid.uid.uidByte[i], HEX);
  }
  cardId.toUpperCase();

  Serial.println(cardId);

  if (WiFi.status() == WL_CONNECTED) {
    WiFiClientSecure client;
    HTTPClient http;
    client.setInsecure();  // Disable SSL certificate verification (not
recommended for production)
    // client.setFingerprint("xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx"); // Configuration to default…

    Serial.println("Sending HTTPS request...");

    http.begin(client, serverName);
    http.addHeader("Content-Type", "application/x-www-form-urlencoded");
    String postData = "cardId=" + cardId;

    int httpResponseCode = http.POST(postData);

    if (httpResponseCode > 0) {
      String response = http.getString();
      Serial.println(httpResponseCode);
      Serial.println(response);

      DynamicJsonDocument doc(1024);
      deserializeJson(doc, response);

      const char* statuse = doc["status"];
      const char* message = doc["message"];
      //const char* nom = doc["student_name"];
      String name = String(doc["student_name"]);
```



```
      const char* roll_number = doc["roll_number"];


      name.toUpperCase();

      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print(name);
      lcd.setCursor(0, 1);
      lcd.print(statuse);
      lcd.setCursor(0, 2);
      lcd.print(roll_number);
      lcd.setCursor(4, 3);
      lcd.print("WiFi connected!");

       if (strcmp(statuse, "Authorized") == 0) {
        digitalWrite(LED2_PIN, HIGH);
        delay(3000);
        digitalWrite(LED2_PIN, LOW);
      } else {
        digitalWrite(LED1_PIN, HIGH);
        delay(3000);
        digitalWrite(LED1_PIN, LOW);
      }

      delay(3000);
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("ULK -- POLYTECHNIC");
      lcd.setCursor(0, 1);
      lcd.print("Approach your card !");
      lcd.setCursor(4, 3);
      lcd.print("Wifi connected!");


    } else {
      Serial.print("Error on sending POST: ");
      Serial.println(httpResponseCode);
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("ERROR -- ERROR");
      lcd.setCursor(0, 2);
      lcd.print("Fail to reach server");
      digitalWrite(LED1_PIN, HIGH);
      delay(1000);
      digitalWrite(LED1_PIN, LOW);
      delay(2000);
      lcd.clear();
      lcd.setCursor(0, 0);
```



```
      lcd.print("ULK -- POLYTECHNIC");
      lcd.setCursor(0, 1);
      lcd.print("Approach your card !");
      lcd.setCursor(4, 3);
      lcd.print("Wifi connected!");
    }

    http.end();
  } else {
    Serial.println("WiFi not connected");
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("ULK -- POLYTECHNIC");
    lcd.setCursor(0, 1);
    lcd.print("ERROR");
    lcd.setCursor(4, 4);
    lcd.print("Connection lost!");
    delay(2000);
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("ULK -- POLYTECHNIC");
    lcd.setCursor(0, 2);
    lcd.print("Initialization...");
    lcd.setCursor(4, 3);
    lcd.print("Connecting...");
  }

  delay(3000);
}
```