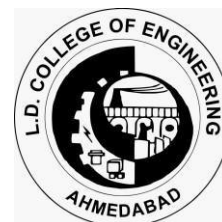


# GUJARAT TECHNOLOGICAL UNIVERSITY

University Area, Ahmedabad  
Affiliated



## L.D. College of Engineering



Project Report on

# KEYGUARD

Under subject of

DESIGN ENGINEERING – II B (3160001)

B. E. Semester – VI

Electronics and Communication Engineering

**Submitted By: Team ID 771039**

Sr.	Name of Student	Enroll. No.
1.	Aryan Chudasama	230283111005
2.	Manan Gohel	230283111008
3.	Meet Modi	230283111019
4.	Dhvanik Surti	230283111048

**Prof. (Dr.) Madhusmita C. Sahoo**  
Faculty guide

**Prof. (Dr.) C. H. Vithalani**  
Head of the Department

**Academic Year (2024 -2025)**  
**L. D. College of Engineering,**

Electronics and Communication Engineering

## CERTIFICATE

**Date: 11/4/2025**

This is to certify that the project entitled “KeyGuard” has been successfully carried out by

<b>Sr.</b>	<b>Name of Student</b>	<b>Enroll. No.</b>
1.	Aryan Chudasama	230283111005
2.	Manan Gohel	230283111008
3.	Meet Modi	230283111019
4.	Dhvanik Surti	230283111048

under my guidance in fulfilment of the Degree of Bachelor of Engineering in Electronics and Communication Engineering – 6<sup>th</sup> Semester of Gujarat Technological University, Ahmedabad during the academic year 2024-2025.

**Internal Guide**

Prof. (Dr.) Madhusmita C. Sahoo  
Electronics and Communication  
Engineering

**Head of Department**

Prof. (Dr.) C. H. Vithalani  
Electronics and Communication  
Engineering

## CANDIDATE'S DECLARATION

We have finished our project report entitled “KeyGuard” and submitted to our respective guide. We have done our work proficiently with utter preciseness and to the best of our knowledge.

First Candidate's Name : **Aryan Chudasama**  
Branch : **Electronics and Communication Engineering**  
Enroll No. : **230283111005**  
Signature :

Second Candidate's Name : **Manan Gohel**  
Branch : **Electronics and Communication Engineering**  
Enroll No. : **230283111008**  
Signature :

Third Candidate's Name : **Meet Modi**  
Branch : **Electronics and Communication Engineering**  
Enroll No. : **230283111019**  
Signature :

Fourth Candidate's Name : **Dhvanik Surti**  
Branch : **Electronics and Communication Engineering**  
Enroll No. : **230283111048**  
Signature :

Submitted to:

Prof. (Dr.) Madhusmita C. Sahoo  
L.D College of engineering, Ahmedabad

## ACKNOWLEDGEMENT

We would like to thank with respect all those who have provided us immense help and guidance during our project. We would like to thank our faculty guide **Prof. (Dr.) Madhusmita C. Sahoo** for providing vision about the system and for giving us an opportunity to undertake such a great challenging and innovative work. We are grateful for the guidance, encouragement, understanding, and insightful support given in the development process. We would like to extend our gratitude to **Prof. (Dr.) C. H. Vithalani**, Head of the EC Department, LD College of Engineering, Ahmedabad, for his continuous encouragement and motivation.

Last but not the least, we would like to mention here that we are greatly indebted to each and everybody who has been associated with our project at any stage but whose name does not find a place in this acknowledgement.

Yours sincerely,

Aryan Chudasama	(230283111005)
Manan Gohel	(230283111008)
Meet Modi	(230283111019)
Dhvanik Surti	(230283111048)

## ABSTRACT

The KeyGuard system is an innovative solution for secure key management, utilizing RFID technology to enhance accessibility and accountability. Aimed at efficient key control, the system employs RFID tags for cabinet access, displaying on the interface the keys assigned to an individual upon successful RFID authentication. Users can then select the desired keys, triggering a distinct LED blink & buzzer sound for identification.

The project involves a comprehensive approach to key security, seamlessly integrating user-friendly RFID interactions with a responsive display system. The system not only facilitates key retrieval but also ensures a transparent tracking mechanism, fostering a heightened sense of responsibility among users. The LED & buzzer auditory signalling provides a clear visual & auditory indicator, streamlining the process of key pick-up and return.

By amalgamating RFID technology, intuitive user interfaces, and dynamic feedback, the KeyGuard system not only enhances the efficiency of key management but also establishes a robust framework for monitoring and accountability. This abstract encapsulates the project's objectives, operational procedures, and the pivotal role of RFID in transforming conventional key management practices.

## TABLE OF CONTENTS

KeyGuard .....	i
Certificate .....	ii
Candidate's Declaration .....	iii
Acknowledgement .....	iv
Abstract.....	v
Chapter 1 .....	1
1.1 Introduction .....	1
1.2 Problem definition.....	2
1.3 Importance of domain .....	3
Chapter 2: AEIOU summary .....	5
Chapter 3: Mind Mapping .....	6
Chapter 4: Empathy Canvas .....	7
Chapter 5: Ideation Canvas .....	9
Chapter 6: Product Development Canvas .....	10
Chapter 7: LNM Canvas .....	11
Chapter 8: Prototype.....	13
8.1: Idealized Block Diagram.....	13
8.2: Current System Implementation .....	14
8.2.1: Hardware Implementation.....	14
8.2.2: Software-side Web UI.....	18
Chapter 9: Conclusion .....	22
Chapter 10: References .....	23

# CHAPTER 1

## 1.1 Introduction

This project presents the development of an innovative Keyguard system, leveraging RFID technology to revolutionize traditional key management processes. The system employs RFID tags for secure unlocking and locking of cabinets containing keys, ensuring a streamlined and efficient approach to key access.

The KeyGuard system enhances user experience by displaying a personalized key assignment interface upon RFID card authentication. Users are presented with a clear list of keys associated with their access credentials, empowering them to make informed selections. The system utilizes a dynamic display to showcase real-time key allocation, fostering transparency in the key management process.

In addition to the visual interface, the project incorporates a tactile feedback mechanism through LED indicators. Upon selecting keys, the corresponding LED lights blink, providing users with a tangible confirmation of their choices. This user-friendly feature enhances the overall accessibility and usability of the Keyguard system.

Furthermore, the system ensures accountability by logging key transactions. Each instance of unlocking or locking the cabinet is recorded, establishing a comprehensive audit trail. This not only promotes security but also facilitates monitoring and reporting for administrative purposes.

The KeyGuard system addresses the need for a sophisticated and intelligent key management solution, catering to diverse environments such as offices, facilities, and institutions. Its RFID-based authentication ensures a robust and secure access control mechanism, mitigating the risk of unauthorized key access.

In conclusion, this project introduces a cutting-edge RFID-Based Intelligent Key Management System that redefines conventional key management paradigms. With its user-centric interface, tactile feedback, and robust security features, the Keyguard system emerges as a pioneering solution for efficient and accountable key access in various organizational settings.

## **1.2 Problem definition**

The current key-based access control systems pose several challenges, including the risk of unauthorized access, the inconvenience of managing physical keys, and the inability to track entry and exit times accurately. The need for a more secure, user-friendly, and technologically advanced solution has led to the identification of the following key problems:

### **A. Security Concerns:**

- Traditional keys can be easily duplicated, leading to the risk of unauthorized access.
- Lost or stolen keys can compromise the security of the controlled environment.

### **B. Inconvenience and Management Issues:**

- Physical keys require manual handling and can be easily misplaced.
- Managing a large number of keys becomes cumbersome and may lead to organizational inefficiencies.

### **C. Lack of Access Tracking:**

- Traditional systems often lack the ability to accurately track entry and exit times.
- The absence of real-time monitoring makes it challenging to respond promptly to security incidents.

### **D. Need for Modernization:**

- In an era of technological advancements, there is a growing need to replace outdated access control systems with more sophisticated and reliable solutions.



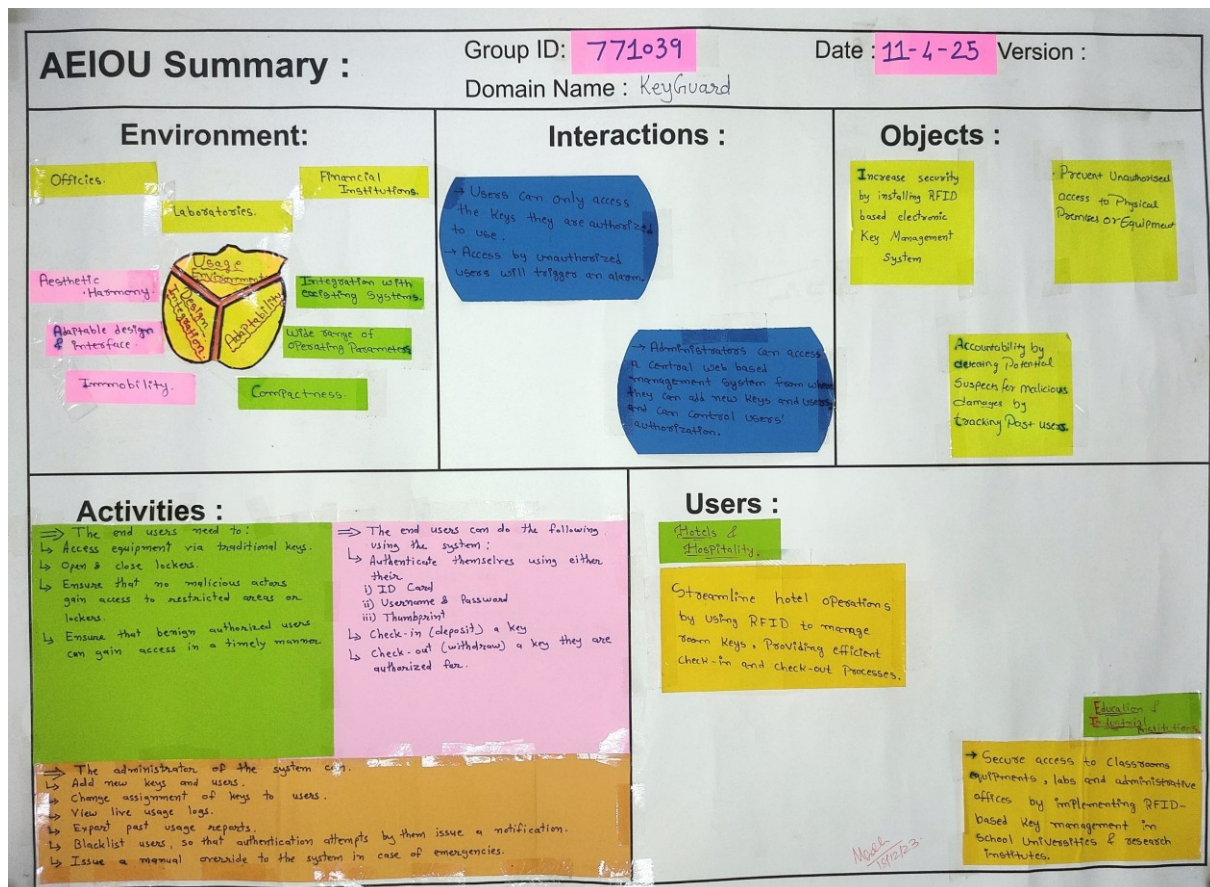
### **1.3 Importance of domain**

The domain of an RFID Key Guard System is crucial for various reasons, as it defines the context and environment in which the system operates. The importance of the domain lies in its impact on the design, implementation, and effectiveness of the RFID Key Guard System. Here are some key aspects of the importance of the domain:

- **Security Requirements:** Different domains have varying security needs. For example, the security requirements for a residential RFID Key Guard System may differ from those of a corporate office or a government facility. Understanding the specific security concerns within a given domain is crucial for tailoring the RFID Key Guard System to meet those requirements effectively.
- **User Interaction and Experience:** The user interaction and experience requirements can vary based on the domain. A system implemented in a commercial environment may need to accommodate a large number of users, whereas a residential system may prioritize simplicity and ease of use for homeowners. Understanding the user needs within the domain helps in designing an interface that is user-friendly and meets the expectations of the users.
- **Integration with Existing Infrastructure:** The domain influences the existing infrastructure and technology landscape. The RFID Key Guard System needs to integrate seamlessly with the current access control systems and technologies present in the domain. Understanding the infrastructure helps in avoiding conflicts, ensuring compatibility, and facilitating a smoother transition to the new system.
- **Compliance and Regulations:** Different domains are subject to specific regulations and compliance standards related to security and privacy. Adhering to these regulations is critical to the success and acceptance of the RFID Key Guard System. Understanding the legal and regulatory environment within the domain ensures that the system is designed and implemented in compliance with applicable laws.
- **Scale and Volume:** The scale and volume of the deployment may vary based on the domain. For instance, an industrial setting may require a system that can handle a large number of access points and users simultaneously. Understanding the scale and volume requirements within the domain is essential for designing a system that is scalable and can handle the anticipated load.

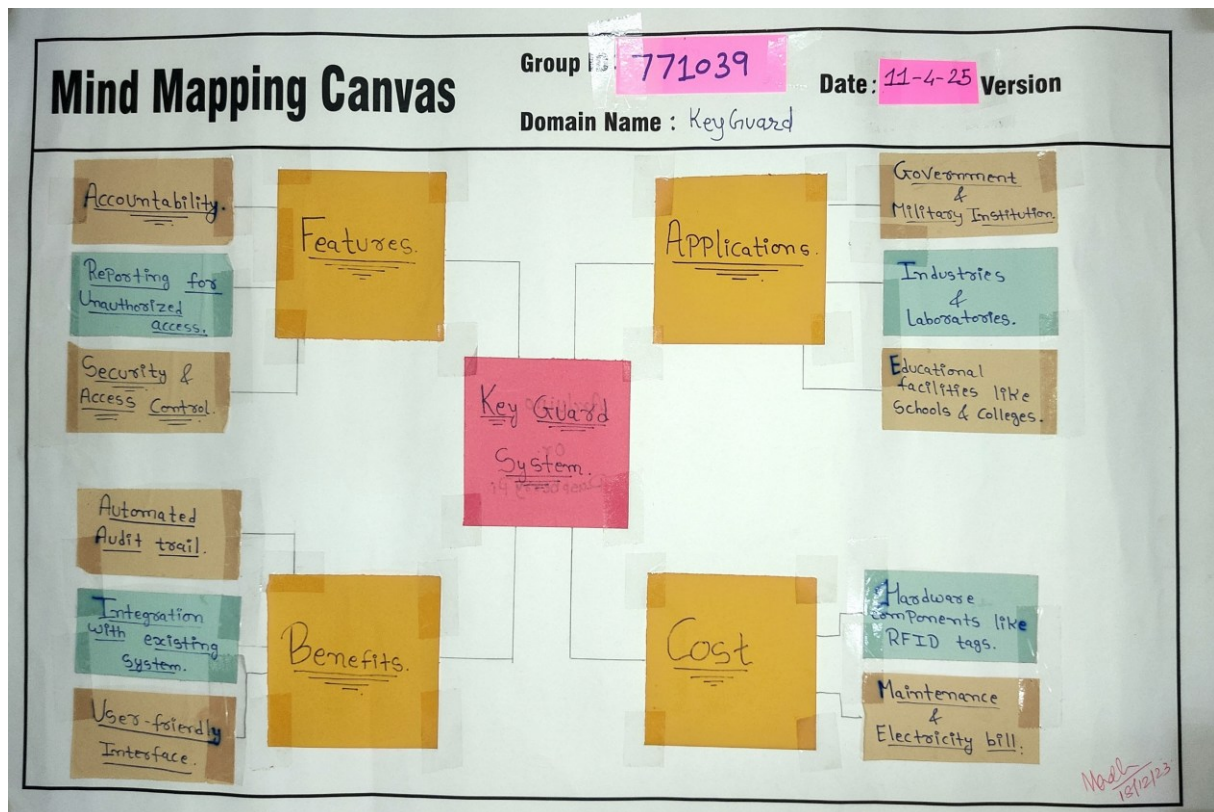
- **Risk Assessment and Mitigation:** Each domain comes with its own set of potential risks and threats. Conducting a thorough risk assessment within the specific domain helps in identifying potential vulnerabilities and developing mitigation strategies. The RFID Key Guard System can then be tailored to address the specific risks relevant to the domain.
- **Customization and Adaptability:** The domain influences the need for customization and adaptability of the RFID Key Guard System. A system designed for a specific domain should be flexible enough to accommodate changes in requirements and technologies within that domain over time.

## CHAPTER 2: AEIOU SUMMARY



- **A - Activities:** Identify key activities that the users need to perform such as RFID scanning, user authentication, access control.
- **E - Environment:** Consider the physical and digital environment where the RFID key guard will be implemented, including potential security threats
- **I - Interactions:** Define user interactions with the RFID key guard, ensuring a seamless and secure experience.
- **O - Objects:** List key objects involved, like RFID tags, authentication mechanisms, and the physical guard structure.
- **U - Users:** Identify user roles and their responsibilities in using the RFID key guard, emphasizing security protocols.

## CHAPTER 3: MIND MAPPING



The Mind Map Canvas specifies the Features, Benefits, Applications & Costs/ Downsides of our system. Mind mapping is to present all these topics or points in the form of diagram, drawing or any other form. Through this mind mapping canvas our intention will be clear about our topic and what we must do further. Mind mapping canvas is for easy understanding of the domain.



## CHAPTER 4: EMPATHY CANVAS

Design For : Design Engineering      Design By : 771039

Date : 11-4-25      Version

USER	STAKEHOLDERS
Laboratory Scientist. Hotel and Hostel residents. Hotel management staffs.	Head of Security. Industries' Stakeholders. Administrative staff.

**ACTIVITIES**

Access Equipments

Open & Close lockers.

Central management of Key access.

Generate Usage logs.

Check-In & Check-Out Keys.

**STORY BOARDING**

**HAPPY :** Mr. Jainam Agrawal, an Executive at the Physics Research Organisation, recently bought our system to combat unauthorized and unscheduled accesses to restricted areas/equipment and damage to sensitive assets by unknown personnel. He has reported great satisfaction with our system in preventing these malpractices.

**HAPPY :** Mrs. Jainam Chaudhary, Head of the Finance Department at RD Institute, has reported not only an increase in safety, but also a decrease in security costs, since security officers previously required for the manual management of keys could be reassigned elsewhere.

**SAD :** Mr. Chatur Chand, an Intern at Scientific Product Creation industries, has reported dissatisfaction with our product, since he feels that his freedom is being restricted. He says, "This process of dispensing keys is highly restrictive and time consuming."

**SAD :** Mr. Bahadur Singh, a former security guard, has reported a resentment with our product. 'Earlier, I had a good job managing assignment of keys, but with the introduction of keyguard, I have lost my job, since I was not longer needed for that task.' He says.

Modul  
EP12/23

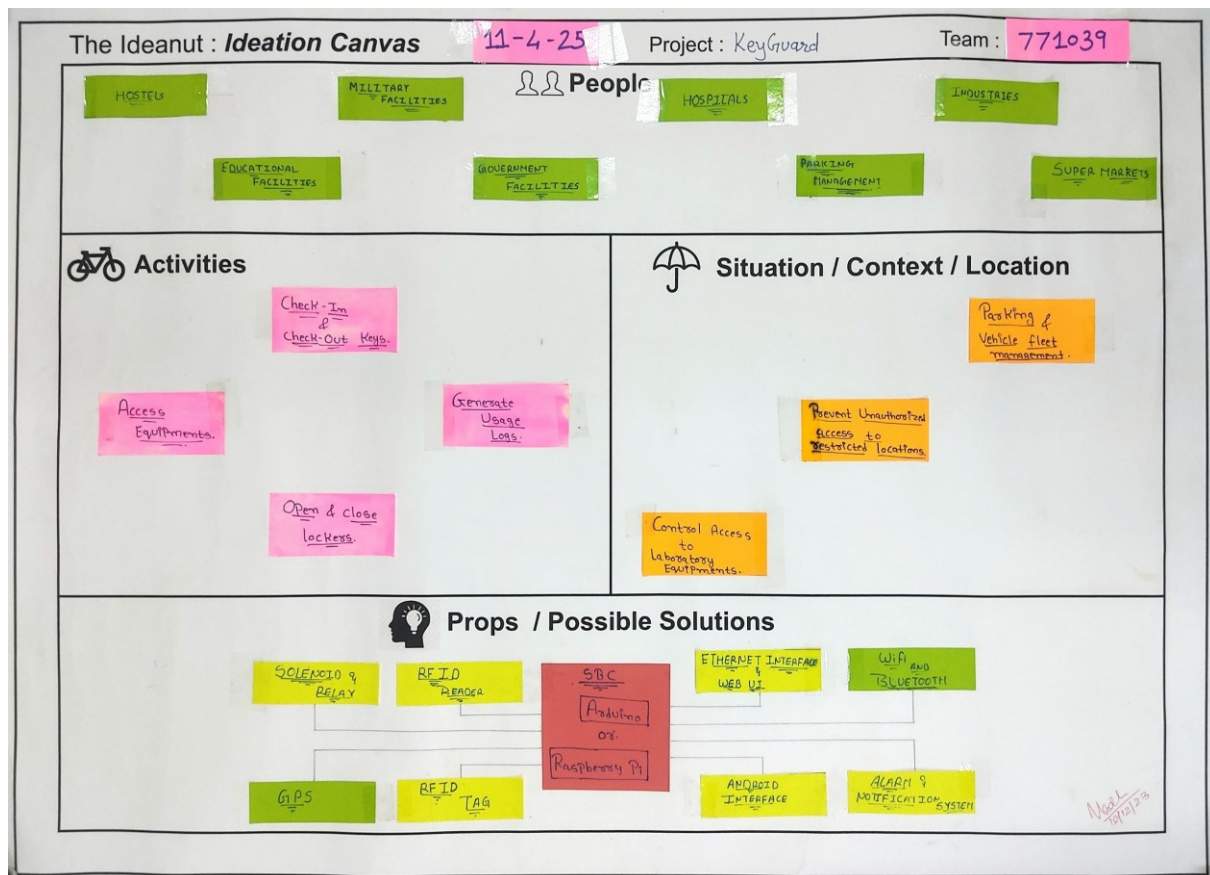
**HAPPY:** Mr. Jainam Agrwal, an Executive at the Physics Research Organisation, recently bought our system to combat unauthorized and unscheduled access to restricted areas/equipment and damage to sensitive assets by unknown personnel. He has reported great satisfaction with our system in preventing the malpractices

**HAPPY:** Mrs. Jasmin Chawda, Head of the Finance Department at RD Institute, has reported not only increase in safety but also a decrease in security costs, since security officers previously required for the manual management of keys could be reassigned elsewhere.

**SAD:** Mr Chatur Chand, an Intern at Scientific Product Creation Industries, has reported dissatisfaction with our product since he feels that his freedoms are being restricted. He says, "This process of dispensing keys is highly restrictive and time consuming."

**SAD:** Mr. Bahadur Singh, a former security guard, has reported a resentment with our product. "Earlier I had a good job managing the assignment of keys, but with the introduction of KeyGuard, I have lost my job, since I was no longer needed for that task" he says.

## CHAPTER 5: IDEATION CANVAS



**People:** Hostels, Education facilities, Military facilities, Government facilities, Hospitals, Parking management, Industries, Super market.

**Activities:** Check in & Check out keys, access equipment, generating usage logs, open & close lockers.

**Situation:** Parking & vehicle fleet management, prevent unauthorized access to restricted location , control access to laboratory equipment.

**Possible Solutions:** Solenoid & Relay, RFID reader, GPS, RFID tags, Ethernet interface & web UI, WIFI and Bluetooth, android interface, alarm & notification system.



# CHAPTER 6: PRODUCT DEVELOPMENT CANVAS

Group ID: 771039 Domain Name: KeyGuard Date: 11-4-2025

## Product Development Canvas

### ① Purpose

What is the purpose of this concept you're developing?  
Does it solve a problem, or it enhances a certain experience?  
Is it serving a need or it is trying to create a new need or tap an untapped need?

INCREASE SECURITY

PREVENT UNAUTHORIZED ACCESS

IDENTIFICATION of FREE SLOTS

ACCOUNTABILITY by KEY TRACKING

### ⚓ Product Experience

Define what your customer should feel like when he uses your product / service? Emotions, feelings would define his experience? feeling Convenience, or feeling of buying more with less (cost conscious) or feeling of greater security, safety etc.

INCREASE SAFETY

TIME SAVING

EASE of USE

### ☑ Customer Revalidation

Once you're finished with your feature set, test with the customer / user if the features, functions are useful. Speak to the customer / user.

① Initial Implementation  
Issue: Only 1 key slot; too limited

② Second Implementation  
Issue: Only provides a CLI; too unattractive

③ Current Implementation  
Issue: Adding users & keys into the database is tedious.

### ⊗ Product Functions

Functions are a products answer to user problems / need. They do something that user wants. They are often verbs in nature. Every function is powered by many features. Multitasking is a function. Browser tabs is a feature that powers the multitasking feature. A function can have one or more features powering it. Functions are very generic in nature, features are often more specific. Functions can be similar to product experience. Safety (product function) provides a feeling of safety (product experience)

SMART LOCKING & UNLOCKING

AUDIT TRAIL of ACCESSSES

ALARMS for UNAUTHORIZED ACCESSSES

### ⊕ Product Features

Product feature are specific. One or more features will power a function. Antilock Brakes, Airbags are feature that power the safety function. Browser tabs, Apple's home button to multitask between apps are features powering the multitasking function. Each feature will have many components/sub-components powering it. Sometimes a very popular component becomes a feature in itself. Like car stereo is a major components and a feature at the same time powering the in car entertainment function powering entertainment as a product experience.

→ Increase security by installing RFID based electronic Key Management System

→ Accountability by detecting potential suspects for malicious damages by tracking Past Users.

→ Prevent Unauthorized access to Physical - Premises or Equipment.

### 🧑 People

Who is the key customer segment who will use this product / service or the end product of the concept you're pursuing?  
Write here about them, describe them a little.

HOTELS

INDUSTRIES

BANKS

STORAGE LOCKERS

LABORATORIES

OFFICES

### ⚙ Components

Components build up the features. For a starting it will comprise a list of component like bags, triggers etc. that go into making it. For a tabbed browser it will comprise of various chunks of code that will make the tabs work. In cases where the feature is a major component, you could list here the auxiliary components that are required to make the major component work. You can also list new adjustments and innovations you're planning here at the component level.

RFID Reader

RFID Tag

Solenoid & Relay

Arduino or Raspberry Pi

Ethernet Interface & Web UI

Android Interface

Alarm & Notification System

### 🧪 Reject, Redesign, Retain

Post customer validation, reject those function or feature that the customers didn't find useful. Redesign those that were partially useful and retain those that met the bar. Iterate with this until all functions / features are accepted.

② Redesign - Add extra key slots

② Redesign - Add a web UI

③ Currently Retain Redesign in Future Scope. Add an administrative dashboard.

Mod 101023

**Purpose:** increase security, prevent unauthorised access, identification of free slots, accountability by key trekking.

**People:** Hotels, industries, Banks, Storage lockers, Laboratories, offices.

**Product Experience:** Increase safety, time saving and ease of usage.

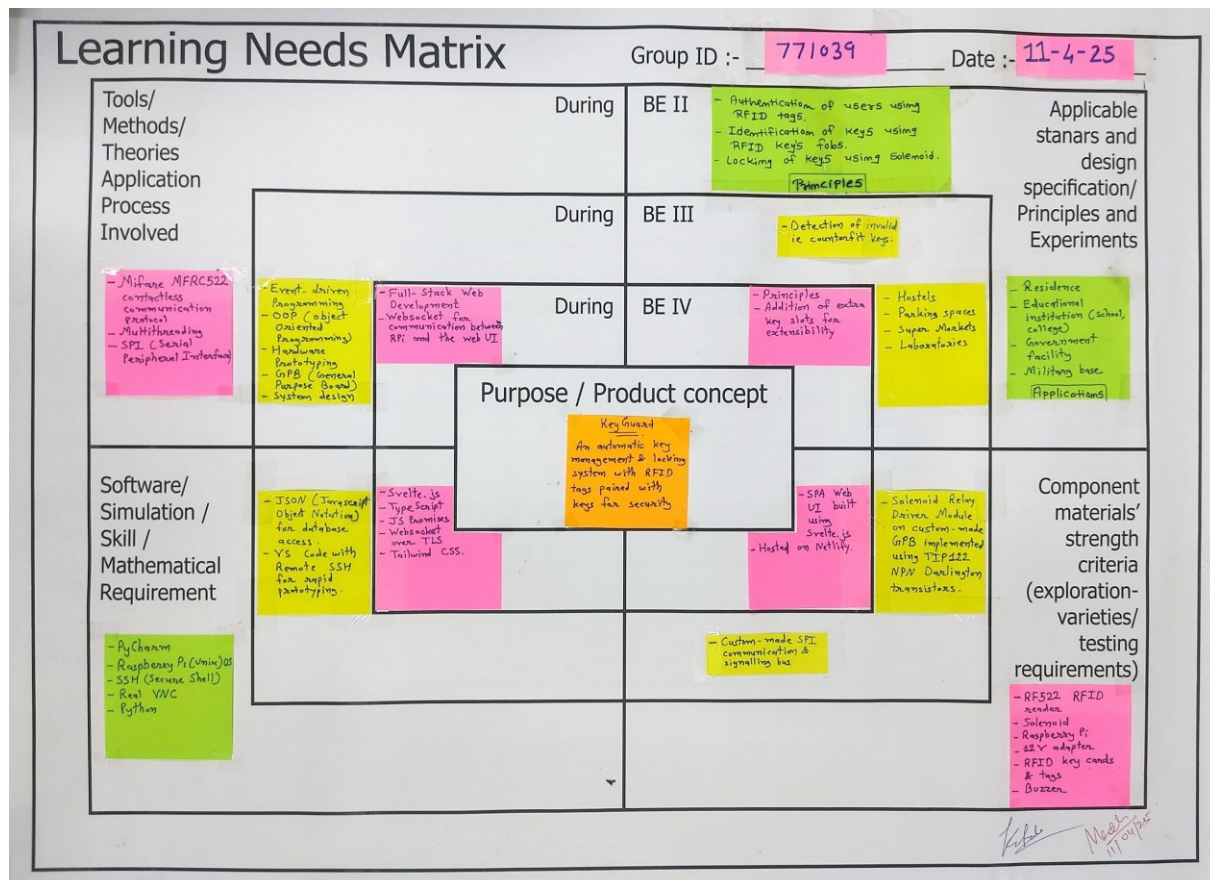
**Product Functions:** smart locking and unlocking, audit trail and accesses, alarms for unauthorised access.

**Product Features:** increase security by installing RFID based electronic key management system, accountability by detecting potential suspects for malicious damage by trekking past users, prevent unauthorised access to physical-premises or equipment.

**Components:** Solenoid & relay, RFID reader, GPS, RFID tags, Ethernet interface & Web UI, WIFI and Bluetooth, Android Interface, Alarm & Notification System, Raspberry PI.



## CHAPTER 7: LNM CANVAS



The LNM (Learning Needs Model) Canvas helps identify the learning requirements of the system being designed.

### Applications:

- Residences, Educational Institutions (Schools & Colleges), Government facilities, Military bases
- Hostels, Parking Spaces, Super Markets, Laboratories

### Principles:

- Authentication of users using RFID tags.
- Identification of keys using RFID tags.
- Locking of keys using solenoid.
- Detection of invalid i.e. counterfeit keys.
- Addition of an extra key slot for extensibility.

### Components:

- RF522 RFID reader, Solenoid, Raspberry Pi, 12V Adapter, RFID cards & tags, Buzzer;

- Solenoid Relay Driver Module on custom GPB (General Purpose Board), Custom made SPI communication bus.
- SPA Web UI built using Svelte.js hosted on Netlify

**Software:**

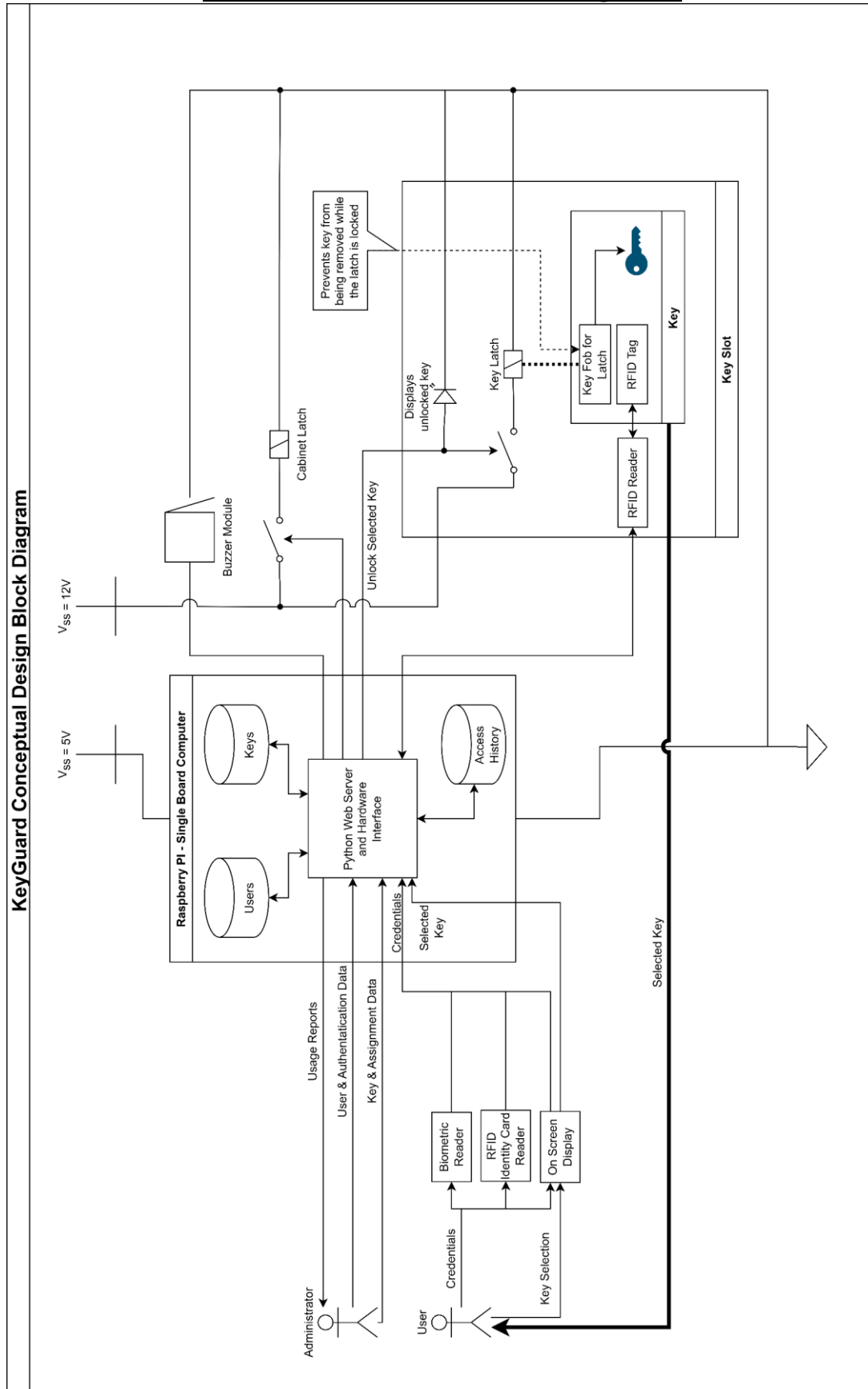
- Raspberry Pi (Unix) OS, Python, PyCharm, SSH (Secure Shell), RealVNC
- JSON (JavaScript Object Notation) for Database access, VS Code with Remote-SSH
- Svelte.js, TypeScript, JS Promises, WebSockets over TLS, Tailwind CSS

**Tools:**

- SPI (Serial Peripheral Interface), Mifare MRFC522 contactless communication protocol, Multithreading
- Event-driven programming, OOP, Hardware Prototyping & System Design, GPB
- Full-Stack Web Development
- WebSocket for communication between the Raspberry Pi and the Web UI.

## CHAPTER 8: PROTOTYPE

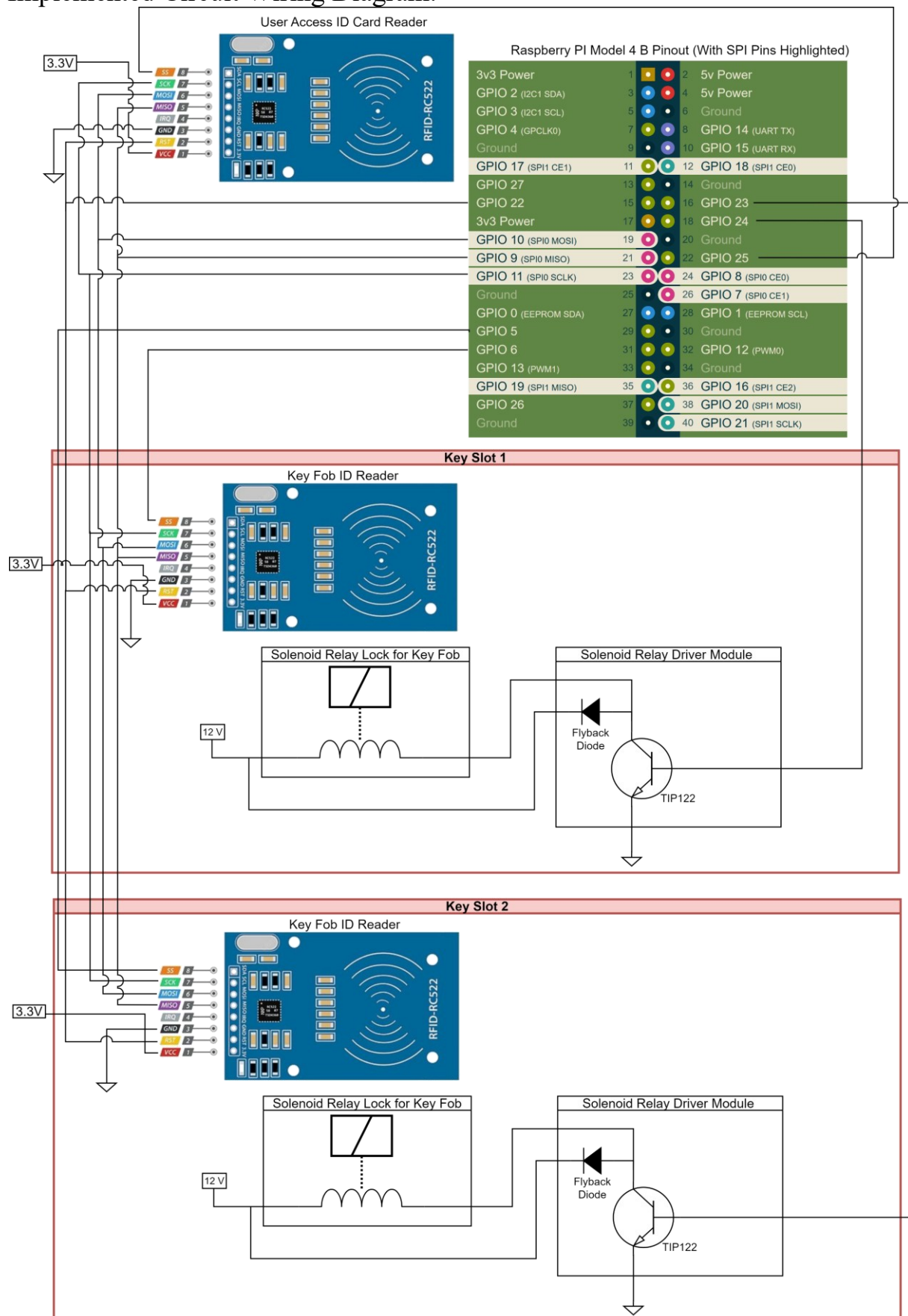
### 8.1: Idealized Block Diagram



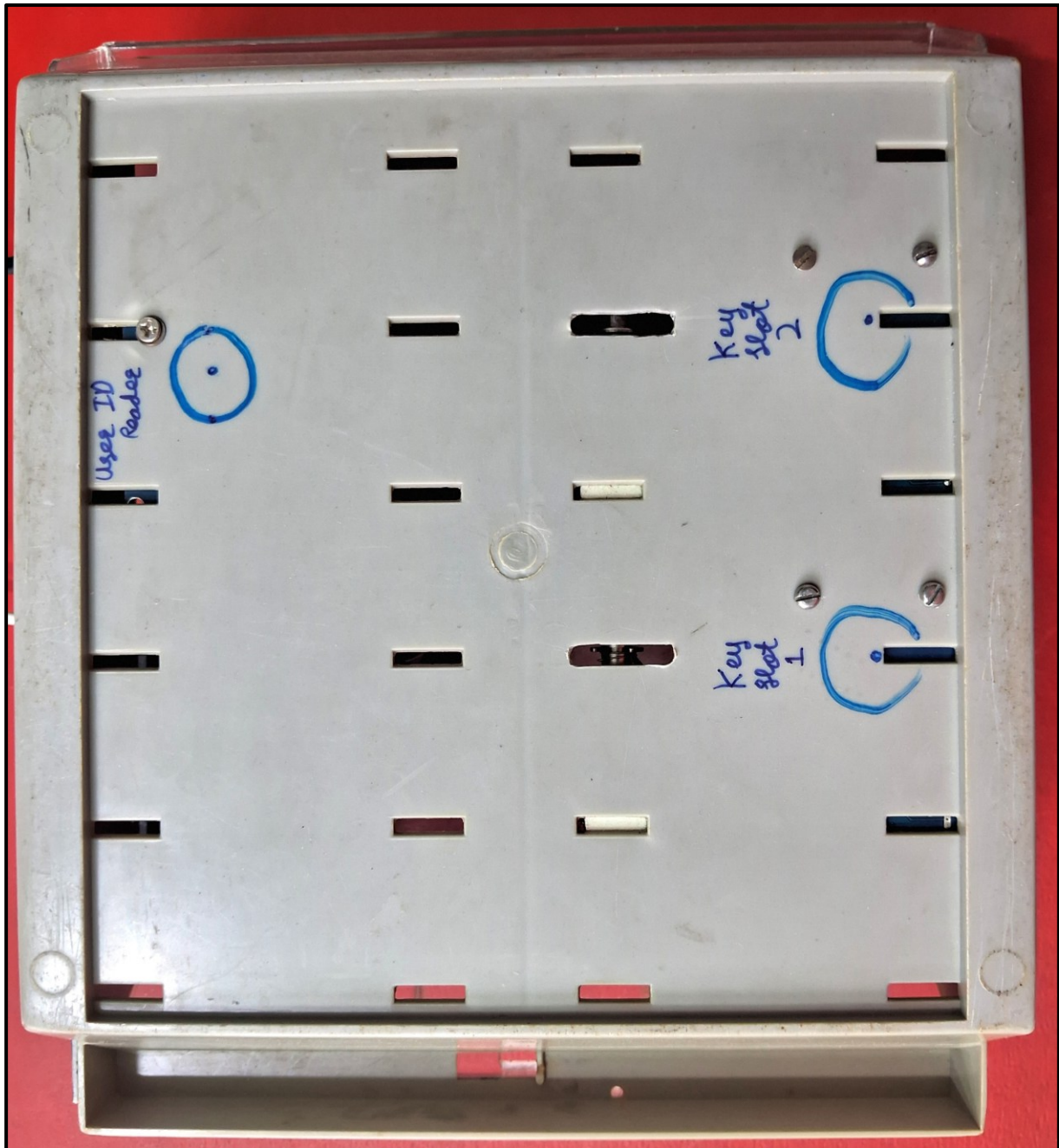
## 8.2: Current System Implementation

### 8.2.1: Hardware Implementation

Implemented Circuit Wiring Diagram:

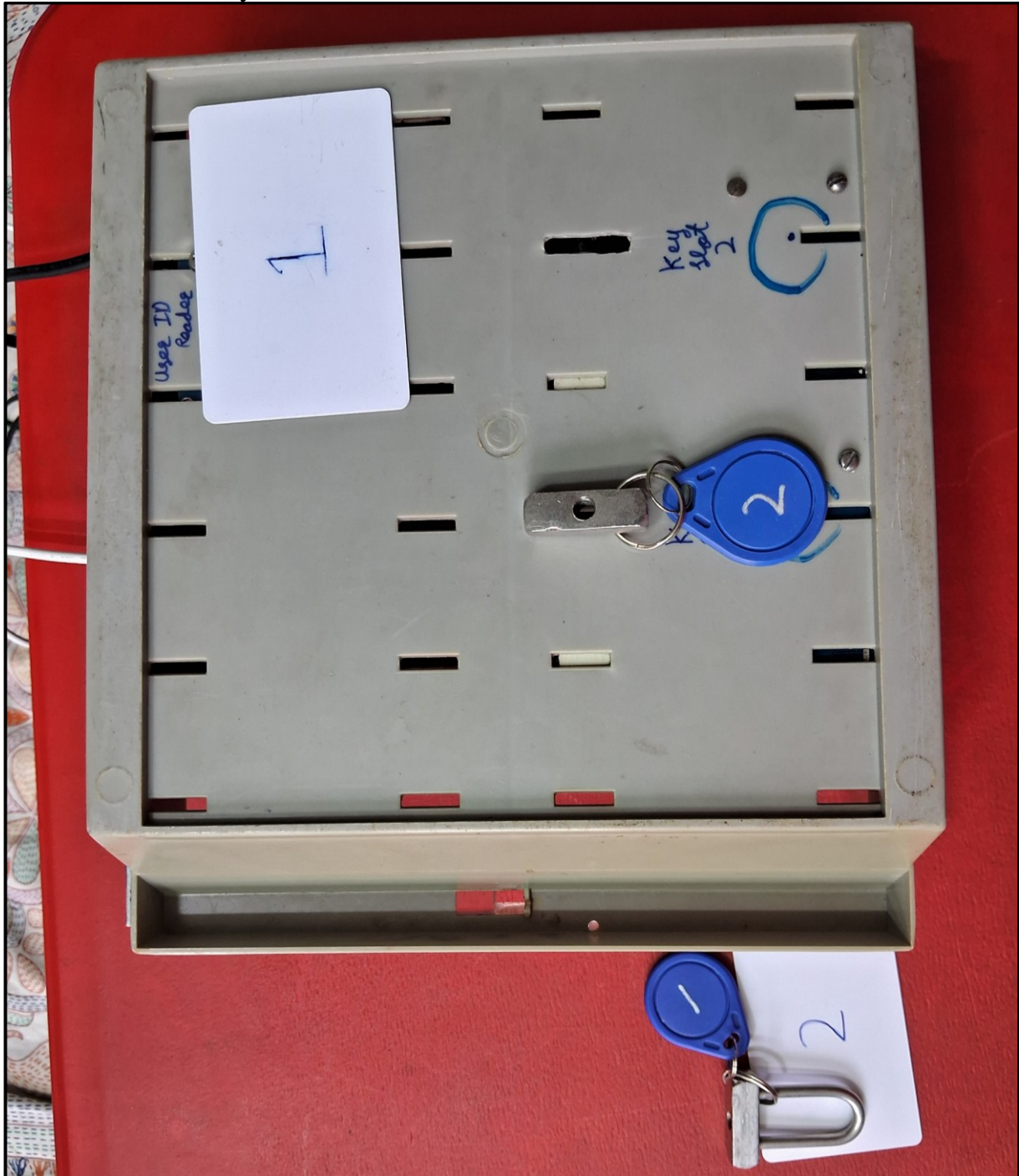


Front view: Visible to end users:

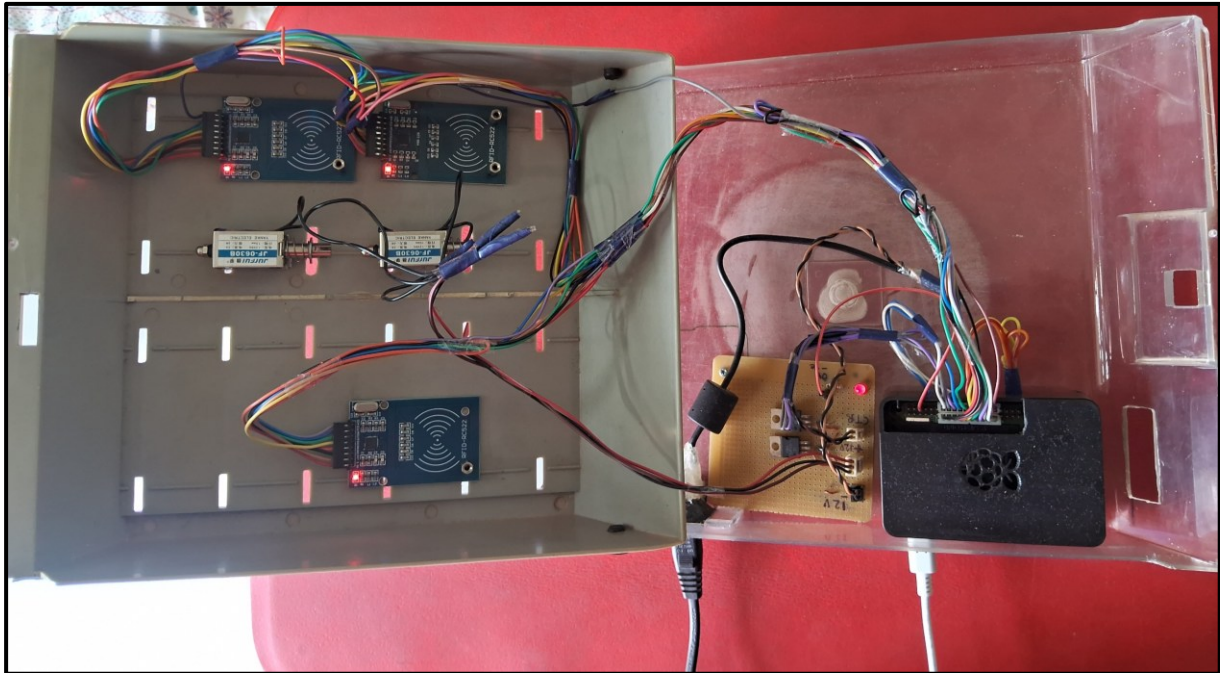




Front view with key inserted and location of user ID card reader shown:



Internal view:

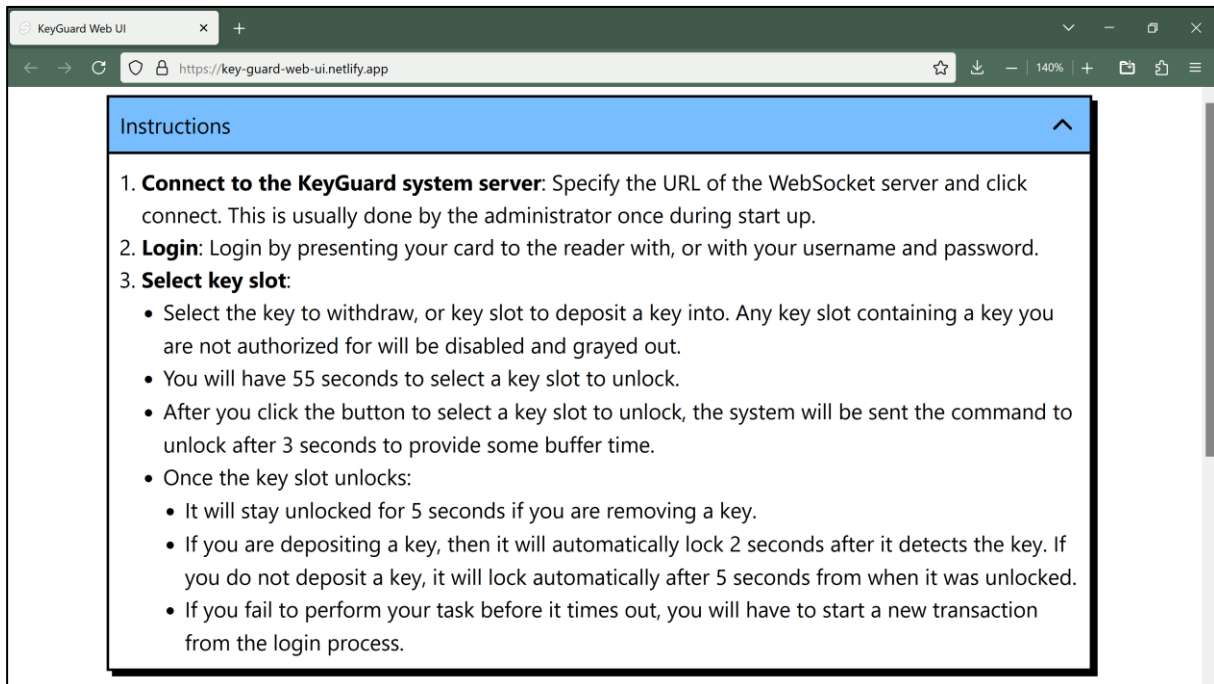


#### **Hardware details:**

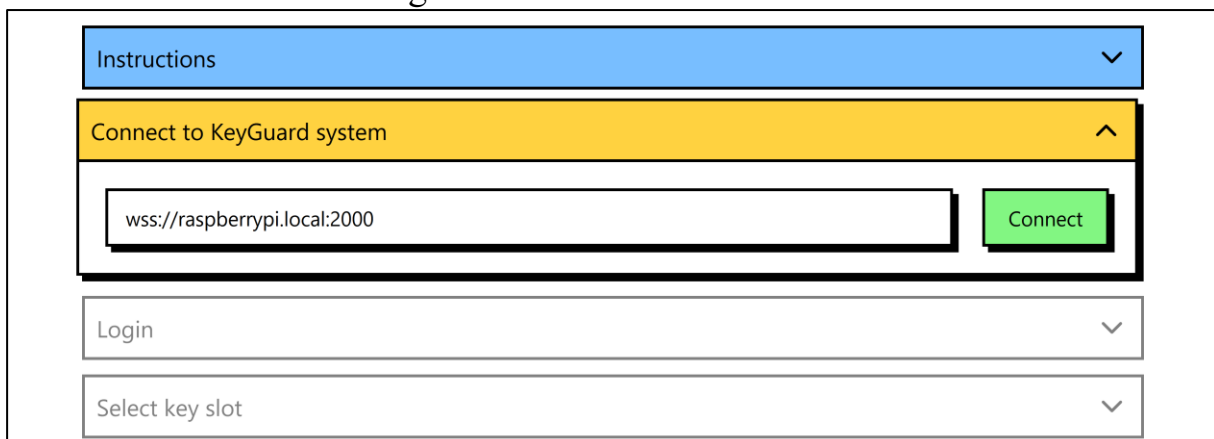
- The currently implemented prototype runs on a Raspberry Pi system.
- It has 2 key slots, each with
  - 1 solenoid to latch the key into the slot.
  - 1 RFID reader to identify the key placed in the slot.
- It also has a RFID reader for the user authentication module.
- The RFID readers are connected to the system via a shared SPI bus.
- The key identification module supports 2 keys:
  - Key 1: Key to Lab Alpha
  - Key 2: Key to Device Beta
- The user authentication module's database currently contains 2 authorized users:
  - User 1: Can access Key to Lab Alpha and Key to Device Beta
  - User 2: Can only access Key to Lab Alpha.
- Any unrecognized keys and user ID cards are rejected.
- The Python WebSocket server is implemented using the websockets PyPi package.

## 8.2.2: Software-side Web UI

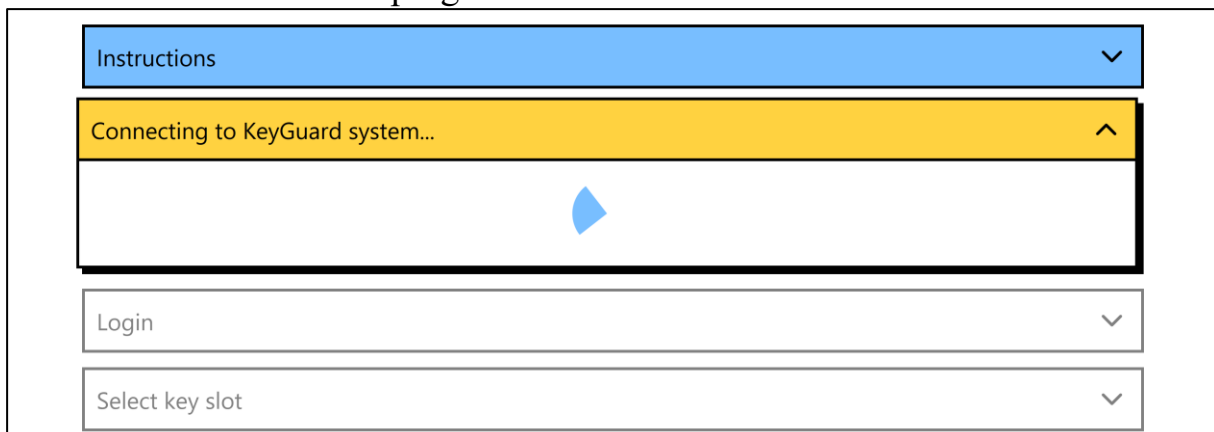
### Instructions:



### WebSocket Connection stage:

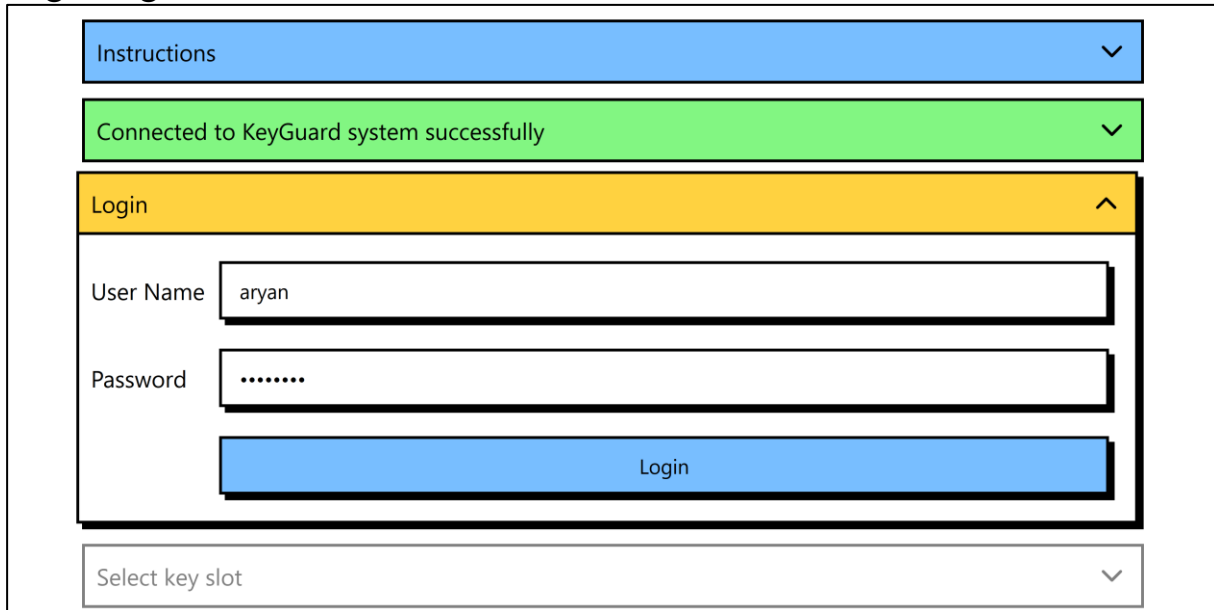


### Connection handshake in progress:



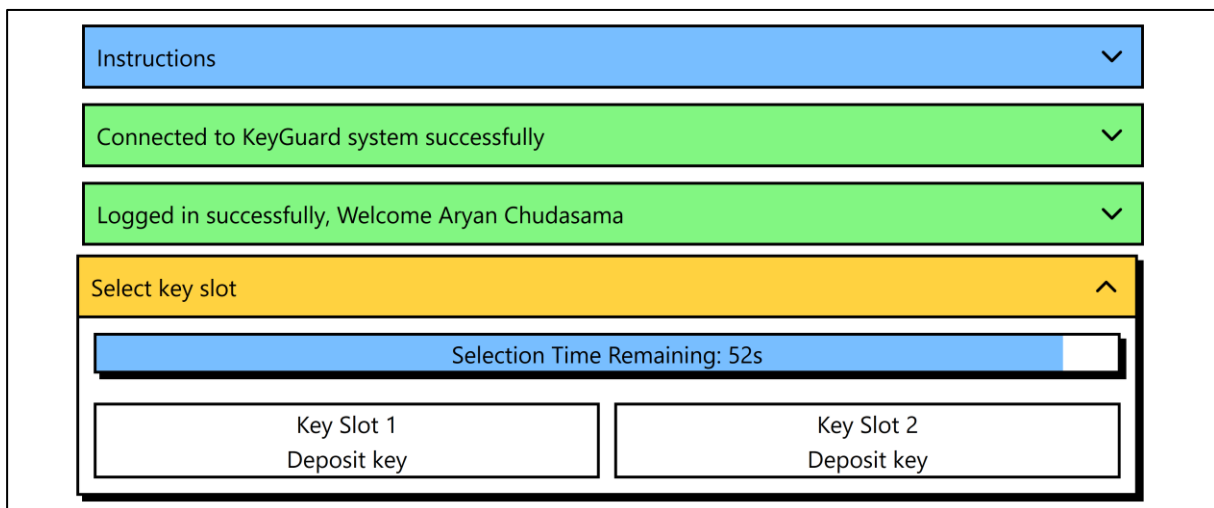


## Login Page:



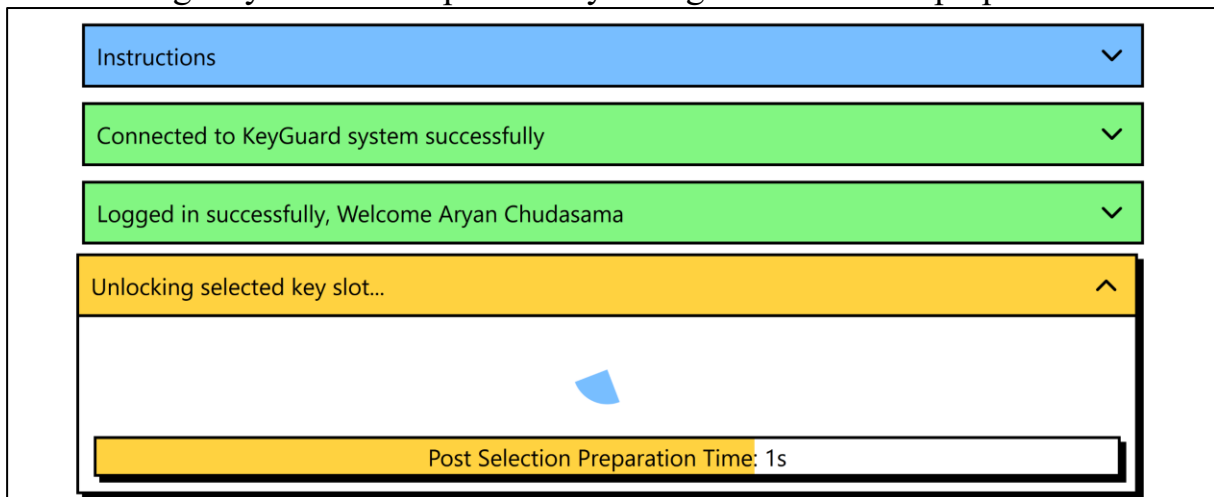
The screenshot shows the login interface. At the top, there is a blue bar labeled 'Instructions' with a downward arrow. Below it is a green bar with the message 'Connected to KeyGuard system successfully' and a downward arrow. The main section is a yellow bar labeled 'Login' with an upward arrow. Inside this section, there are two input fields: 'User Name' with the text 'aryan' and 'Password' with masked characters '.....'. Below these fields is a blue 'Login' button. At the bottom of the page, there is a white bar labeled 'Select key slot' with a downward arrow.

After logging in using the username & password or the user ID card of User 1:



The screenshot shows the system after successful login. The top three bars (Instructions, Connected to KeyGuard system successfully, and Logged in successfully, Welcome Aryan Chudasama) are the same as in the login page. The main section is now a yellow bar labeled 'Select key slot' with an upward arrow. Below this bar is a blue bar with the text 'Selection Time Remaining: 52s'. At the bottom, there are two white boxes: 'Key Slot 1 Deposit key' and 'Key Slot 2 Deposit key'.

On selecting Key Slot 1 to deposit a key: We get 3 seconds to prepare ourselves.



The screenshot shows the system during key preparation. The top three bars (Instructions, Connected to KeyGuard system successfully, and Logged in successfully, Welcome Aryan Chudasama) are the same. The main section is a yellow bar labeled 'Unlocking selected key slot...' with an upward arrow. Below this bar is a large white area with a blue circular arrow icon. At the bottom, there is a yellow bar with the text 'Post Selection Preparation Time: 1s'.

Then the key slot unlocks:

The screenshot shows a software interface with a list of messages on the left and a main display area on the right. The messages are: 'Instructions' (blue bar), 'Connected to KeyGuard system successfully' (green bar), 'Logged in successfully, Welcome Aryan Chudasama' (green bar), and 'Unlocking selected key slot...' (yellow bar). The main display area shows a blue circular progress indicator and a blue progress bar at the bottom labeled 'Auto-Relock Timeout: 4s'.

After depositing the key:

The screenshot shows the same interface as before, but with the 'Login' message (yellow bar) instead of 'Unlocking selected key slot...'. The main display area now contains input fields for 'User Name' and 'Password', and a blue 'Login' button. Below these fields is a dropdown menu labeled 'Select key slot'. At the bottom right, a green notification box states: 'Key slot transaction successfully completed. To perform another transaction please login again.'

Then, after logging in we can see that we now have the option to withdraw the key, right now we will deposit the other key.

The screenshot shows the interface with the 'Select key slot' message (yellow bar). The main display area shows a blue progress bar labeled 'Selection Time Remaining: 47s'. Below the progress bar are two buttons: 'Key Slot 1 Withdraw Key to Lab Alpha' and 'Key Slot 2 Deposit key'.

Then after logging in again we see that User 1 has the option to withdraw either key:

Instructions

Connected to KeyGuard system successfully

Logged in successfully, Welcome Aryan Chudasama

Select key slot

Selection Time Remaining: 52s

Key Slot 1  
Withdraw Key to Lab Alpha

Key Slot 2  
Withdraw Key to Device Beta

However, User 2 is forbidden from accessing the Key to Device Beta:

Instructions

Connected to KeyGuard system successfully

Logged in successfully, Welcome Astha Chudasama

Select key slot

Selection Time Remaining: 53s

Key Slot 1  
Withdraw Key to Lab Alpha

Key Slot 2  
ACCESS DENIED

To withdraw any key simply click on the button and proceed similarly to the key check-in process.

### **Software details:**

- The Web UI is developed using the Svelte.js 5 & SvelteKit framework(s).
- The codebase is in TypeScript to provide static typing during bundling time.
- The component styling is implemented using Tailwind CSS in conjunction with Svelte's scoped CSS styles (on top on PostCSS).
- It uses WebSockets to communicate with the RPi server.
  - The websocket-as-promised library is used as a wrapper over the native JS WebSocket class to provide a support for fluent asynchronous code using Promises and the async/await syntax.

## CHAPTER 9: CONCLUSION

The KeyGuard project has showcased the versatility and efficacy of hardware key management systems (KMSes). It is useful across various domains. From schools to factories, the project has demonstrated the potential to revolutionize industries & institutes and enhance efficiency. The successful integration of automatic authentication features and seamless access to assigned keys signifies a promising future for the KeyGuard key management system technology.

### **Future Scope:**

1. GUI based administrator panel for addition of users & keys.
2. Notification system to inform the administrator when a noteworthy event occurs like when a key is stolen.
3. Addition of more key identification modules, and correspondingly more keys.
4. Automatic tracking of the location of the keys via GPS trackers
5. Facial recognition or thumbprint biometric technology for authorization purposes.
6. Extension cabinet support to add a new cabinet to hold more slots for keys.

## CHAPTER 10: REFERENCES

[https://www.mivanta.com/Assets/KeyGuard-Assets/images/products\\_page\\_images/KeyGuard-Manual.pdf](https://www.mivanta.com/Assets/KeyGuard-Assets/images/products_page_images/KeyGuard-Manual.pdf)  
<https://robu.in/product/mifare-rfid-readerwriter-13-56mhz-rc522-spi-s50-fudan-card-and-keychain/>  
<https://www.raspberrypi.org/>  
<https://docs.python.org/3.11/>  
<https://github.com/pimylifeup/MFRC522-python>  
<https://pimylifeup.com/raspberry-pi-rfid-rc522/>  
<https://gpiozero.readthedocs.io/en/latest/>  
<https://pypi.org/project/pyjson5/>  
<https://pinout.xyz/pinout/spi>  
<https://pypi.org/project/spidev/>  
<https://svelte.dev/>  
<https://github.com/vitalets/websocket-as-promised>  
<https://tailwindcss.com/docs>  
<https://www.typescriptlang.org/docs/>  
<https://websockets.readthedocs.io/en/stable/>