SOMAIYA
VIDYAVIHAR
K J Somaiya Institute of Technology
An Autonomous Institute Permanently Affiliated to the University of Mumbai

DEPARTMENT OF INFORMATION TECHNOLOGY

Synopsis of Minor Project On

NFC Door Guard

Prepared By:

Bruce Fernandes (Roll No. 7)
Ayush Hariya (Roll No. 9)
Sakshi Salvi (Roll No. 38)
Samarth Amodkar (Roll No. 41)

Under the guidance of:

Mrs. Sudeshna Baliarsingh

Department of Information Technology

Academic Year: 2023-2024

Autonomy Syllabus Scheme-II - SEMESTER V (TY - IT)

SOMAIYA
VIDYAVIHAR

K J Somaiya Institute of Technology
An Autonomous Institute Permanently Affiliated to the University of Mumbai

DEPARTMENT OF INFORMATION TECHNOLOGY

CERTIFICATE

This is to certify that following students:

	Roll No. / Seat No.
Bruce Fernandes	7
Ayush Hariya	9
Sakshi Salvi	38
Samarth Amodkar	41

have submitted PBL – Minor Project I Report on "NFC Door Guard" as the partial fulfillment for the requirement of Third Year of Engineering (5th Semester) in T.Y. - Information Technology under my guidance during the academic year 2023-2024.

Mrs. Sudeshna Baliarsingh
Project Guide
Assistant Professor
Department of Information Technology

Dr. Radhika Kotecha
Head of Department
Professor
Department of Information Technology

Date of Examination: _____

Signature of Internal Examiner

Signature of External Examiner

Table of Contents

Acknowledgement

We would like to express our sincere thanks to Assistant Professor Sudeshna Baliarsingh for her valuable guidance and support in completing our project. The completion of this assignment gives us immense pleasure. In performing our project, we had to take the help and guidelines from some professors, who deserve our greatest gratitude. We would like to express our gratitude to Prof. Sarita Rathod, Project guide, K. J. Somaiya Institute of Engineering and Information Technology for her valuable guidance for minor projects throughout numerous consultations. We would also like to extend our deepest gratitude to all those who have guided us in this project. We thank each and everyone who has extended help directly or indirectly to complete our project. We also thank the Head of Department, Dr. Radhika Kotecha, for introducing minor projects in the third year itself, hence providing exposure to students at an early stage.

We would also like to express our gratitude towards our principal Dr. Suresh Ukarande and vice principal Dr. Sunita Patil for giving us this great opportunity to do a project on NFC Based Door Guard System, without whose support, the project would not have been completed.

Abstract

In the age of automation where almost all household appliances are having the term“smart”, the need for a secured door system together with an automated circuit breaker is indeed a must have for being in the trend. With the use of NFC technology, entering a door hassle-free without countless keys and opening any door with just a tap of a single tag, which can be used as a keychain, is possible. The NFC Door Guard which comes with an PN532 Reader Writer and Raspberry pi for controlling the operations for door opening and closing and with the help of the servo motor. We will read the encrypted password through the NFC tag and the door will open if the password matches. For extra security we are storing passwords in the encrypted format. For Encryption we are using a symmetric type of encryption. The system prototype is evaluated, and it is 100% accurate when recognizing and authorizing an NFC card. It can also be reset in case of any theft of a card. For this purpose, we have developed an app which can monitor the log and add new users and users will also be able to see the logs of the person who has unlocked the door, all accessible through an Android application.

Keywords: NFC technology, PN532 Reader Writer, Raspberry Pi, Symmetric encryption

Chapter 1: Introduction

The project develops a smart door lock system using NFC technology for keyless entry and access control. It allows users to unlock doors by simply tapping encrypted NFC tags or cards on a reader. The system uses a Raspberry Pi as the core controller interfaced with an NFC reader module and servo motor for automatically locking/unlocking the door. Android app provides user management features like adding new users, resetting NFC tag passwords, viewing access logs etc. Encryption is implemented for security by encrypting the data on the NFC tags. The Raspberry Pi handles authentication by decrypting tapped tag data and unlocking the door if valid.Firebase Realtime Database enables remote logging and syncing of access events and credentials across devices.

1.1 Motivation

The need for secure and convenient access control systems in homes and offices is increasing. Traditional lock and key mechanisms are prone to issues like losing keys, making duplicate keys without authorization, and are not efficient for managing access for multiple users. This highlights the need for smart, digital access control solutions. NFC based systems provide a promising solution as they eliminate the need to carry physical keys, provide efficient access control through digital authentication, and offer features like access logs and user management.

Our motivation is to develop an affordable, smart NFC based access control system that provides both security and convenience. The system will use NFC tags that can be programmed with access credentials and carried like a keychain. Tapping the tag on a reader will authenticate the user and open the door. An accompanying mobile app will provide user management, access logs, and other smart features. Encryption will be used for security. Overall, the system will be low-cost compared to commercial electronic lock systems. It will benefit home users, small offices, and organizations needing convenient yet secure access control for multiple users. Such a system has immense application potential. Our project aims to develop a prototype of such an NFC based access control system and demonstrate its real-world viability. The learning outcomes in terms of technologies like NFC, encryption, microcontrollers etc. will also be significant.

1.2 Problem Analysis

Losing your keys is one of the most common and most frustrating mishaps. Usually, breaking locks using any heavy objects; but in case of Automatic Door Locks, one has to take down their whole door; which might result in a huge hole in bills. Considering the issue of forgetting or losing keys, security systems are quite popular these days to resolve that issue. Although, due to increase in demands, the price of these security systems are too high and not affordable for middle and lower classes. Making an alternate key to anyone's house is the most common method in theft; as it is easy to access.

1.3 Objectives

- Research Finding: Approximately 20 million people lose their keys annually in the US, contributing to security concerns and potential theft due to the availability of alternate keys.
- Affordability Goal: Develop an NFC-based security system that is cost-effective, making it accessible to a larger population.
- Alternate Key Registration: Implement a registration process through a mobile app to ensure that any alternate keys are authorized by the owner.
- Visitor Tracking: Enable users/owners to track visitors by associating their names with registered NFC keys, enhancing control and awareness of home entries.
- Unauthorized Entry Monitoring: Empower users to monitor and detect unexpected or unknown entries into their premises.
- Lost Key Access: Provide a secure mechanism for individuals who have lost their NFC key/tag/sticker to gain entry to their homes, subject to a series of verification processes through the mobile app.
- Mitigating Price Growth: Address the issue of rising security system costs by offering an affordable alternative based on NFC technology.

1.4 Scope

The main objective behind this project was to provide an alternate solution of the usual lock and key for locking system and make it more convenient for users. To provide the technological advancement in Smart Security System which is also affordable and budget friendly.

• To provide security from thieves and make it unable to bypass without proper NFC card . It will also allow user to keep an eye on the house entries through the application.
• The designed application has a user-friendly GUI, providing user all the access to handle their system feasibly.
• The designed application will provide user the control of passwords of both Application and NFC.

Chapter 2: Literature Review

2.1 Related Work

The authors propose a mutual authentication and attestation scheme for Internet of Things (IoT) devices using Near Field Communication (NFC) and secure elements. They use the secure element in NFC devices for storing keys and performing cryptographic operations. This provides tamper resistance and secure storage compared to software implementations. Their scheme involves mutual authentication between an IoT device and a reader using challenge-response with keys stored in their secure elements. This ensures both parties are legitimate. After authentication, the IoT device provides an attestation of its software state to the reader, proving it is in a trusted state. This prevents compromised devices from accessing the system.

The authors propose a smart door system for home security using a Raspberry Pi 3. They use a Raspberry Pi 3 as the central controller for the system. It interfaces with various sensors, actuators, and other hardware components. Sensors like PIR motion sensors and magnetic door sensors are interfaced to detect intrusions or door openings/closings. A camera module is connected to capture images when motion is detected. Images are processed to detect human faces. For access control, they implement RFID tag authentication. Approved RFID tags are stored in a database. The system actuates electro-mechanical locks, buzzers, and other devices to lock/unlock the door, sound alarms etc. It provides a graphical user interface using OpenCV and Python to display status and control the system. The paper "IoT and Image Processing based Smart Door Locking System"

The authors propose an IoT-based smart door locking system using image processing. They use a Raspberry Pi as the core controller and an IP camera module for image capture. The IP camera continuously captures images of the door area and sends them to the Raspberry Pi. Image processing algorithms are implemented on the Pi to detect faces in the images. OpenCV library is used for this. Recognized faces are compared against a database of approved persons. On match, the door is unlocked. For unauthorized or unrecognized faces, the door remains locked and an alert is sent to the owner via emails and SMS.

The authors propose a web-based smart security door system using QR code authentication. They use a Raspberry Pi as the core controller and a Pi camera module for QR code scanning. Users are provided unique QR codes which are scanned by the Pi camera when they present it in front of the door. The Pi processes the QR code, validates it against an online database, and triggers the door unlocking if authenticated. A central server hosts the user database and web interfaces for system control/monitoring. Pi connects to it over the internet. Users can login to the web interface through laptops/smartphones to view door cam feeds and unlock doors remotely via QR codes. An electromagnetic door lock mechanism is integrated with the Raspberry Pi using a relay circuit for automated locking/unlocking. Alerts and logs are available on the web interface when the door is accessed. Email/SMS notifications are also sent.

2.2 Existing System

Existing systems in NFC-based access control, along with references to relevant research papers:

Multiple commercial electronic door lock systems such as Yale's Assure Lock and Schlage's Encode Lock leverage NFC technology to enable keyless entry. Users can conveniently tap NFC cards or tags to gain access to secured areas. These advanced systems are complemented by mobile applications that facilitate remote user management and log monitoring. [2] Nevertheless, they are exclusive and high-cost solutions

Certain access control systems reliant on smartphones harness the NFC capabilities inherent in modern mobile devices for authentication purposes. Through emulating an NFC card, the smartphone interacts with door-installed readers. Access is granted upon successful matching of the phone's ID. [7] Notable providers of such systems include companies like Kisi, OpenPath, and HID Global. However, a drawback of standard NFC communication is its susceptibility to potential attacks .[1]

In response to the security vulnerabilities associated with NFC, several strategies have been employed, including the encryption of NFC data, integration of secure elements, and the implementation of two-factor authentication. HID Global, for instance, has introduced the Seos credential technology, which utilizes NFC in conjunction with a secure enclave chip for authentication and cryptography purposes [4].

Chapter 3: Proposed System

The project develops an NFC-based door lock system using Raspberry Pi and Android app. It allows door access through encrypted NFC tags tapped on a reader. The app provides user management and activity logs.

- **Log-in:**

  This allows users to get logged in into their registered account. While logging in, it asks for username and password credentials. It checks if the entered username and password matches with the registered or saved credentials. If it matches, then it'll allow the user to login else it will get canceled.

- **Register**

  This page helps users to save to create their account using their Name, Email-ID and NFC Password along with user password. Once the user clicks the register button it will store all the entered data into the firebase database.Additionally, Firebase provides authentication and security features, offering encrypted storage and access rules, ensuring that only authorized entities can retrieve or modify the stored user data. This registration process, integrated with Firebase, not only captures user information but also establishes a foundation for a robust, cloud-based infrastructure that can support the NFC-based access control system with reliability and data security.

- **Reset password:**

  To reset password due to any personal reasons, users have to enter their username and password. The entered credentials will get compared to the already saved data. Only if they match, the "Enter new password" will get active. Then users just have to enter their new password.

- **Past entries of user (logs):**

  This page is supposed to display the entries of users using their assigned tag and card. It displays entered time, registered tag and date is displayed. The same gets recorded in the firebase database.Furthermore, the log data stored within Firebase can be leveraged for statistical analysis or reporting purposes. Trends in entry times, frequently accessed areas, or other patterns can be extracted, aiding in optimizing security protocols or understanding user behaviors within the controlled environment.

3.1 Proposed Approach and Details

The use case diagram depicts the key users of the system like users and the core functions they can perform. This includes registering new tags, tapping tags to unlock doors, viewing access logs in the app. It captures the high-level user interactions.

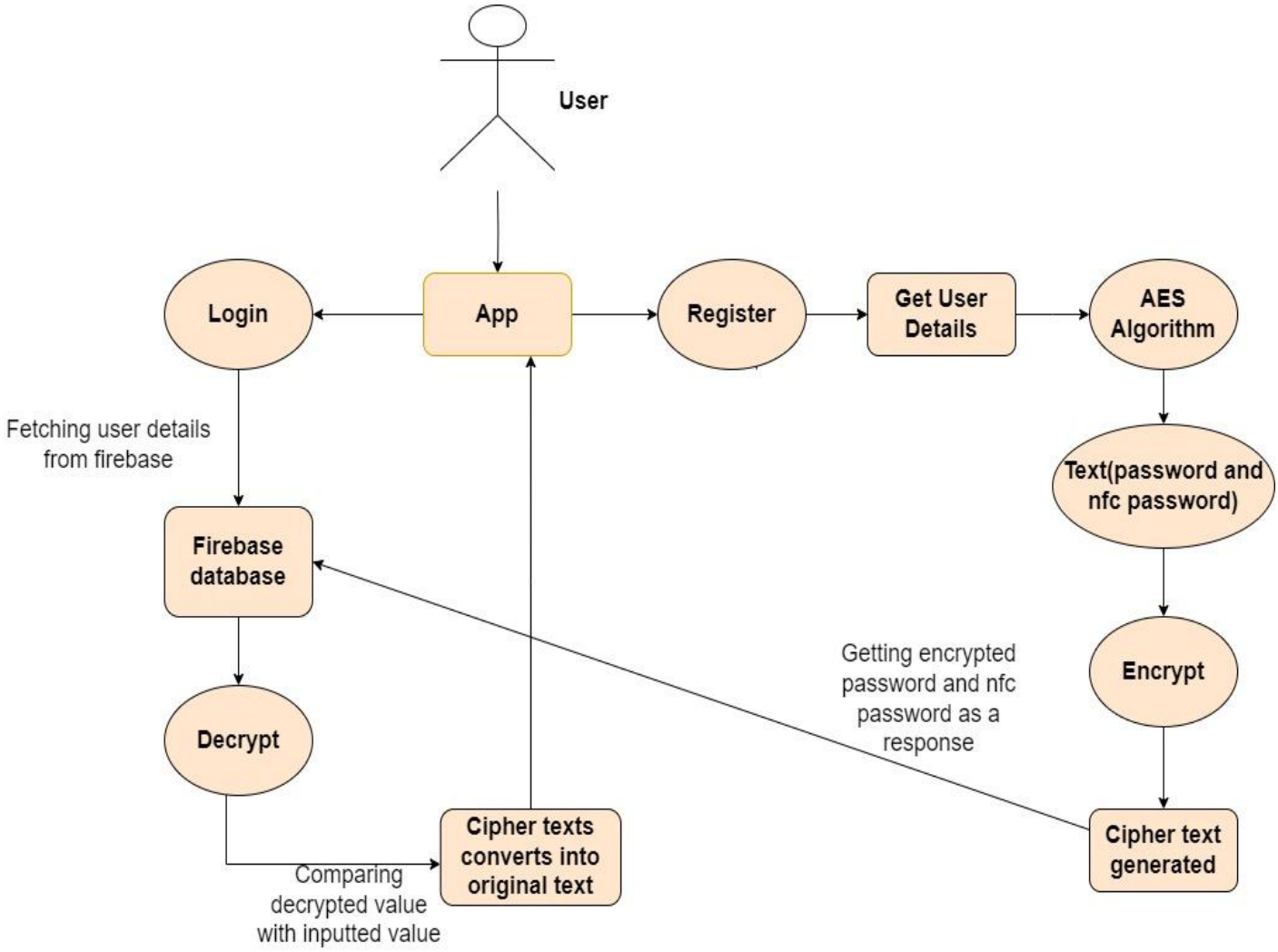


Fig No 3.1 Use Case Diagram

Figure No 3.1 shows the use case of our app. The key users of the system (owner, authorized users) and the main functions they can perform like registering tags, tapping tags to unlock doors, viewing access logs, etc. It captures the high-level user interactions with the system.

Hardware DFD

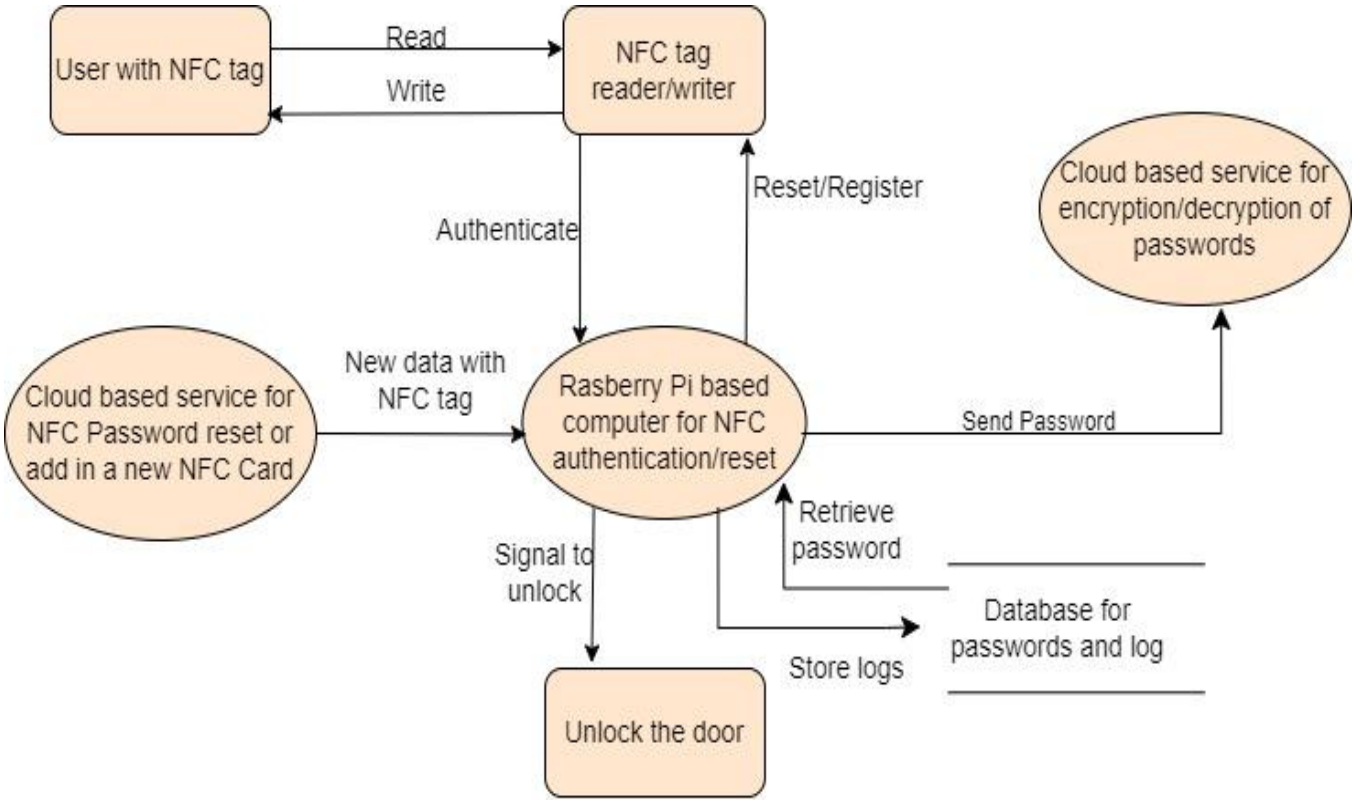


Fig No 3.2 Hardware DFD

Figure No 3.2 depicts the flow of data in our hardware components.The key hardware components of the system like the NFC reader, Raspberry Pi, servo motor, mobile app, and Firebase database. It shows how these components interact and exchange data. For example, the NFC reader sends tag data to the Raspberry Pi which processes it, queries the database, and controls the servo motor to unlock the door accordingly. The mobile app interfaces with the database.

3.2 Innovation in Idea

Key innovative ideas in this NFC-based security system are:

1. Using NFC technology for access control:
- Replacing physical metal keys with NFC tags or cards provides a more convenient and customizable way to grant access to doors. Users can simply tap their card on the reader instead of fumbling with keys.
- The system allows easy provisioning of access rights by writing credential data to inexpensive NFC tags that function as digital keys. Old keys can be revoked and new ones issued easily.

2. Encrypted NFC card data:
- The password or credential data stored on the NFC card is encrypted using symmetric key cryptography before writing to the tag.
- This adds an extra layer of security, as simply copying or scanning the data on the tag will not work to gain access without the decryption key.
- It prevents unauthorized access even if NFC cards are lost, protecting the system.

3. Mobile app for access management:
- The Android app allows administrators/home owners to conveniently manage the system remotely using their smartphones.
- Features like adding new user credentials to the database, viewing logs of door accesses, resetting passwords of lost NFC cards etc. are provided.
- Remote monitoring and control of the system is enabled without needing physical access to the device.

4. Integrated door unlock mechanism:
- The system directly integrates door locking/unlocking mechanisms by interfacing a servo motor with the Raspberry Pi controller.
- This eliminates the need for any manual operation like turning keys or pressing buttons for access.
- The NFC tag authentication controls the servo to provide hands-free, automated entry.

5. Flask server for encryption/decryption:
- A separate Flask server handles the encryption/decryption of NFC tag data and key management.
- This provides modularity and separation of the security critical aspects from the main mobile app and hardware system.
- It also allows encryption keys to be stored securely on the server side rather than the local device.

3.3 Timeline

The project timeline spanned over 6 months, divided into requirements gathering, system design, mobile app development, Raspberry Pi programming, encryption implementation, integration, testing, and deployment phases. An iterative agile approach was followed with weekly sprints to incrementally build and validate the system.

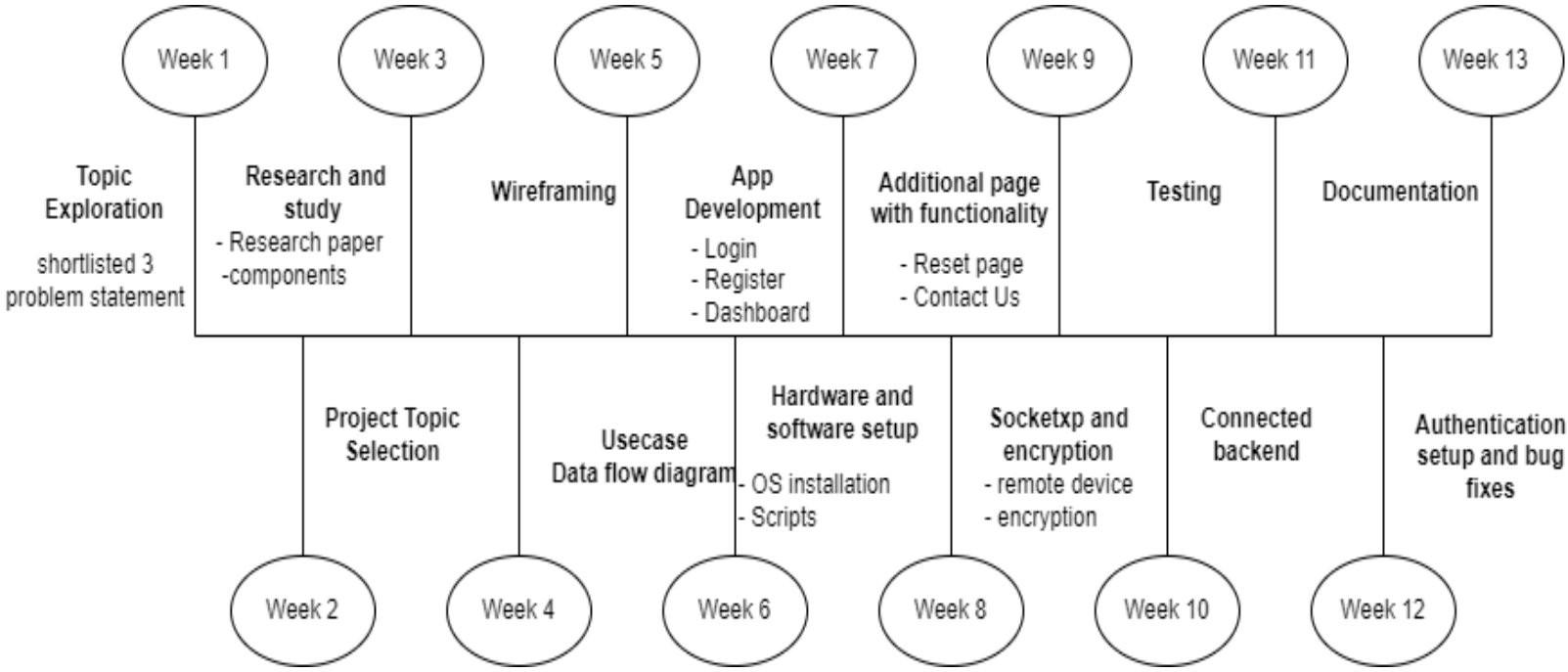


Fig No 3.3 Timeline chart

3.4 Roles and Responsibilities

It outlines the specific roles that individuals or teams will play in the project and the associated responsibilities. It serves as a foundational document to ensure clarity, accountability, and efficient project management.

Frontend:

Sakshi Salvi, Ayush Hariya:
– App Development (UI development)

- Home Page
- Login Page
- Register Page
- Dashboard
- Reset Page
- Contact Us page

Backend:

Samarth Amodkar , Bruce Fernandes:
– Server setup
– Database
– Encryption implementation

Hardware Setup:

- Raspberry Pi configuration - Samarth
- Servo motor connection - Ayush, Bruce
- PN532 connection with raspberry pi - Sakshi

3.5 Software Lifecycle Model

An iterative and incremental agile software development lifecycle model was followed in this project. This was needed because of the hardware-software integration nature of the system involving the mobile app, Raspberry Pi, and various modules. The agile approach allowed us to work in short sprints and continuously test and integrate components. The phased testing and continuous integration of the mobile, hardware, and cloud components made agile methodologies more suitable for this project.

Requirements Gathering:

Functional requirements

- User registration and login for the mobile app
- Allowing users to reset passwords

- Displaying logged access events and details
- Encrypting/decrypting passwords using a Flask server
- Reading NFC tags and unlocking door using Raspberry Pi

Non-functional requirements around:

- Usability - Intuitive mobile app UI/UX
- Security - Encrypted NFC tag data
- Performance - Fast unlocking mechanism
- Availability - Data persistence using Firebase

Analysis and Design:

High-level system design created using Data Flow Diagrams showing:
Components like mobile app, NFC reader, door lock
Flow of data between components
How encryption/decryption server interacts with app
Detailed component design not explicitly specified, seems to have followed an iterative approach
Database schema not covered in detail, but Firebase would provide flexibility here Interactions between app, Flask server, Raspberry Pi and Firebase database outlined at a high-level

Implementation:

- Mobile app was implemented using Android Studio and Java.
- Flask server was built using Python for encryption/decryption functions.
- Raspberry Pi integrated with PN532 NFC module and servo motor for unlocking.

Testing:

- Test cases were written to validate different features and user flows of the mobile application.
- Hardware integration was tested by simulating NFC tag reading and door unlocking.

Deployment:

- The app, Flask server and Raspberry Pi compile into an integrated system for deployment.
- Firebase database enables persistence and availability of data across devices.

Maintenance:

- Future work is highlighted like enhancements to the mobile app features.
- Iterative development allows incorporating feedback and improvements.

Chapter 4: Implementation Details and Results

In this chapter, we delve into the technical aspects of implementing our NFC-based security system. We provide insights into the technology stack utilized, key hardware and software components, and the encryption methods employed to ensure the system's security and functionality.

4.1 Technology Stack

Technology stack used for implementing this NFC-based security system comprises:

Android Studio: For developing the Android application using Java
Firebase Realtime Database: For storing and syncing user data across devices
Android Smartphone: Acts as the client device for the management mobile application
Java: For developing the core Android application logic
Python: For implementing Flask server and Raspberry Pi programming

4.2 Implementation Parameters

key implementation parameters for the NFC-based door access system:

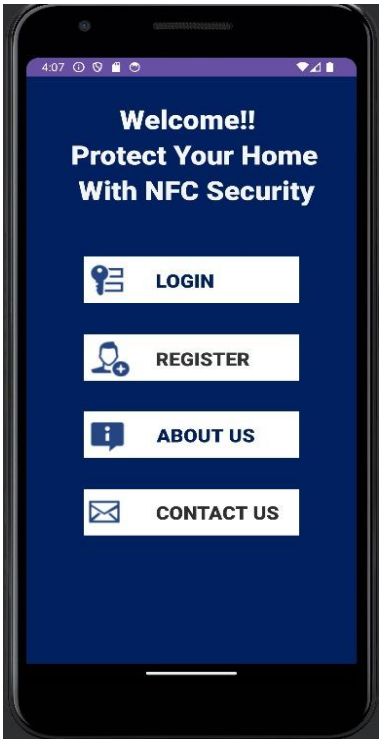
Hardware:
Raspberry Pi: Acts as the core controller
PN532 NFC Module: Used to read NFC tags
Servo Motor: For automatically locking/unlocking the door
Smartphone with NFC support: For the mobile app

Software:
Android Studio: For developing the mobile app
Python: For programming the Raspberry Pi
Firebase Realtime Database: For storing access logs and credentials

Encryption:
Symmetric encryption used to encrypt/decrypt NFC tag passwords
AES algorithm implemented for encryption

4.3 Preliminary Results

NFC Door Guard project encompasses user login and registration for access control, a dashboard for giving options, a reset feature for lost credentials, and a contact us page for user support. This ensures a secure and user-friendly experience in managing access to secured areas.



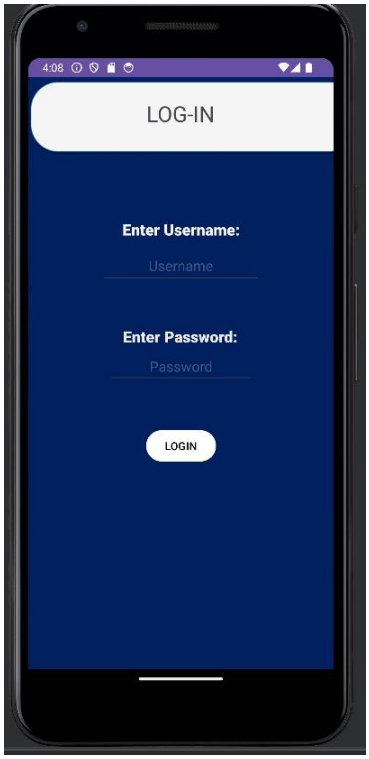


Fig No 4.1 Home Page

Fig No. 4.2 Log-In

Fig No. 4.1 Home Page: This is the landing screen of the mobile application. Two prominent buttons for Login and Register are present to allow users to either enter their credentials or sign up for a new account. This provides an overview of the app's capabilities.

Fig No. 4.2 Log-In: The Log-in page contains fields for users to enter their username and password. There is also a Forgot Password link for password recovery. Upon tapping the Login button after entering credentials, validation is performed against the back-end database. If valid credentials are entered, the user is taken to the main Dashboard screen. Else, an error message is displayed.

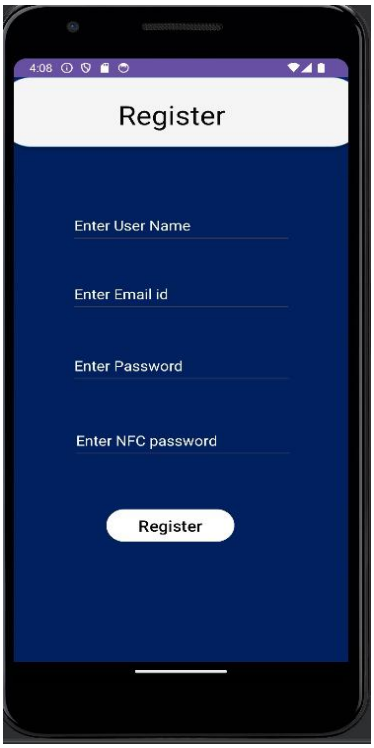
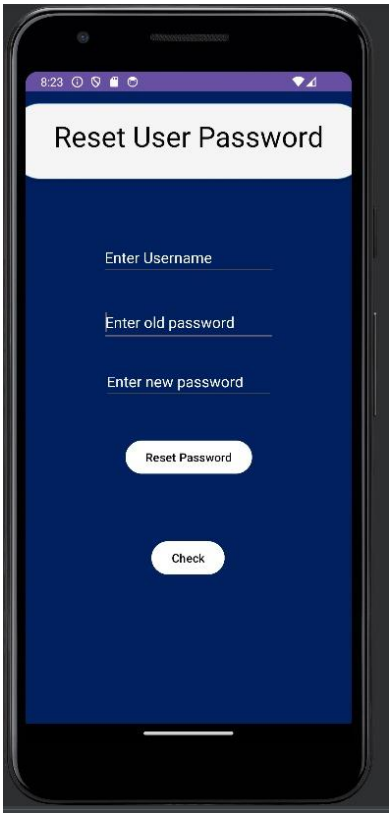


Fig No. 4.3 Registration page

Fig No. 4.4 Dashboard

Fig No. 4.3 Registration Page: This page allows new users to sign up for the system. Fields are provided to enter details like Full Name, Email ID, Password and Confirm Password. There are also options to enter the NFC Tag Password which will be programmed onto the physical NFC card provided to the user. Tapping Register will create a new user account in the backend database.

Fig No. 4.4 Dashboard: Post login, this is the main screen where users land. It displays a summary of recent door accesses by showing details like Date, Time, User etc in a tabular format. There are also options provided to add a new user, view detailed logs, reset NFC passwords etc. The menu bar gives access to other screens.



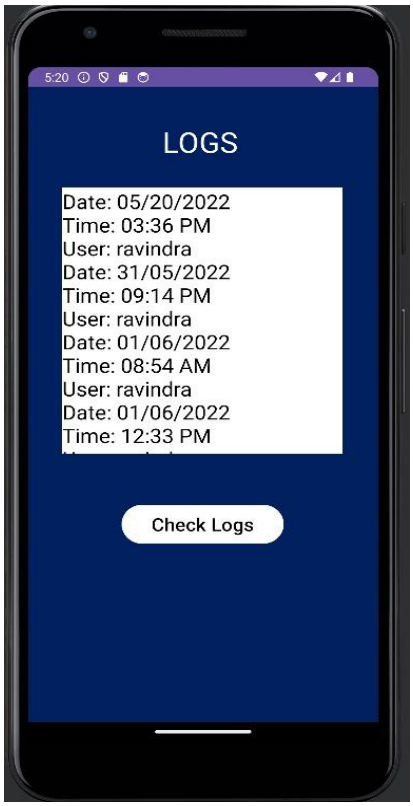


Fig No. 4.5 Reset Password

Fig No. 4.6 Logs

Fig No. 4.5 Reset Password: This page contains fields for users to enter their username and current password. Once validated, it allows them to enter and confirm the new NFC password which will be re-programmed onto their access card for door entry.

Fig No. 4.6 Logs: This screen shows the detailed logs of all door accesses with granular data like user name, NFC tag ID used, timestamp etc. in an ordered table. Tapping on each log provides additional details

Fig No. 4.7 Contact Us

.

Fig No. 4.7 Contact Us: This simple page displays the contact information of the developer or company handling the app and system for user support purposes. It contains details like Email ID, Phone number, Address etc.

Chapter 5: Conclusion

5.1 Conclusion

Traditional physical key based systems are inconvenient and prone to theft. Hence, advanced tech-driven security solutions are needed, though expensive smart systems are unaffordable for most. This project aimed to develop a cost-effective yet advanced NFC based automated door lock system to address these challenges.

This project successfully demonstrates a working prototype of an NFC enabled smart lock with key features like cryptography, automation, connectivity and remote access. As an affordable solution built using Raspberry Pi and NFC modules, it proves the concept of developing security systems for the average household.

With further enhancements in terms of additional sensors, alarms, biometrics and cloud connectivity, this foundational NFC enabled system can become a full-fledged home security product. In conclusion, the project delivers a cost-effective smart lock solution with strong potential for further expansion.

5.2 Future Scope

- The system can be enhanced by adding automatic door closing and displaying it in the app.
- Sensory systems can be integrated to detect forced entries and inform users.
- A database and GPS can be connected to the app so that users can quickly contact police in case of emergencies.
- More security features like fingerprint or face recognition can be incorporated along with NFC.
- The system can be expanded into a complete home automation system with centralized control.
- Cloud connectivity can be provided to enable access through web interfaces.
- Machine learning can be implemented for intelligent monitoring and access control.

References

[1] S. Sugano, S. Kawazoe, K. Takahashi, and M. Nishida, “Indoor Localization System using RSSI Measurement of Visible Light Communication and Acceleration Responses,” 2015 Int. Conf. Indoor Position. Indoor Navig., pp. 1–6, 2015.

[2] J. Choi, K. Lee, R. Elmasri, and D. W. Engels, “Pedestrian tracking using Inertial Sensors with indoor landmarks,” 2013 IEEE Int. Conf. Syst. Man, Cybern., pp.

[3] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, “Practical NFC peer-to-peer relay attack using mobile phones,” 2010 6th Int. Conf. Radio Frq. Identify. Secur. [1] NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access. (2018, November 1). IEEE Journals & Magazine

[4] Smart Door System for Home Security Using Raspberry pi3. (2017, September 1). IEEE Conference Publication

[5] IoT and Image Processing based Smart Door Locking System. (2022, December 13). IEEE Conference Publication

[6] JosephNg, P. S., BrandonChan, P. S., & Phan, K. Y. (2023, July 24). Implementation of Smart NFC Door Access System for Hotel Room. Applied System Innovation; Multidisciplinary Digital Publishing Institute.

[7] Rastogi, R., Sharma, B., Gupta, N., Gaur, V., Gupta, M., Kohli, V., Sharma, A., K., Srivastava, P., & Rai, A. (2022, January 1). NFC-enabled packaging to detect tampering and prevent counterfeiting: Enabling a complete supply chain using blockchain and CPS. Elsevier eBooks.

[8] Mostakim, N., Sarkar, R. R., & Hossain, M. A. (2019, May 8). Smart Locker: IOT based Intelligent Locker with Password Protection and Face Detection Approach. International Journal of Wireless and Microwave Technologies

[9] Pau, G., Arena, F., Collotta, M., & Kong, X. (2022, August 1). A practical approach based on Bluetooth Low Energy and Neural Networks for indoor localization and targeted devices’ identification by smartphones. Entertainment Computing; Elsevier BV.

[10] Saravia, M. W. D. (2015, November 1). Access control system using NFC and Arduino.