3 Factor Authentication System

Submitted In Fulfillment of Requirements
For the Degree Of

Honours in Cyber Security & Forensics
(Offered by Department of Computer Engineering)

By

Vedansh Hetal Avlani
Roll No: 16010120001

Arvin William Dias
Roll No: 16010120012

Khushi Kenia
Roll No: 16010120020

Guide

Swati Mali

Somaiya Vidyavihar University
Vidyavihar, Mumbai - 400 077

2020-24

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya Vidyavihar University
K. J. Somaiya College of Engineering

Certificate

This is to certify that the dissertation report entitled **3 Factor Authentication System** submitted by Vedansh Avlani, Arvin Dias and Khushi Kenia at the end of semester VIII of LY B. Tech is a bona fide record for fulfillment of requirements for the degree Honours in Cyber Security & Forensics (**Offered by Department of Computer Engineering**) of Somaiya Vidyavihar University

Guide

Head of the Department

Student 1 (001)
Vedansh Avlani

Student 2 (012)
Arvin William Dias

Student 3 (020)
Khushi Kenia.

Examiner
04-03-2024

Date: 26-02-2024

Place: Mumbai-77

Abstract

In today's increasingly digitized world, cybersecurity threats pose a significant challenge to the integrity and confidentiality of sensitive information. To address these challenges, this project proposes the development of an advanced multifactor authentication system aimed at enhancing security while ensuring user convenience. By leveraging innovative techniques such as OTPs (one-time passcodes) and RFID (Radio Frequency Identification) card scanning, the system aims to mitigate common vulnerabilities associated with traditional username-password authentication methods.

The project encompasses a comprehensive literature review to analyze existing authentication protocols and technologies, followed by meticulous system design and development. Through iterative refinement and rigorous testing, the authentication system aims to achieve optimal performance, robust features, and resilience against various cyber threats. Furthermore, user feedback and performance metrics will be collected to assess usability and effectiveness, facilitating continuous improvement and adaptation to evolving security needs.

This project contributes to the field of cybersecurity by offering a practical and robust authentication solution that balances security requirements with user experience. By incorporating multifactor authentication mechanisms and leveraging cutting-edge technologies, the system aims to establish a secure foundation for safeguarding digital assets and mitigating cyber risks in this progressively digitized world.

Keywords: cybersecurity, authentication, multifactor authentication, one-time passcodes, OTP, RFID, system design, user-friendly interface, cyber threats, digital security.

Contents

Chapter 1

Introduction

This chapter provides the rationale behind the chosen thesis topic, outlines project objectives for enhancing security measures, and summarizes the methodologies employed, including literature review, system design, implementation, and evaluation, to achieve the stated goals effectively.

In this age of immense technological evolution, safeguarding sensitive information of individuals has become a priority for the users. The escalating threats violating confidentiality and integrity as technology advances, the methods and tactics employed by malicious actors seeking unauthorized access to personal and confidential data. In light of these challenges, the implementation of robust authentication mechanisms has become imperative in safeguarding digital assets. Vulnerabilities in real-world systems like data leaks due to unauthorized access to personal information, financial assets, organization-wide strategies and many more.

This project focuses on eradicating such challenges occurring due to incorrect or frail authorization processes. Authentication in an MFA system can include three types of factors that enable a user to prove their identity. These three factors include: Something the user has which could be any physical object in the possession of the user, such as an RFID card in this case. Something the user knows: Certain knowledge only known to the user, such as a password or a PIN. Something the user is: Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, pattern in key press intervals, etc.

The focus of this thesis is on the design and implementation of a comprehensive three-factor authentication system aimed at enhancing the security of user logins within a system. This system integrates traditional username-password authentication with email-based one-time passwords (OTPs) and radio-frequency identification (RFID) card scanning, thereby providing multiple layers of security both software and hardware comprehensive to verify the identity of the user.

1.1 Motivation

The motivation behind selecting this thesis topic stems from the growing concerns surrounding cybersecurity threats and the need for more robust authentication measures. With the explosion of online services and the increasing digitization of sensitive information, traditional username-password authentication has proven to be vulnerable to various forms of attacks such as phishing, brute force, and dictionary attacks. By incorporating additional factors such as One-Time Passwords (OTPs) and Radio-Frequency Identification (RFID) card scanning, we aim to mitigate these vulnerabilities and enhance the overall security posture of the system. Through the integration of these advanced authentication mechanisms, the system seeks to establish a multi-layered defense strategy that significantly reduces the risk of unauthorized access and data breaches, thereby ensuring the integrity and confidentiality of user information in today's interconnected digital landscape.

1.2 Objectives

The primary objective of this project is to develop a multifaceted authentication solution that enhances security without compromising user experience. Specific goals include:

- Designing an intuitive and user-friendly interface for seamless interaction with the authentication system, prioritizing accessibility and ease of use for users of all technical backgrounds.
- Implementing robust algorithms for generating and validating one-time passcodes, ensuring resistance against common attacks such as replay and brute-force attacks, while also considering factors like expiration times and session management.
- Integrating RFID technology for swift and reliable identification of authorized users, exploring techniques to prevent cloning or spoofing of RFID cards and ensuring compatibility with existing RFID infrastructure where applicable and reducing the threat to physical access to systems.
- Evaluating the performance, reliability, and security of the authentication system through rigorous testing and analysis, including simulated attack scenarios, usability studies, and feedback from end users to identify areas for improvement and refinement.
- Developing comprehensive documentation and training materials to facilitate the deployment and adoption of the authentication system, empowering administrators and end users with the knowledge and resources needed to effectively utilize and maintain the system over time.
- Establishing a roadmap for future enhancements and updates to the authentication system, incorporating feedback from ongoing monitoring and evaluation processes as well as emerging technologies and security trends to proactively address evolving threats and user needs.
- Promoting awareness and education around cybersecurity best practices and the importance of strong authentication measures, advocating for a culture of security-conscious behaviour and proactive risk management within organizations and communities.

1.3 Methodology

The methodologies employed in this thesis will involve a combination of literature review, system design and development, experimentation, and evaluation. Firstly, a comprehensive review of existing authentication protocols and technologies will be conducted to understand their strengths, weaknesses, and applicability to the project objectives. This will entail identifying key research papers, articles, and industry reports related to OTPs, RFID card scanning, and multifactor authentication to inform the design and development process. Subsequently, the system will be designed with a focus on integrating OTPs and RFID card scanning while prioritizing user experience and security. This phase will involve developing detailed system architecture diagrams, data flow diagrams, and interaction diagrams to visualize the flow of information and interactions within the system, alongside designing a user-friendly interface that streamlines the authentication process and provides clear feedback to users at each stage.

Once the design phase is completed, the authentication system will be implemented using appropriate programming languages, frameworks, and development tools. This includes incorporating algorithms and protocols for generating, transmitting, and validating one-time passcodes, as well as authenticating RFID cards and verifying user identities. Compatibility with existing hardware and infrastructure, such as RFID readers and backend databases, will be ensured to facilitate seamless integration and interoperability. Subsequently, comprehensive testing of the authentication system will be conducted to validate its functionality, security, and performance under various scenarios and conditions. This will involve vulnerability assessments, penetration testing, and simulated attack scenarios to identify and address potential security vulnerabilities and weaknesses. Additionally, user feedback will be gathered through usability studies, surveys, and interviews to assess the effectiveness, ease of use, and overall user satisfaction with the authentication system. Finally, performance metrics such as authentication latency, error rates, and system uptime will be analyzed to evaluate the system's reliability and scalability in real-world deployments. The findings and insights from these phases will be documented in a detailed technical report or thesis document, along with clear guidelines and instructions for system administrators and end users on deployment, configuration, and usage of the authentication system.

Chapter 2

Literature Survey

This chapter provides a comprehensive overview of existing authentication methods, highlighting their strengths, weaknesses, and relevance to the project's objectives. It serves as a foundation for designing and implementing the multifaceted authentication system.

2.1 [1] Three factor authentication

-William Kennedy, Aspen Olmsted

The paper titled "Three Factor Authentication" by William Kennedy and Aspen Olmsted explores the implementation and implications of a three-factor authentication model for enhanced security in websites and mobile apps. The research focuses on developing an application that combines password-based authentication, username, and facial recognition for a more robust authentication process. The motivation of this paper is to design a secure three-factor authentication app that prioritizes user privacy, convenience and no latency. The implementation involves the use of MIT App Inventor 2 beta, with facial recognition functionality provided through the CamVision extension and the integration of Microsoft Cognitive Service for computer vision API.

Advantages:

1. **Enhanced Security:** Three-factor authentication combines something the user knows (password), something they have (username), and something they are (facial recognition), providing a higher level of security.
2. **User Privacy:** The use of facial recognition as one of the authentication factors adds an extra layer of privacy compared to traditional methods.
3. **Efficiency:** The developed app demonstrates simplicity and convenience with a one-click sign-in capability, minimizing the cost of convenience for users.
4. **Reliability:** The combination of multiple authentication factors increases confidence and reliability in the security of the platform.

Limitations:

1. **Prototype Stage:** The app is in the prototype phase, with certain features like user account creation not fully implemented at the time of the study.
2. **Hard-Coded Credentials:** The initial implementation relies on hard-coded credentials, limiting user customization. Future iterations should allow users to create their own accounts.
3. **Dependency on External Services:** The app relies on external services like CamVision and Microsoft Cognitive Service, introducing a dependency that may impact reliability if these services face disruptions.
4. **Facial Recognition Concerns:** While facial recognition adds privacy, concerns regarding the security and ethical implications of biometric data storage and processing should be considered.
5. **Limited Scope:** The study primarily focuses on the implementation of the app and its functionality, with limited exploration of potential vulnerabilities or real-world testing scenarios.

Conclusion and Future Work: The authors suggest that a three-factor authentication method is likely to become a future market standard due to its efficiency and increased reliability. Future work includes further research and development of the app to allow users to create accounts, save credentials, and biometric reference tags. Additionally, addressing limitations and conducting further analysis on the security and privacy aspects of the proposed authentication model would contribute to the continued success and adoption of such systems.

2.2[2] Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System

-Bintang Wahyudono, Dion Ogi

This paper introduces a two-factor authentication system for access control, utilizing RFID and face recognition with the Local Binary Pattern (LBP) algorithm to enhance security. The system achieves 100% accuracy in RFID authentication and 80% in face recognition. RFID authentication takes 0.03 seconds on average, face recognition 6.3885 seconds, and verification 0.1970 seconds. The system demonstrates stability over three consecutive days.

Advantages:

1. **High Accuracy:** The system achieves excellent accuracy, with 100% in RFID authentication and 80% in face recognition.
2. **Security Against Spoofing:** The LBP algorithm effectively detects face spoofing attacks, providing a robust defense against photo attacks.
3. **Quick RFID Authentication:** RFID authentication is swift, averaging 0.03 seconds, contributing to efficient access control.
4. **Stable Performance:** The system maintains functionality over three consecutive days without interruptions, ensuring reliability.

Limitations:

1. **Face Recognition Speed:** The face recognition process takes comparatively longer at 6.3885 seconds, which might impact the overall speed of the system.
2. **Face Recognition Accuracy:** Although achieving 80% accuracy, improvements could be made to enhance the reliability of face recognition.
3. **Complex Implementation:** The use of the LBP algorithm adds complexity to the system, potentially requiring more computational resources.
4. **Limited Spoofing Scenarios:** The study specifically addresses photo attacks; however, the system's effectiveness against other spoofing methods remains unexplored.

In conclusion, the proposed system offers strong security features against spoofing attacks, but there is room for improvement in terms of face recognition speed and accuracy. The advantages include high RFID accuracy and robust spoofing detection, while limitations involve longer face recognition times and the need for further optimization.

2.3[3] Adoption of a Secure ECC-based RFID Authentication Protocol - Souhir Gabsi; Yassin Kortli; Vincent Beroulle; Yann Kieffer; Hamdi Belgacem

The paper discusses Radio Frequency Identification (RFID) technology, focusing on securing RFID systems through the adoption of elliptic curve cryptography (ECC) in authentication protocols. It compares three ECC-based RFID authentication protocols – Naeem, Dinarvand, and Benssalah – with a focus on their computational performance and security against wireless attacks.

Advantages:

1. **ECC Integration:** The paper highlights the advantages of using ECC-based cryptographic algorithms in RFID systems, emphasizing the high security level with relatively low computational complexity compared to other asymmetric cryptographic systems.
2. **Authentication Protocols:** The paper presents three recent ECC-based RFID authentication protocols - Naeem, Dinarvand, and Benssalah - each aiming to enhance security against various wireless attacks, including cloning, eavesdropping, tracking, and server spoofing.
3. **Comparative Study:** A comparative study is conducted, evaluating the computational performance and security strengths of the three protocols. This analysis involves the implementation cost and vulnerability assessment against attacks such as replay, impersonation, denial-of-service, and tracking.
4. **Performance Analysis:** The paper provides a detailed performance analysis, considering computation time and communication cost. It identifies the strengths and weaknesses of each protocol in terms of scalability, efficiency, and resource utilization.
5. **Security Evaluation:** The protocols' security against different wireless attacks is thoroughly evaluated, providing insights into their strengths and vulnerabilities. The Benssalah protocol is highlighted for its efficiency in resisting various attacks.

Limitations:

1. **Desynchronization Vulnerability:** The Dinarvand protocol is noted to have a vulnerability against desynchronization attacks. The updating phase for pseudonyms and secret keys may be exploited if an attacker intervenes to block the latest message sent by the tag.
2. **Impersonation Vulnerability:** The Naeem protocol is found to be vulnerable to impersonation attacks, allowing attackers to discover the tag's identity and potentially present themselves as legitimate readers.
3. **Security Concerns:** The paper identifies security concerns in the Naeem and Dinarvand protocols, emphasizing the need for a balance between security and computational efficiency.
4. **Communication Cost:** While the Benssalah protocol exhibits lower communication costs, the paper does not delve into potential trade-offs or practical considerations associated with these costs.

Conclusion: The paper concludes that the Benssalah protocol demonstrates the best security against various wireless attacks with acceptable computational performance. It suggests the optimization of scalar multiplication operations to further enhance performance in future implementations.

2.4[4] Research on RFID attack methods

- Yisen Wang; Jianjing Shen; Xiaofeng Guo; Weiyu Dong

This research paper investigates the security vulnerabilities of RFID technology. Despite its widespread applications, RFID systems face challenges such as susceptibility to side channel attacks and system spoofing. The paper explores four attack methods against RFID and proposes an RFID security detection model. The study analyzes the RFID system's bidirectional authentication process, identifying vulnerabilities such as parity bit vulnerability and nested authentication vulnerability. Attack methods, including brute force, random number attacks, multisector authentication, and password sniffing, are detailed, outlining potential exploits in the authentication process. The paper concludes with a discussion on the proposed RFID security detection model, emphasizing the need for further research to enhance RFID security mechanisms.

Advantages:

1. **Comprehensive Coverage:** The paper provides a thorough examination of RFID technology, covering its background, security mechanisms, vulnerabilities, attack methods, and the proposal of a security detection model.

2. **Detailed Attack Analysis:** The research offers in-depth analyses of four RFID attack methods, shedding light on specific vulnerabilities and potential exploits in the authentication process.

3. **Practical Relevance:** By discussing real-world examples like the cracking of Mifare Classic chip, the paper establishes the practical relevance of its findings and emphasizes the urgency of addressing RFID security issues.

Limitations:

1. **Assumed Knowledge:** The paper assumes a certain level of familiarity with RFID technology and security concepts, potentially limiting accessibility for readers with less background in these areas.

2. **Currentness:** The knowledge cutoff date is not specified, and the paper may not include recent developments in RFID security, making it important to verify the currency of the information.

3. **Focus on Vulnerabilities:** While the paper thoroughly explores vulnerabilities and attack methods, it could benefit from a more extensive discussion of potential countermeasures and solutions to enhance RFID security.

2.5[5] RFID systems integrated OTP security authentication design

- Chao-Hsi Huang; Shih-Chih Huang

The paper introduces a security authentication design for RFID systems, focusing on countering security threats associated with data transactions in a public wireless environment. The proposed solution employs a one-time password (OTP) authentication method to enhance RFID tag security. The system uses the RFC-6238 Time-Based One-Time Password (TOTP) algorithm, based on HMAC-SHA1, to generate OTPs for RFID tags. NFC-enabled smartphones are utilized to generate TOTPs and write them to the tags. The paper also integrates RADIUS AAA authentication mechanisms for flexible integration into existing systems and introduces roaming capabilities for users across different service providers.

Advantages:

1. **Enhanced Security:** The OTP authentication method improves RFID tag security by preventing forgery and attacks. It addresses issues like eavesdropping, replay attacks, and cloning.

2. **Cost and Complexity Reduction:** The system proposes a method to write OTPs to RFID tags without modifying the tag circuit, reducing implementation costs and complexity.

3. **Wide Applicability:** The solution is designed to be applied to various RFID tags with more than 20 bits of rewritable memory space, offering flexibility and compatibility.

4. **Flexible Integration:** Integration with existing systems is facilitated through the use of RADIUS AAA authentication mechanisms, allowing easy adoption by different RFID systems.

5. **Roaming Functionality:** The system supports roaming, enabling users to use the same RFID tag across different systems, provided they use the same frequency and RFID technology standard.

Limitations:

1. **Limited Memory Space:** The paper acknowledges the limited memory space of RFID tags, which may constrain the implementation of complex cryptographic operations.

2. **Sensitivity to Consecutive Failed Attempts:** The system automatically locks the tag after a certain number of consecutive failed authentication attempts, which might inconvenience users in case of legitimate issues.

3. **Dependence on NFC-Enabled Smartphones:** The proposed OTP generator relies on NFC-enabled smartphones, potentially limiting its usability for users without such devices.

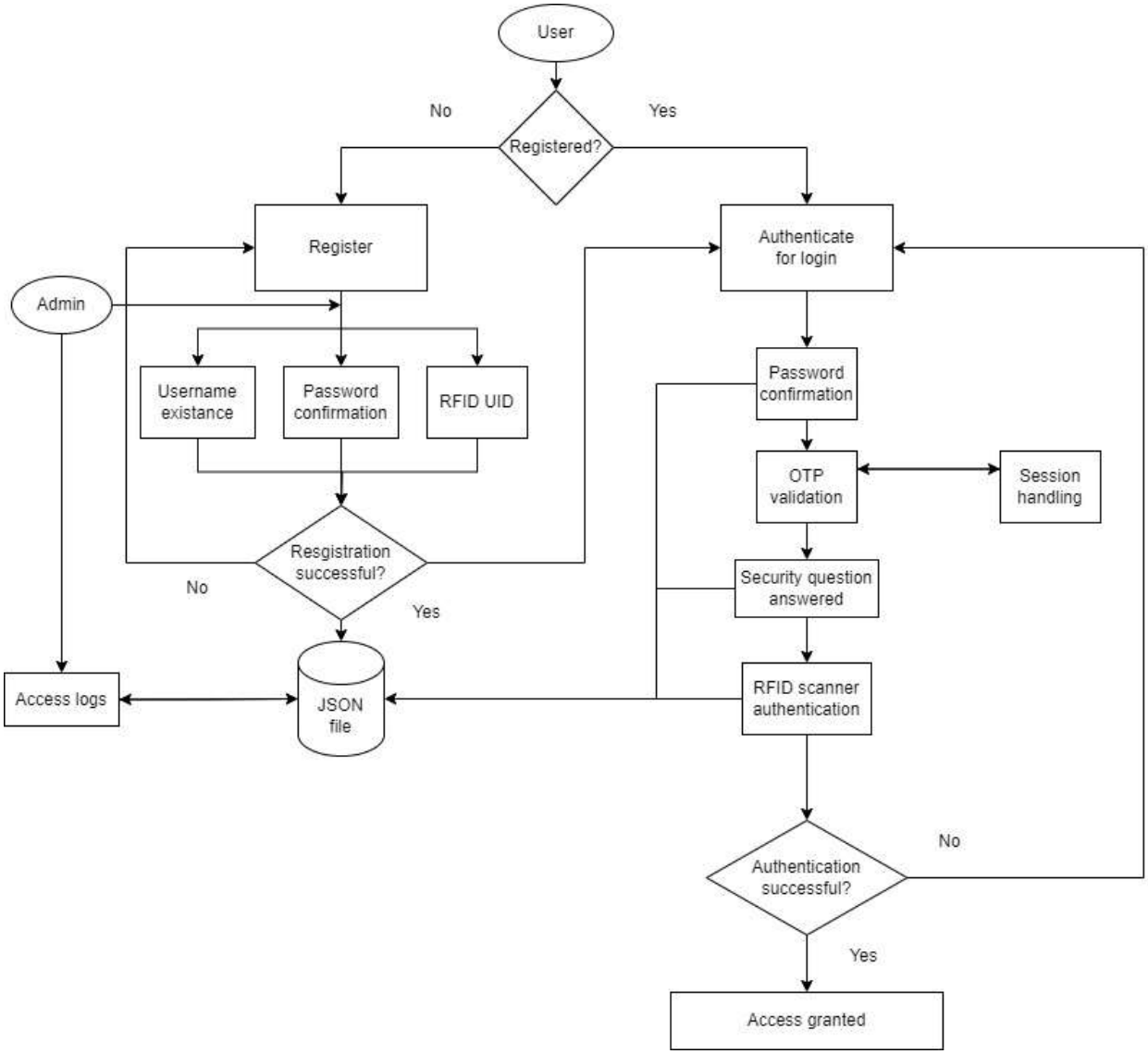
4. **Security Concerns in Wireless Communication:** While the paper addresses security concerns in RFID communication, it does not extensively discuss potential vulnerabilities in the wireless transmission environment.

5. **Assumption of Standardized RFID Technology:** The roaming functionality assumes the use of the same frequency and standard of RFID technology across different service providers, which may not always be the case in diverse systems.

Chapter 3

Project Design

This chapter provides a comprehensive overview of the logical background, user flow structures, and user cases underlying the authentication system development. It outlines the foundational concepts, illustrates the flow of interactions within the system, and delineates various user scenarios to guide the design and implementation process.



3.1 Logical Background

1. **Authentication Workflow**:
    - The system orchestrates a sequential process for user authentication, starting from registration and extending to login, password reset, and user deletion.
    - This logical workflow ensures that each user interaction follows a predefined sequence, enhancing the overall security and usability of the system.

2. **Multi-Factor Authentication (MFA):**
    - MFA is a security mechanism that requires users to provide multiple forms of identification to access their accounts.
    - In this system, MFA is implemented through a combination of password-based authentication, one-time passwords (OTPs), and RFID authentication.
    - By incorporating multiple layers of verification, the system mitigates the risk of unauthorized access and strengthens overall security.

3. **User Registration and Security Questions:**
    - During the registration process, users are prompted to select a security question from a predefined list and provide a corresponding answer.
    - Security questions add an additional layer of security beyond passwords by requiring users to provide personalized information that is typically known only to them.
    - This logical step helps prevent unauthorized access, especially in cases where passwords may be compromised.

4. **Password Management and Reset:**
    - Users have the option to reset their passwords in case they forget or need to change them.
    - The password reset process involves answering the security question chosen during registration, thereby verifying the user's identity.
    - This logical approach ensures that only authorized users can change their passwords, enhancing security and preventing unauthorized access to user accounts.

5. **User Activity Logging:**
    - The system logs user activities, including login attempts, password resets, and user deletions, in a dedicated log file.
    - User activity logging serves multiple purposes, including security monitoring, audit trail generation, and forensic analysis.
    - By maintaining a comprehensive record of user interactions, the system enables administrators to track user behavior, detect suspicious activity, and investigate security incidents.

6. **Error Handling and Validation:**
    - The system incorporates logical checks and validation mechanisms to ensure that user inputs are accurate and within expected parameters.
    - Error handling routines detect and gracefully handle invalid inputs, preventing system crashes and enhancing user experience.
    - Validation logic includes checks for input length, format, and content to mitigate common security vulnerabilities such as injection attacks and buffer overflows.

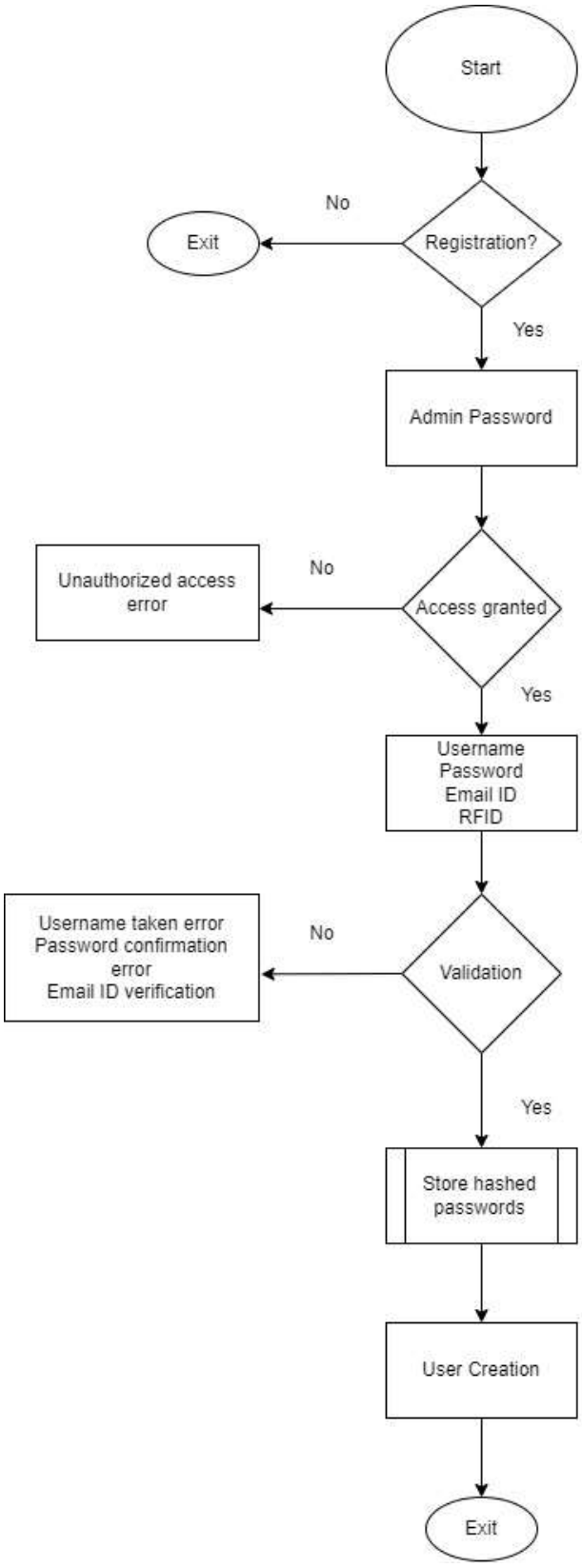
7. **Integration with External Devices:**
    - The system seamlessly integrates with external RFID readers for authentication purposes.
    - Logical protocols and communication standards facilitate reliable data exchange between the system and external devices.
    - Integration with RFID readers enhances security by enabling physical authentication factors, such as proximity cards or key fobs, to be used in the authentication process.
8. **Administrator Access Control:**
    - Certain operations, such as user deletion, require administrative privileges for execution.
    - Access control mechanisms enforce logical restrictions on administrative actions, ensuring that only authorized administrators can perform sensitive operations.
    - Authentication of administrators typically involves additional security measures, such as stronger passwords or multifactor authentication, to prevent unauthorized access to administrative functions.

9. **User Notification and Feedback:**
    - The system provides logical notifications to users regarding important events, such as password changes or successful logins.
    - Notifications may be delivered via email or displayed within the user interface, depending on the nature of the event and user preferences.
    - Feedback mechanisms enhance user awareness and engagement, fostering a transparent and user-friendly authentication experience.

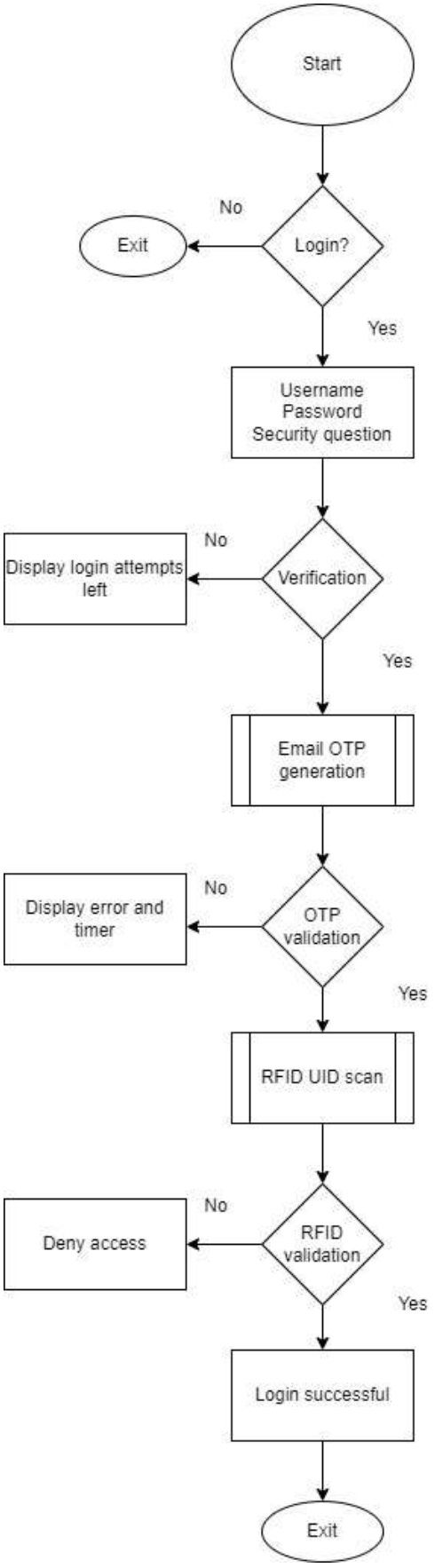
10. **Continuous Improvement and Security Updates:**
    - The system is designed to accommodate ongoing maintenance and security updates to address emerging threats and vulnerabilities.
    - Regular updates may include bug fixes, performance enhancements, and security patches to mitigate newly discovered vulnerabilities and improve overall system resilience.
    - Continuous improvement ensures that the system remains robust and secure in the face of evolving cybersecurity challenges and changing user requirements.

3.2 User Flow Structures

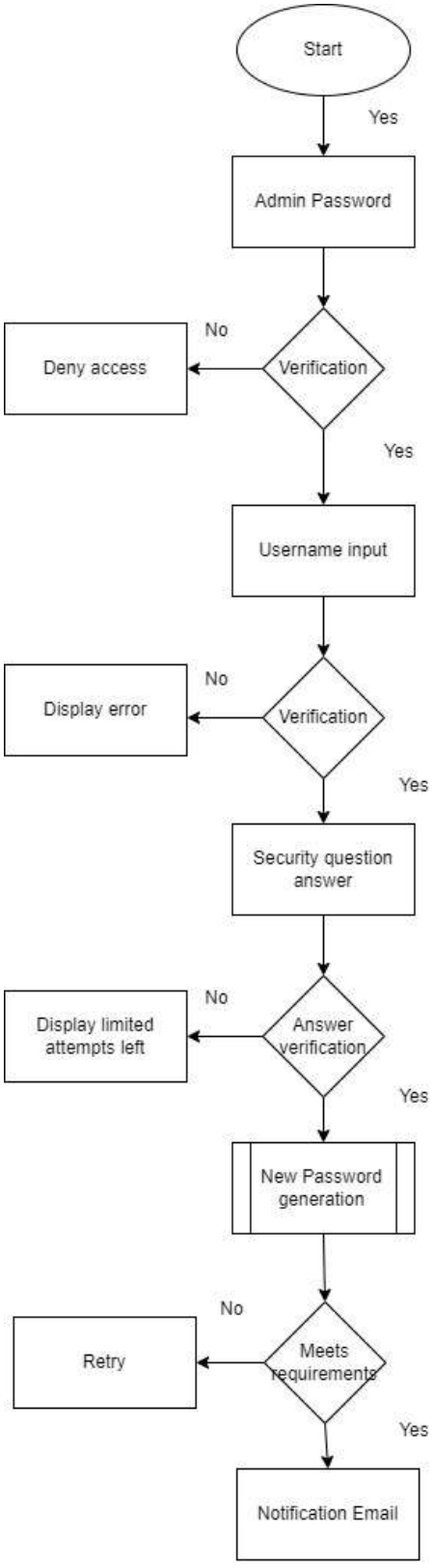
1. Registration Flow:



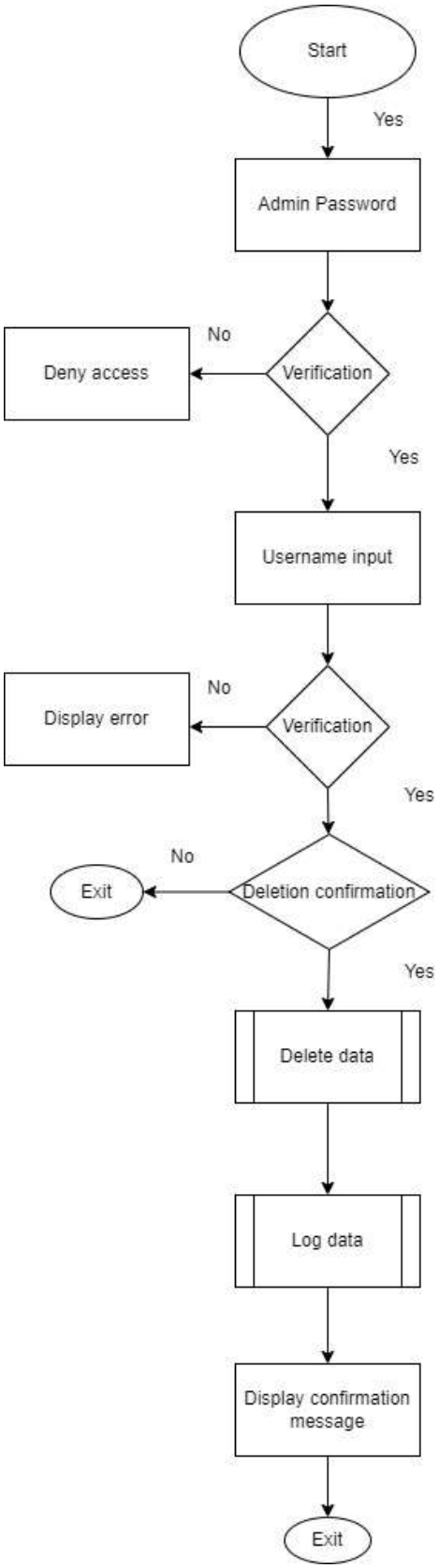
2. Login Flow:


Start
Login?
No
Exit
Yes
Username
Password
Security question
Verification
No
Display login attempts left
Yes
Email OTP generation
OTP validation
No
Display error and timer
Yes
RFID UID scan
RFID validation
No
Deny access
Yes
Login successful
Exit

3. **Reset Password Flow:**



4. **Delete User Flow:**



3.3 User Cases

1. **Register New User:**
   i. Actors: User, Admin
   ii. Preconditions: None
   iii. Postconditions:
   - User account is created with username, password, security question, email, and RFID UID stored securely.
   - Log entry is created for user registration.

2. **Login:**
   i. Actors: User
   ii. Preconditions: User account exists
   iii. Postconditions:
   - If successful:
     User is authenticated through three factors (password, OTP, RFID).
     Log entry is created for successful login.
     Login notification email is sent.
     System opens a YouTube link (if implemented).
   - If unsuccessful:
     Error message is displayed to the user.

3. **Reset Password:**
   i. Actors: Admin, User
   ii. Preconditions:
   - Admin: None
   - User: User account exists
   iii. Postconditions:
   - User's password is reset based on admin verification and security question answer.
   - Reset notification email is sent to the user.
   - Log entry is created for password reset.

4. **Delete User:**
    i. Actors: Admin
    ii. Preconditions: Admin is logged in.
    iii. Postconditions:
        - User account is deleted securely.
        - Log entry is created for user deletion.
        - Confirmation message is displayed to the admin.

Chapter 4

Implementation

The chapter offers a concise overview of the libraries and functions utilized in the project, highlighting their roles and functionalities. Additionally, it includes screenshots showcasing the program's output, providing visual insights into its execution and user interactions.

4.1 Libraries Used

1. **Python Libraries**

i. random:

Used for generating random numbers, particularly for generating one-time passcodes (OTPs).

ii. smtplib:

Enables sending emails via Simple Mail Transfer Protocol (SMTP), essential for sending OTPs and password reset notifications.

iii. email.mime.text.MIMEText:

Part of the email module, facilitates creating email messages with plain text content.

iv. hashlib:

Provides secure hash and message digest algorithms, utilized for hashing passwords before storage.

v. serial:

Allows communication with serial ports, used for interfacing with an RFID card reader.

vi. webbrowser:

Used for opening URLs in web browsers, utilized for automatically opening a designated link upon successful authentication.

vii. json:

Enables encoding and decoding JSON data, utilized for reading and writing user data to JSON files.

viii. stdiomask:

Provides functionality for masking user input, particularly useful for password entry to enhance security.

ix. datetime:

Facilitates working with dates and times, used for timestamping activities in the log file.

x. re:

Provides support for regular expressions, used for password validation.

2. Arduino Libraries

i. SPI:

The Serial Peripheral Interface (SPI) library provides functions for communicating with devices that support the SPI protocol. In this context, it facilitates communication between the Arduino board and the RFID (Radio-Frequency Identification) reader module.

ii. MFRC522:

This library is specifically designed for interfacing with MFRC522-based RFID reader modules. It simplifies the process of reading data from RFID tags or cards and allows the Arduino to interact with them seamlessly. The MFRC522 library abstracts the low-level details of communication with the RFID reader, making it easier to integrate RFID functionality into Arduino projects.

4.2 Functions Used

i. load_users():
Loads user data from a JSON file.

ii. save_users(users_data):
Saves user data to a JSON file.

iii. log_activity(activity):
Logs activity to a log file with a timestamp.

iv. masked_input(prompt):
Prompts the user for input without displaying it on the screen.

v. validate_password(password):
Validates a password based on specified criteria.

vi. hash_password(password):
Hashes a password using SHA-256 algorithm.

vii. register_user():
Registers a new user by collecting relevant information.

viii. send_email(receiver_email, subject, message_body):
Sends an email with specified content to a given recipient.

ix. send_otp(receiver_email):
Sends a One-Time Password (OTP) to a user's email address.

x. reset_password():
Resets a user's password after verifying security question.

xi. delete_user():
Deletes a user account.

xii. send_login_notification(username):
Sends a notification email when a user logs in.

xiii. authenticate_user():
Authenticates a user based on username and password.

xiv. verify_otp(stored_otp, receiver_email):
Verifies a One-Time Password entered by the user.

xv. verify_rfid(authenticated_username):
Verifies RFID card scanning for user authentication.

xvi. is_authorized_card(scanned_uid, expected_uids):
Checks if a scanned RFID card is authorized.

xvii. view_registered_users():

Displays a list of registered user names.

xviii. main():

Main function controlling the flow of the program.

4.3 Results

i. Registration

```
------------------------------------------------------------------------------------------------------------------------
                                    Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 1
------------------------------------------------------------------------------------------------------------------------
                                                  Registration
------------------------------------------------------------------------------------------------------------------------
Enter Admin Password: *****
------------------------------------------------------------------------------------------------------------------------

Enter a Username: test
Enter a Password: ***********

Select a Security Question:
1. What is the name of your first school?
2. What is your mother's name?
3. In which city were you born?
4. What is your first cars name?
5. What is your favourite movie?
6. What is the name of your first pet?
Enter the number corresponding to your chosen question: 3
Security Question: In which city were you born?
Answer: ******

Enter your Email Address: vedansh.avlani@gmail.com

Enter RFID UID (comma-separated hex values without spaces): 0A,65,DF,C4

Registration successful!
------------------------------------------------------------------------------------------------------------------------
```

ii. Login

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 2
------------------------------------------------------------------------------------------------------------------------

                                                First Stage
------------------------------------------------------------------------------------------------------------------------
Enter your Username: test2
Enter your Password: ***********

Authentication Successful! Proceed to the Second Stage.

                                                Second Stage
------------------------------------------------------------------------------------------------------------------------
---------------------------------
| Email with OTP sent Successfully |
---------------------------------
Enter the OTP you received: ******

OTP Verified Successfully!

Proceed to the Third Stage (RFID authentication).

                                                Third Stage
------------------------------------------------------------------------------------------------------------------------

Place the RFID Card near the Reader
RFID recognized! Authentication Successful.

------------------------------------------------------------------------------------------------------------------------
   Congratulations! All stages of Authentication Passed Successfully.
------------------------------------------------------------------------------------------------------------------------
```

iii. Password Reset

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 3
------------------------------------------------------------------------------------------------------------------------

                                                Password Reset
------------------------------------------------------------------------------------------------------------------------
Enter Admin Password: *****
Enter the Username: vedansh
What is the name of your first school?: *****
Enter a New Password: ***********
Re-enter the New Password: ***********
Password Reset Successfully
```

iv. Delete User

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 4
------------------------------------------------------------------------------------------------------------------------

                                                Delete User
------------------------------------------------------------------------------------------------------------------------
Enter Admin Password: *****
Enter the Username to delete: test
User 'test' deleted successfully.
```

v. List of Registered Users

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 5
------------------------------------------------------------------------------------------------------------------------


                                              Registered Users
------------------------------------------------------------------------------------------------------------------------
Registered Usernames:
- vedansh
- test
- test2
- test3
- test4
```

vi. Activity Log Book

log_book.json > ...

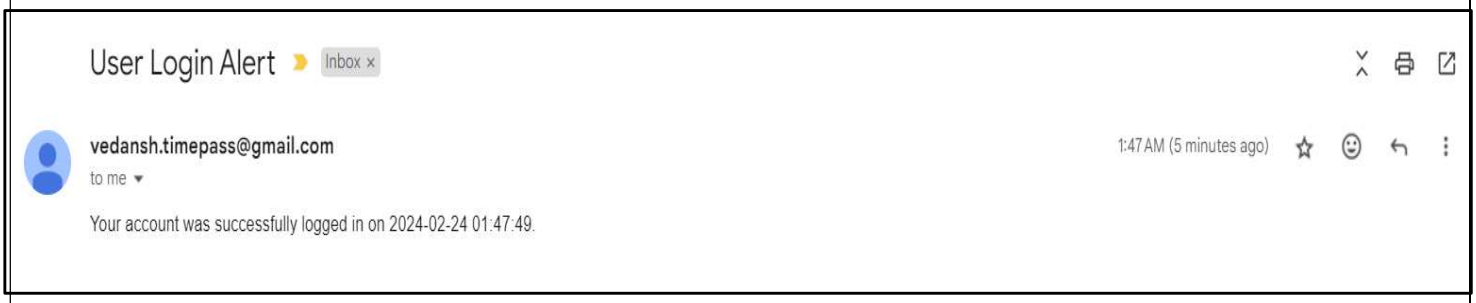

```
{"timestamp": "2024-02-24 01:24:39", "activity": "New user registered: vedansh"}
{"timestamp": "2024-02-24 01:29:19", "activity": "New user registered: test"}
{"timestamp": "2024-02-24 01:35:09", "activity": "New user registered: test2"}
{"timestamp": "2024-02-24 01:38:05", "activity": "New user registered: test3"}
{"timestamp": "2024-02-24 01:40:03", "activity": "New user registered: test4"}
{"timestamp": "2024-02-24 01:42:31", "activity": "Password reset for user: vedansh"}
{"timestamp": "2024-02-24 01:47:53", "activity": "User logged in: test2"}
{"timestamp": "2024-02-24 01:52:31", "activity": "User logged in: test4"}
{"timestamp": "2024-02-24 01:55:32", "activity": "User logged in: vedansh"}
{"timestamp": "2024-02-24 01:56:24", "activity": "User logged in: test3"}
{"timestamp": "2024-02-24 02:04:15", "activity": "User 'test' deleted by admin."}
```


vii. Users File

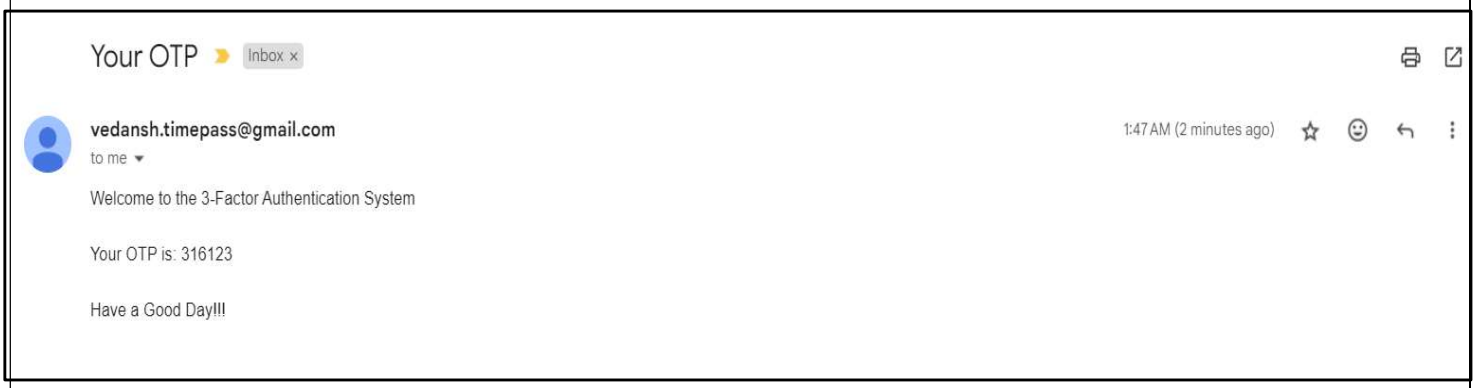

```
"test2": {
    "password": "4e4bdfacd8c157653b68361d1ce163d76393aeaea753737ea97c48b4d5a66aa0",
    "security_question": "What is your mother's name?",
    "security_answer": "7e7ac11c6033a6b84f9cfd10bbf3f33ee00ef6948a874ffa00b9787c725ffc0f",
    "receiver_email": "vedansh.avlani@gmail.com",
    "rfid_uid": [
        "AA",
        "C1",
        "14",
        "C5"
    ]
},
```


viii. Password Reset Alert Email

ix. Login Alert Email



x. OTP for Login Email



xi. First Stage Authentication Failure

```
-----------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
-----------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 2
-----------------------------------------------------------------------------------------------------------------------

                                                First Stage
-----------------------------------------------------------------------------------------------------------------------
Enter your Username: test
Enter your Password: ***********
Invalid Password.

Authentication Failed.
```

xii. Second Stage Authentication Failure

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 2
------------------------------------------------------------------------------------------------------------------------

                                                First Stage
------------------------------------------------------------------------------------------------------------------------
Enter your Username: test
Enter your Password: ************

Authentication Successful! Proceed to the Second Stage.

                                                Second Stage
------------------------------------------------------------------------------------------------------------------------
----------------------------------
| Email with OTP sent Successfully |
----------------------------------
Enter the OTP you received: ******

Invalid OTP. Authentication Failed.

Authentication Failed.
```

xiii. Third Stage Authentication Failure

```
------------------------------------------------------------------------------------------------------------------------
                                Welcome to the 3-factor authentication system.
------------------------------------------------------------------------------------------------------------------------

1. Register a New User
2. Login
3. Reset Password
4. Delete User
5. View Registered Users
6. Exit
Enter your Choice : 2
------------------------------------------------------------------------------------------------------------------------

                                                First Stage
------------------------------------------------------------------------------------------------------------------------
Enter your Username: test
Enter your Password: ************

Authentication Successful! Proceed to the Second Stage.

                                                Second Stage
------------------------------------------------------------------------------------------------------------------------
----------------------------------
| Email with OTP sent Successfully |
----------------------------------
Enter the OTP you received: ******

OTP Verified Successfully!

Proceed to the Third Stage (RFID authentication).

                                                Third Stage
------------------------------------------------------------------------------------------------------------------------

Place the RFID Card near the Reader
Invalid RFID card. Access denied.

Authentication Failed.
```

Chapter 5

Conclusion and Further Work

This chapter highlights the project's main outcomes, underscoring the importance of the authentication system in bolstering security with user-friendly features. It also identifies potential future enhancements to further strengthen the system and adapt to evolving cybersecurity landscapes.

5.1 Conclusions

In conclusion, the development of the multi-factor authentication (MFA) project, integrating password verification, OTP via email and RFID tag scanning, has been successfully implemented to enhance the security measures for authentication. By combining these authentication factors, we have created a more resilient system that significantly reduces the risk of unauthorized access and provides a robust mechanism. Along with the basic password verification, a dynamic authentication element is offered via OTP sent through the registered email. RFID tags add a tangible layer of security which has valuable uses in real time interaction for physical access control. The implementation of this project in python and Arduino provides a seamless integration between the software and hardware components of the system contributing to a robust and holistic security system.

5.2 Future Work

To address the limitations identified, future work should focus on enhancing both the security and user experience aspects of the MFA system. The following recommendations provide a roadmap for future development:

- Multiple RFID Scanners:
  Integrate support for multiple RFID scanners to eliminate the single point of failure. This enhancement will distribute the authentication process across multiple devices, enhancing overall system resilience.

- Automated RFID Tag Registration:
  Develop an automated registration process for RFID tags to streamline user onboarding. This could involve implementing a user-friendly web interface or mobile application for users to register their RFID tags securely.

- Biometric Authentication:
  Consider incorporating biometric authentication methods, such as fingerprint or facial recognition, to further enhance security. Biometrics provide an additional layer of personalization and can complement existing authentication factors.

- Mobile Application Integration:
  Develop a mobile application that allows users to receive OTPs and manage their authentication settings more conveniently. This can improve the overall user experience and provide a centralized platform for users to interact with the MFA system.

- Continuous Monitoring and Analytics:
  Implement continuous monitoring and analytics to detect and respond to suspicious activities. By incorporating machine learning algorithms, the system can learn and adapt to new threats, providing a more proactive approach to security.

- Scalability:

  Consider the scalability of the system to accommodate a growing user base. This involves optimizing the architecture and infrastructure to handle increased registration and authentication requests efficiently.

List of References

[1] Kennedy, W., & Olmsted, A. (2017). Three factor authentication. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST).

[2] Wahyudono, B., & Ogi, D. (2021). Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System. 2020 International Conference on ICT for Smart Society (ICISS).

[3] Gabsi, S., Kortli, Y., Beroulle, V., Kieffer, Y., & Belgacem, H. (2022). Adoption of a Secure ECC-based RFID Authentication Protocol. 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT).

[4] Y. Wang, J. Shen, X. Guo and W. Dong, "Research on RFID attack methods," 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China.

[5] C. -H. Huang and S. -C. Huang, "RFID systems integrated OTP security authentication design," 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, Kaohsiung, Taiwan.

Glossary

1. Authentication: The process of verifying the identity of a user or system before granting access.
2. Multifactor Authentication (MFA): A security mechanism that requires users to provide two or more forms of verification to access a system.
3. One-Time Passcode (OTP): A temporary code generated for authentication purposes, typically valid for a single login session.
4. RFID (Radio-Frequency Identification): A technology that uses radio waves to identify and track tags attached to objects or individuals.
5. Username: A unique identifier chosen by a user to access a system or service.
6. Password: A secret combination of characters used to authenticate a user's identity.
7. Hashing: The process of converting input data into a fixed-size string of characters, often used for storing passwords securely.
8. Security Question: A predefined question used for verifying a user's identity, commonly used in password recovery processes.
9. SMTP (Simple Mail Transfer Protocol): A protocol used for sending and receiving email messages over the internet.
10. SPI (Serial Peripheral Interface): A synchronous serial communication interface used to connect microcontrollers and peripheral devices.
11. MFRC522: A RFID reader/writer module commonly used in RFID-based projects.
12. JSON (JavaScript Object Notation): A lightweight data interchange format used for storing and transmitting data between a server and a web application.
13. Penetration Testing: A method of evaluating the security of a system by simulating real-world attacks.
14. Vulnerability Assessment: The process of identifying and prioritizing security vulnerabilities in a system or network.