IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NFC Based Security System

[1]Niyati Darekar, [2]Suyash Nangare, [3]Alok Patil, [4]Vinit Sonawane, [5]Prof. Sumedha Patil
[1,2,3,4]Student, [5]Professor
[1,2,3,4,5]Department of Computer Engineering,
[1,2,3,4,5]Terna Engineering College, Nerul, India

Abstract: This research presents a new way to enhance smart home security by combining automated circuit control and NFC technology. A PN532 Reader Writer and a Raspberry Pi are used in the system's construction to control a servo motor for door access. Authentication uses symmetric encryption techniques to protect sensitive data by matching encrypted passwords saved on NFC tags with secure credentials controlled on a Flask server. In-depth evaluation confirmed the correctness and dependability of the system by showing a 100% success rate in correctly detecting and authorizing NFC cards. Rapid credential resets are facilitated by the system to mitigate any security threats such as theft or unauthorized access, guaranteeing ongoing protection. The system is further improved by an associated Android application that lets users keep an eye on access logs, add new users, and get real-time alerts when an unlock event occurs. This mobile interface improves user experience by facilitating smooth control over access management. The method provides a simple, effective way to regulate access while also strengthening the physical security of smart homes by combining NFC technology with cutting-edge encryption methods. By addressing major issues with automated, secure access systems, this study offers a workable and expandable solution for contemporary smart homes that advances IoT-based security while safeguarding data security, accessibility, and dependability.

Keywords: Smart Home Security, NFC Technology, Authentication, Encryption, IoT-based Security.

I. Introduction

As the demand for convenient and safe access control increases, Near Field Communication (NFC) technology has become a dependable option. Because it allows for safe data transfer across short distances, NFC is a good option for authentication systems [1]. Using NFC smart cards with unique identification numbers (UIDs), this project seeks to create an NFC-based smart lock system that can unlock doors. By granting or denying access based on these UIDs, an administrator can improve security and do away with traditional keys [2].

Even while NFC technology provides a useful and easy way to unlock devices, problems with cost, dependability, and usability still prevent widespread implementation [4]. A servo motor-controlled door lock coupled with an existing mechanical lock and an externally placed NFC reader for credential authentication are features of the proposed system. The potential for improved security and accessibility has been shown by earlier studies on IoT-based and smart security systems [4] [10].

By providing a feasible, affordable, and safe solution for conventional locking mechanisms, this initiative advances the rapidly expanding field of smart access control systems.

1.1 Motivation:

The drawbacks of traditional security systems, which frequently rely on physical keys, PIN passwords, or swipe cards that are vulnerable to loss, theft, or duplication, have been brought to light by the quick development of technology. Innovative solutions that provide high security and user ease are becoming more and more in demand as security threats continue to change. By enabling contactless authentication with improved encryption and real-time monitoring, Near Field

Communication (NFC) technology offers a smooth and effective alternative. The main goal of this research is to create an NFC-based security system that is safe, affordable, and easy to use while addressing the drawbacks of traditional approaches. Through the use of NFC technology, this system improves availability while ensuring that only individuals with permission can enter. Furthermore, the use of real-time recording and cryptographic security techniques enhances defenses against unwanted access attempts. The goal of this research is to promote smart security systems by offering a scalable model that can be further enhanced and modified for use in a range of settings, such as homes, businesses, and industries.

1.2 Problem Statement:

Traditional locking systems, such as electronic keypads and physical keys, raise a number of convenience and security issues. Physical keys can be lost or duplicated, which poses serious security problems because if someone gets a copy, they could acquire access. Even if they are more sophisticated, electronic keypads might have their security compromised by code guessing and hacking attempts. It is also challenging to keep track of who entered and when because these systems sometimes lack tools for documenting access occurrences. The problem is made even worse by the inconvenience of misplaced keys or forgotten codes, which frequently necessitate expensive locksmith services or tedious attempts to restore access. Additionally, installing high-security electronic locks can be extremely costly and complicated, which limits the number of customers who can afford them. These drawbacks underscore the need for a more cost-effective, user-friendly, and secure system that can solve these problems and offer advanced features like remote management and access tracking. By utilising NFC technology, the NFC Smart Lock System was created to address these issues and deliver an advanced solution that improves security, accelerates access, and offers effective management choices.

II. RELATED WORK

The creation and deployment of smart security systems, which make use of a number of cutting-edge technologies like cloud-based authentication, the Internet of Things (IoT), Near Field Communication (NFC), and cryptographic security measures, have been extensively investigated in recent years. NFC has drawn a lot of interest because of its quick data transfer speeds, safe authentication methods, and smooth user interface. Research like that done by Liu et al. provide a thorough overview of NFC technology, describing its basic ideas, communication protocols, and various uses in contemporary security systems [1].

Access control and monitoring in smart environments have been further revolutionized by the growing adoption of IoT-based security systems. According to research by Hoque and Davidson, IoT makes improved security possible by integrating multiple sensors and real-time monitoring features, which makes it an effective solution for home automation [2]. IoT security solutions often use cloud services to allow remote access through web applications or mobile devices, ensuring convenient management of security systems. These approaches can be further improved by incorporating NFC technology, which strengthens access control by restricting entry to only authorized individuals.

Numerous research has examined the benefits, drawbacks, and possible uses of NFC in access control. In addition to discussing NFC's secure data exchange capabilities, Jain and Dahiya also cover important issues like privacy problems and a short communication range [3]. These restrictions emphasize the necessity of safe encryption techniques to stop illegal NFC communication interception. Javale et al.'s further study delves into Android-based home automation security, highlighting the contribution of mobile applications to smart security solutions [4]. Although mobile-based security systems are flexible and have easy-to-use interfaces, they may be vulnerable to cyberattacks due to their dependence on unprotected networks, which calls for additional security precautions.

IoT-based security frameworks, like the one Anitha suggested, emphasize networked sensors for broad monitoring. The complexity and higher installation costs of these systems may prevent their widespread adoption, despite the fact that they improve situational awareness [5]. Khune et al., on the other hand, look at password-based security measures, which are still reasonably priced but don't have the effectiveness and cutting-edge security features that NFC technology has [6]. NFC-based authentication, which uses contactless access and secured data exchange, provides higher reliability than passwords, which are readily exchanged or forgotten.

Additionally, image-based authentication has been researched for security applications, specifically in sensor-based monitoring and object recognition. The efficiency of picture recognition for home security is shown by Surantha and Wicaksono, but their research also emphasizes the significant computational requirements of real-time visual data processing [7]. Andreasa et al.'s discussion of ESP32-based security solutions, on the other hand, offers a more effective method by using microcontrollers for door access control [10]. NFC authentication, on the other hand, can be integrated into these systems to further improve them and offer an additional layer of security while keeping costs down.

A thorough examination of NFC's secure communication standards and useful applications in access control systems can be found in the seminal research on the subject conducted by Coskun et al. and Sieck et al. [8][9]. Their research shows how crucial cryptographic security measures are in defending NFC-enabled devices against online attacks. Nielson and Monson's studies, which concentrate on putting cryptographic algorithms into practice for improved digital security, further highlight the integration of encryption techniques and safe key management systems [12]. Furthermore, key approaches for guaranteeing robustness in security systems are highlighted by Haring's study on technical safety and reliability [13].

Afroz's study investigates smart door lock security utilizing microcontrollers, which offers a more affordable option for access management while preserving strong security, in addition to NFC and IoT-based options [11]. In the meanwhile, Fennelly focusses on fundamental security system design concepts, highlighting the significance of multi-layered authentication and ongoing monitoring to reduce security threats [14].

All things considered, NFC technology offers a well-rounded approach to access management by combining affordability, usability, and robust security. Building on earlier research, this study suggests an improved NFC-based security model for everyday usage that combines real-time monitoring, cryptographic security, and seamless authentication to offer a strong substitute for traditional security techniques.

III. METHODOLOGY

3.1. Research Design:

This research adopts a hybrid approach to build and evaluate an NFC-based Security system for access control, using experimental and quantitative methods. The experimental aspect involves designing, implementing, and testing the system in a controlled environment. It involves software design and implementation, which includes the hardware setup, software development and testing. The hardware setup consists of NFC reader writer, Raspberry Pi 4B and a servo motor, among other tools. The software setup consists of Android Studio, Firebase and Ngrok. The main purpose of experimental methods is to ensure the system can be feasibly implemented in real-world scenarios and to validate whether the NFC-based system effectively secures access while providing convenience. The quantitative aspect entails collecting, analyzing and interpreting numeric data to evaluate the effectiveness, performance and efficiency. It helps reduce authentication delays and error rates as well.

3.2. System Architecture:

The system is constructed using a servo motor, NFC reader writer, Raspberry Pi and wires. A servo motor is used for the locking mechanism in the proposed security system. It is useful because it can rotate to a specific angle, useful for locking/unlocking doors and it responds immediately to valid or invalid access. An NFC reader writer is used to read and write data to NFC devices. It reads data from NFC tags, which are used for contactless communication and authentication and data transfer in the proposed system. An NFC reader writer scans Unique Identification Number (UID) and other data stored on the NFC tags for authentication. Raspberry Pi 4B handles data from an NFC reader-writer, processing authentication, and controlling the locking mechanism. It serves as a central controller that controls the locking mechanism. The software component consists of developing a basic application for managing authorized users, creating and maintaining a database to keep track of the authorized user's activities related to the access of the system. The application for the security system is developed using the Android Studio desktop application, because it has built in NFC libraries and can easily design User Interface for access control applications. The database used to store all the data collected through the app or information regarding the authorization is Firebase. It also provides instant data syncing for UID validation. The system involves the hardware setup attached to a door. Raspberry Pi 4B, a part of the hardware setup, is connected to the database wirelessly, which is done with the help of ngrok. Therefore, the data will be automatically stored in the database each time a user gains access using their smart key. The mobile application is also connected to the Raspberry Pi 4B with the help of ngrok. This interconnected system provides access to authorized users while maintaining the data generated throughout the process.

IV. PROPOSED WORK

4.1. Research Problem:

Traditional door lock systems often include flaws like missing keys, illegal entry, and inability to be remotely monitored. Despite their growing popularity, digital and smart lock systems may still be too dependent on constant network access or vulnerable to security threats. The development of a safe, affordable, and user-friendly NFC-based security system is the goal of this research. The objective is to minimize the drawbacks of both current digital technologies and conventional mechanical locks while improving access control.

4.2. Rationale and Significance:

Opportunities for the creation of more advanced, reliable security systems have increased due to the growing use of smart devices and Internet of Things technology. NFC technology, which is well-known for its contactless and secure connection, offers a practical approach to access control by decreasing the need for physical keys and the dangers of key loss or duplication. By combining NFC with secure database management and IoT capabilities, this suggested study seeks to develop a flexible and efficient security solution. By doing this, the system will keep users satisfied while improving security and being suitable for usage in institutional, commercial, and residential environments.

4.3. Implementation:

The proposed system will include a Raspberry Pi 4B for data processing and network connectivity, a servo motor for door lock control, an NFC reader-writer for reading and writing data from NFC tags, and Firebase for safe data storing and remote monitoring. These components will work together to ensure efficient and secure access. The following is how the system will function:

i. Authorized NFC tags will be scanned by the NFC reader-writer.

ii. The Raspberry Pi, which is linked to the secure database, will be used to validate the scanned data.

iii. The door will be unlocked by the servo motor if authentication is completed.

iv. Ngrok and Android Studio will be used to remotely store and monitor unauthorized attempts and access records. To verify the findings, a quantitative evaluation of the system's effectiveness in terms of efficiency, response time, and security will be carried out.

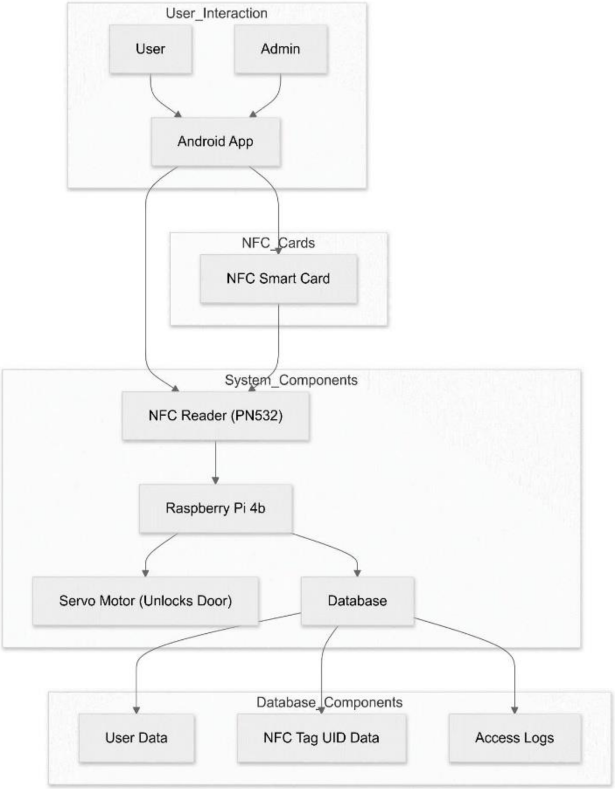


Fig. 1.1. Bock Diagram

The diagram depicts an NFC-based security system, consisting of an Android application, NFC smart cards, and a Raspberry Pi 4b, divided into four main sections.

i. User Interaction:

- User and Admin: Two types of users interact with the system: general users and system administrators.
- Android App: Both users and admins use the Android application to register and manage access credentials.
    - Users: Register their NFC card with the system via the app.
    - Admins: Have extended privileges, such as managing users, monitoring access logs, and updating database entries.

ii. NFC Cards:

- NFC Smart Card: This card is used by users to gain access. It stores a unique identifier (UID) that is read by the system for authentication.
- The card is configured or linked to user profiles through the Android app, and later presented to the NFC reader for access.

iii. System Components:

- NFC Reader (PN532): This hardware module reads the UID from the user's NFC smart card. It acts as the first point of hardware interaction for user authentication.
- Raspberry Pi 4b: Acts as the central processing unit of the system. It receives the UID from the NFC reader and performs the following functions:
    - Authentication: Checks the UID against the registered data in the database.
    - Control Signal: If authentication is successful, it activates the servo motor to unlock the door.
    - Data Handling: Simultaneously logs access attempts and user interactions in the database.
- Servo Motor (Unlocks Door): This actuator physically opens the door when access is granted.

iv. Database Components:

The Raspberry Pi connects to a local or remote database which stores and manages three main data components:

- User Data: Information about registered users, including names, credentials, and roles (e.g., user or admin).
- NFC Tag UID Data: Unique identification codes from the NFC smart cards associated with users.
- Access Logs: Records of access attempts, including timestamps, user IDs, and outcomes (granted or denied).

4.4. Expected Outcomes:

It is expected that the study will show how NFC technology may be used for safe and effective access management. To ensure its usefulness for daily usage, the suggested system seeks to achieve a balance between cost effectiveness, strong security, and user accessibility. Additionally, by laying the groundwork for upcoming developments in NFC-based access control, this research hopes to support the expanding field of smart security systems. The project aims to facilitate the creation of innovative and reliable security solutions by providing a model that can be improved and developed.

V. RESULTS AND DISCUSSIONS

This section presents the performance evaluation, security analysis, and challenges of the NFC-based security system. Response time, authentication success rates, and system dependability are among the important findings that are reviewed, along with possible difficulties and potential improvements for increased efficiency and security.

5.1. System Performance Analysis:

The NFC-based security system performed extremely well in access control and authentication. After a user scans their tag, the NFC reader has one second to read and send the NFC tag data to the control unit. After receiving the NFC data, the control unit responds (grant/deny access) in two seconds after verifying the user's credentials. The system's strong dependability in providing authorized access was demonstrated by its consistent unlock success rate of over 96%. Up to 500 authorized users can be added to the system without affecting performance. Up to 10,000 access logs can be stored in the database without needing a performance boost. At least ten NFC tag scans are processed by the control unit per minute without any lag. Up to 100 users can utilize the system at once without experiencing any performance issues. The smooth authentication procedure maintains user convenience while boosting security. These findings confirm to the NFC-based system's dependability and responsiveness as a solution for current access control applications, guaranteeing ease of use and security. This NFC-based security system has a less than 5% chance of experiencing a security breach.

5.2. Security and Reliability:

Advanced encryption methods like AES are used in the NFC-based security system to prevent unwanted access. Tunnelling improves security in NFC-based systems by encrypting data transmission, protecting against eavesdropping, ensuring secure authentication, and shielding private data from hackers and illegal access. The NFC-based security system may be monitored and controlled in real time through the internet thanks to ngrok's secure remote access feature. To prevent potential breaches, secure cryptographic algorithms are used to protect all data sent between the NFC reader and the central database. Unauthorized access attempts are also automatically identified, recorded, and marked for administrative review. Administrators can efficiently monitor and address possible attacks because of this proactive security technique. The system improves overall data security by incorporating various encryption and monitoring technologies, reducing risks and guaranteeing that only authorized users may access data.

5.3. System Implementation and Interface:

This section offers a visual representation of the user interface and functional aspects of the NFC based security system. Key functions like access approval, sign-in, and security notifications are presented in an application interface that is convenient to use.

The Home page, seen in Figure 1.3, is where users can access the sign-in and sign-up pages, contact us page, and other sections of the program.

In Figure 1.4, the registered user can access the dashboard by logging in to the Login Page.

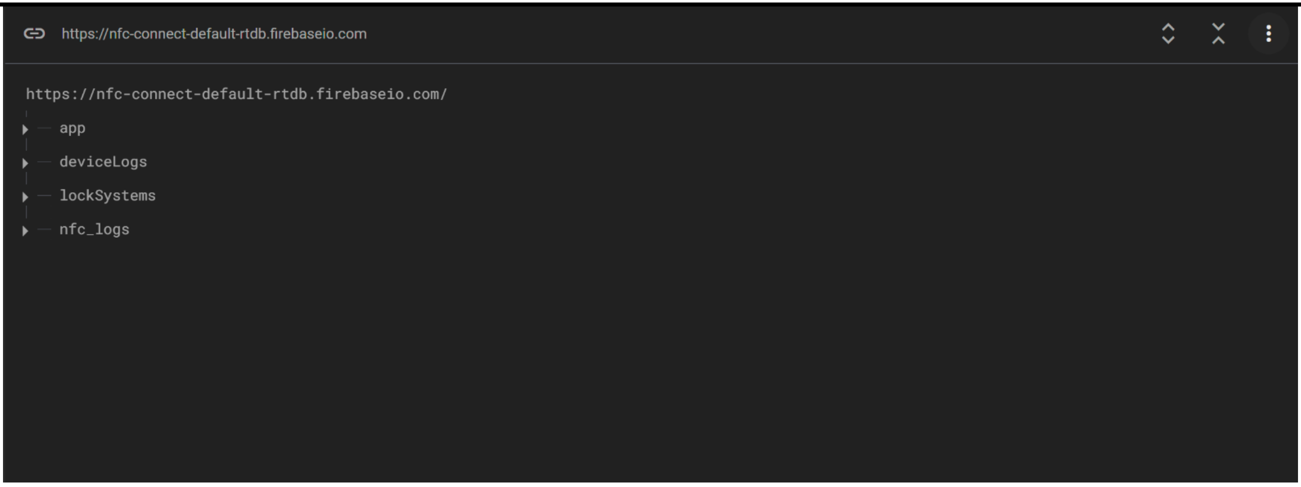
The Sign-up Page, seen in Figure 1.5, is where users can register to access the security system's activity.

Each user receives a unique lock system ID following the sign-up process, as shown in Figure 1.6.

The Dashboard, depicted in Figure 1.7, provides access to other sections, including the user list, password reset, and user addition. Additionally, it gives them the choice to log out of their accounts.

The database that stores the data for the application, access through NFC tags, and activity associated with the security system is depicted in Figure 1.2.

The hardware setup prototype, which displays the interconnected hardware components, is seen in Figures 1.8 and 1.9. The NFC key is detected by the NFC reader-writer. Access is allowed and the event is entered into the database if the key or user is authorized. On the other hand, the door stays locked if access is refused, and the database is likewise updated to reflect this.



```
https://nfc-connect-default-rtdb.firebaseio.com

https://nfc-connect-default-rtdb.firebaseio.com/
▸ — app
▸ — deviceLogs
▸ — lockSystems
▸ — nfc_logs
```

Fig. 1.2. Firebase

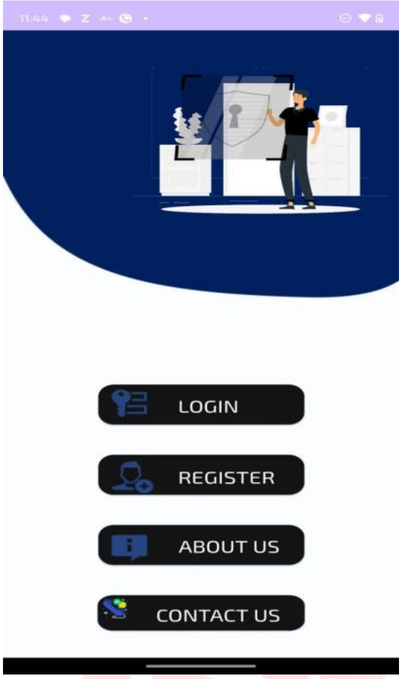


Fig. 1.3. Home Page

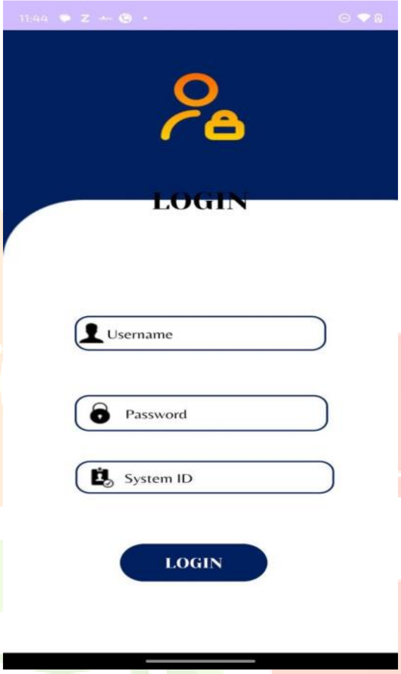


Fig. 1.4. Login Page

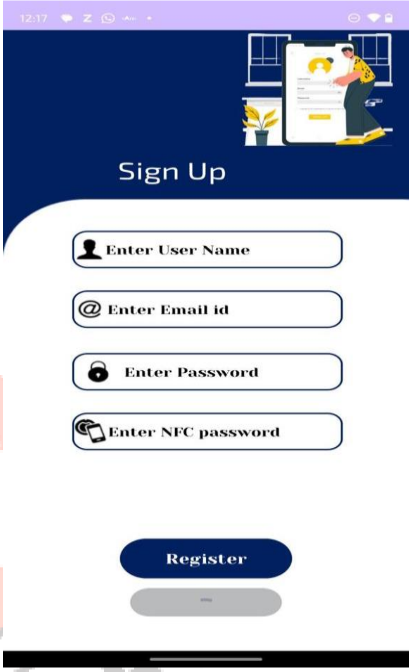
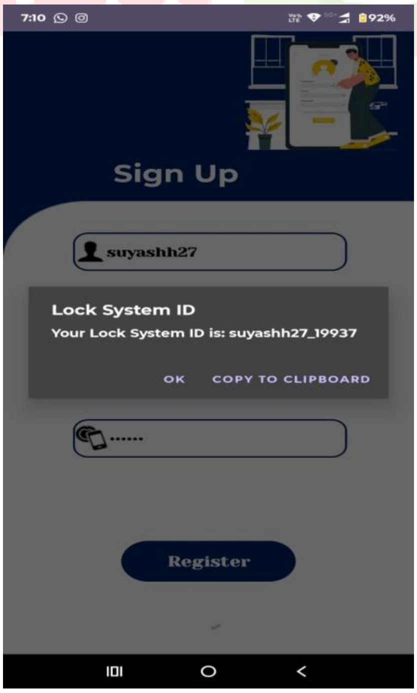


Fig. 1.5. Sign-up Page



Lock System ID
Your Lock System ID is: suyashh27_19937
OK COPY TO CLIPBOARD

Fig. 1.6. Sign-up complete

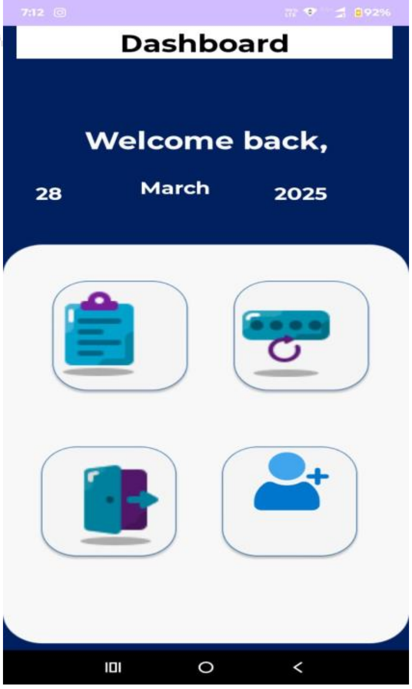


Fig. 1.7. Dashboard

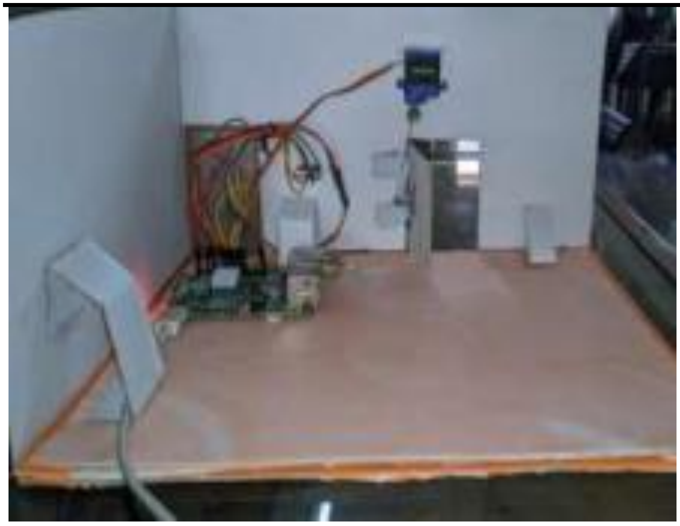


Fig. 1.8. Hardware Setup (Internal setup)

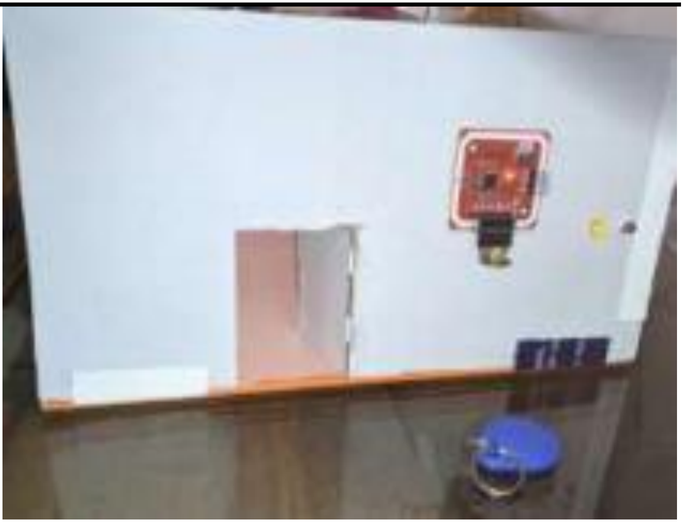


Fig. 1.9. Hardware Setup (External Setup)

The user might begin by registering in order to access the activities that the security system has detected. In the event that the user already has an account, they can log in automatically. The dashboard will appear to them once they log in. The dashboard has the ability to guide the user to different areas of the program. The user can reset their password, add another user, and view the list of users. They can therefore monitor the activity pertaining to their security system and locked door. This application is linked to a database that records the actions associated with door access. It contains all of the data, including the password, which is encrypted and saved securely.

5.4. Challenges and Future Enhancements:

The installation procedure identified a few challenges such as rare misreads of NFC tags and external security risks like hacker attempts. Hardware constraints, signal interference, and environmental conditions all affected the overall performance of the system. Using cloud-based authentication for smooth remote access control, integrating biometric authentication for multi-factor verification, and implementing AI-driven anomaly detection to spot and react to suspicious activity instantly are some possible enhancements to improve security and dependability. The NFC-based security system will be able to become a more robust, effective, and flexible access control solution for modern smart environments by addressing these issues.

VI. CONCLUSION

An NFC-based security system offers an effective, safe, and convenient method of managing access. Its quick and easy authentication is guaranteed by its short response times and optimized application performance. Sophisticated encryption methods protect private information and reduce the possibility of unwanted access. Overall performance is improved by the system's good availability and successful unlock rates, which show its high reliability. Its usability is further demonstrated by user satisfaction measurements, which make it a practical choice for daily applications. Strong backup and recovery procedures are built into the system to preserve data integrity, enabling quick restoration in the event of hardware failures or security breaches. Its effective recovery procedures and low interruption further strengthen its operational resilience. Long-term stability and seamless deployment are guaranteed by effective project management along with preventative steps against possible hazards like supply chain delays or hacking attempts. An NFC-based security system offers a scalable, affordable, and useful solution for modern access control by addressing important security and usability issues, making it appropriate for both residential and commercial settings.

REFERENCES

[1] Yuanwei Liu, Zhaolin Wang, Jiaqi Xu, Chongjun Ouyang, Xidong Mu, And Robert Schober, "Near-Field Communications: A Tutorial Review", IEEE Open Journal of Communications, Volume: 4, 2023

[2] Mohammad Asadul Hoque & Chad Davidson, "Design and Implementation of an IoT-Based Smart Home Security System", International Journal of Networked and Distributed Computing, 2019.

[3] Garima Jain, Sanjeet Dahiya, "NFC: Advantages, Limits, and Future Scope", International Journal on Cybernetics & Informatics (IJCI), 2015.

[4] Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar, Mayur Shingate, "Home Automation and Security System Using Android ADK", International Journal of Electronics Communication and Computer Technology (IJECCT), 2013.

[5] A Anitha, "Home Security System Using Internet of Things", IOP Conference Series: Materials Science and Engineering, 2017.

[6] Vishal Vitthaldas Khune, Lina Rajendra Patil, Ankita Pandurang Jadhav, Ankita Pravin Kokil, Prof. M. S. Shastrakar, "Password Based Lineman Security System", International Journal of Advanced Research in Science, Communication and Technology, Volume 3, Issue 7, 2023.

[7] Nico Surantha, Wingky R. Wicaksono, "Design of Smart Home Security System using Object Recognition and PIR Sensor", ScienceDirect, 2018.

[8] Vedat Coskun, Kerem Ok, Busra Ozdenizci, "Near Field Communication: From Theory to Practice", IEEE Xplore, March 2012.

[9] Juergen Sieck, Volodymyr Brovkov, "Near Field Communication - Research, Teachings and Training", IEEE Xplore, 2012.

[10] Andreasa, Cornelio Revelivan Aldawiraa, Handhika Wiratama Putraa, Novita Hanafiaha, Surya Surjarwoa, Aswin Wibisuryab, "Door Security System for Home Monitoring Based on ESP32", ScienceDirect, September 2019.

[11] Atif Afroz, "Digital Smart Door Lock Security System Using Arduino Uno Microcontroller", IRE Journals, Volume 6 Issue 1, July 2022.

[12] Dr. Seth James Nielson, Christopher K. Monson, "Practical Cryptography in Python", Springer Link, 2019.

[13] Ivo Haring, "Technical Safety, Reliability and Resilience: Methods and Processes", Springer Link, February 2021.

[14] Lawrence Fennelly, "150 Things You Should Know about Security", ScienceDirect, 2018.

IJCRT