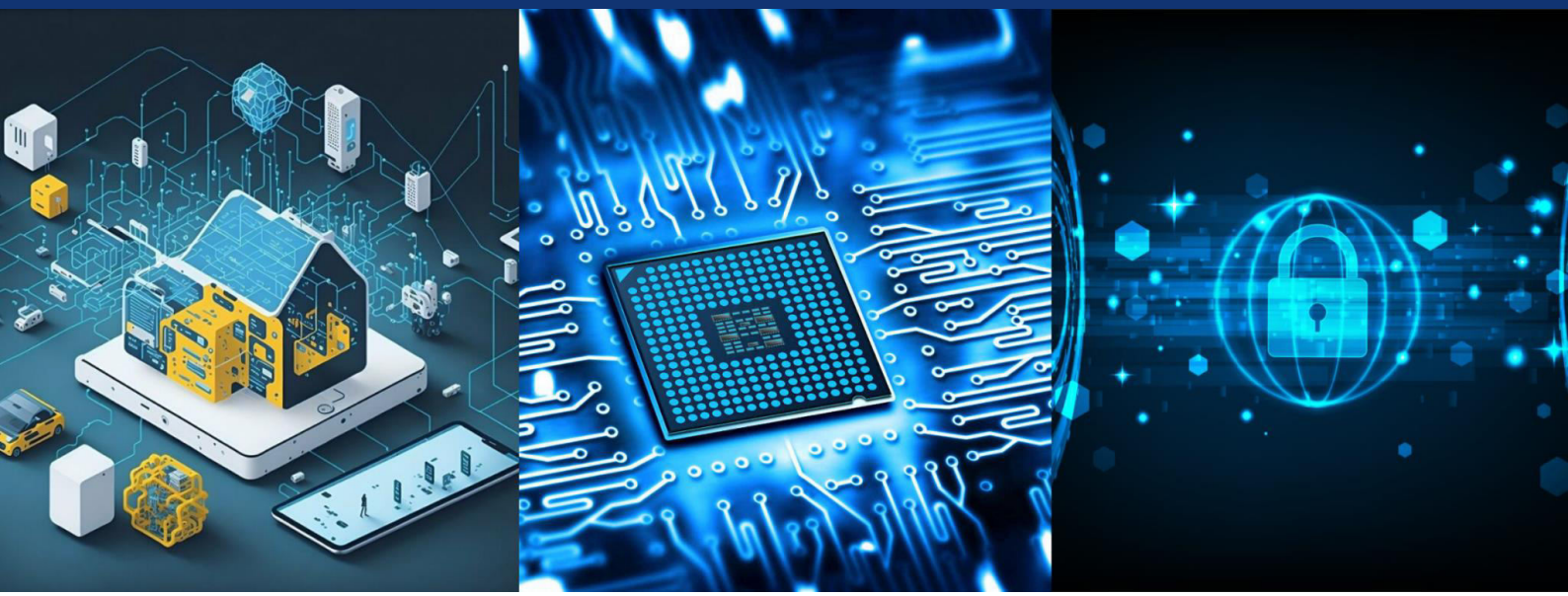
IJIRCCE

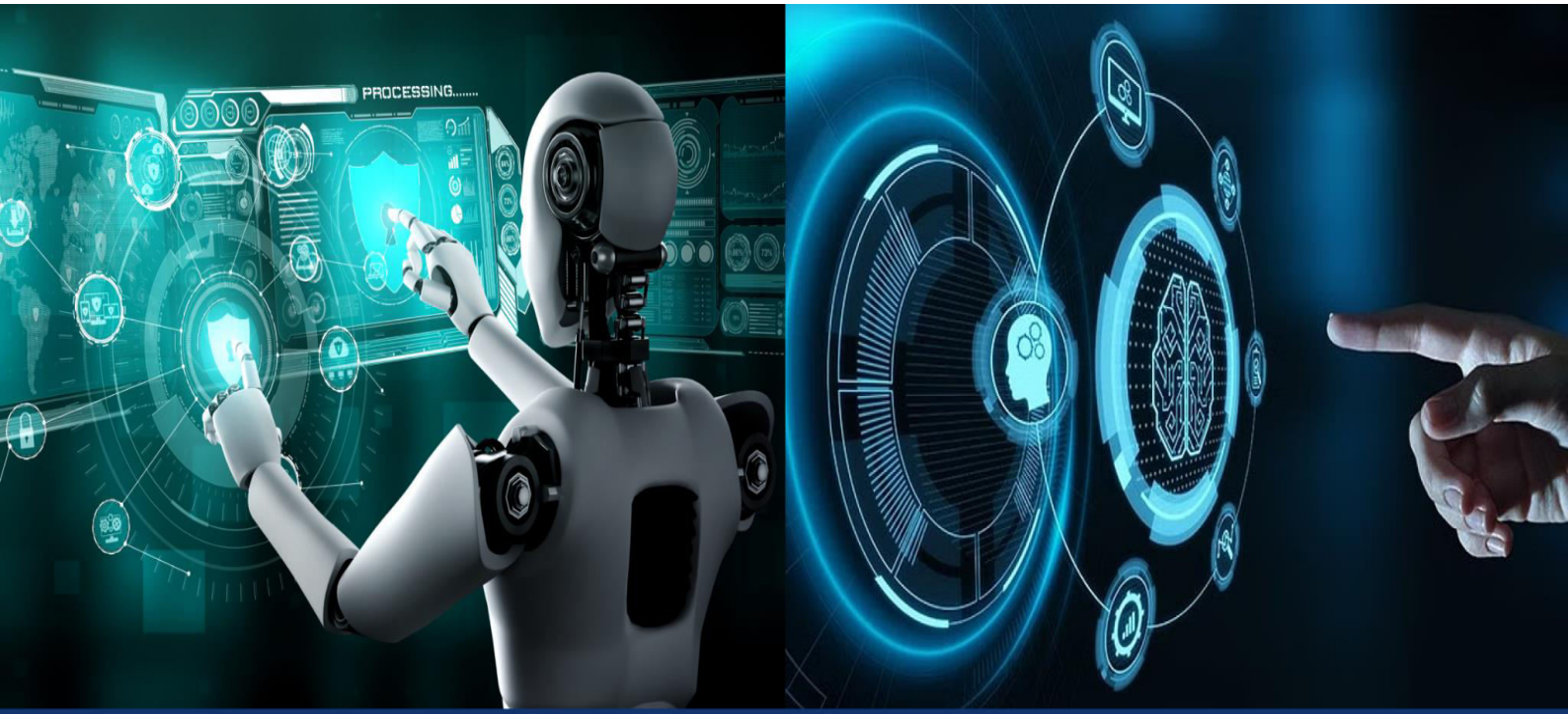
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304231

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Password-Based Lineman Security System

Prof. Sumedha Patil[1], Niyati Darekar[2], Suyash Nangare[3], Vinit Sonawane[4], Alok Patil[5]

Project Guide, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, India[1]

Students, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, India2-5

ABSTRACT: Password-Based Security Systems are elements of an authentication mechanism for controlling access into digital systems that are frequently used in your daily life. The user walks up to a digital system (computer/smartphone) and enters their privileged passcode that is verified by the confirmation methods of an encrypted version of their passcode. The security practice of how effective the password-based system is related to two independent cases of secured compliance, the strength of the password itself, and whether any other systems are in place such as hashing the password or salting the password. Password-based security systems are similarly weaker and vulnerable to unauthorized access using weak passwords, someone whom the user trusts, phishing, and brute force attacks. In order to mitigate these possibilities, security systems become more all-inclusive to include mandates of authorization using multi-factor authentication (MFA) in collusion with passwords. A Lineman Security System centers around the security of utility employees who are working on power lines. Therefore, this type of system is developed to help control linemen security and unauthorized access to critical electrical infrastructure. In order to engineer advance security spatial systems would be implemented using MFA devices, locking devices, access control mechanisms, cameras, data integration, the vision is to limit access, so only authorized utility workers have access, and limit unauthorized workers from tampering with electrical grid access that involve a lineman as active. This security system helps worker's safety and maintains reliability to the electric grid and electrical infrastructure. Even though this just described the first set of security systems employ distinct access, the meaning remains the same how effectively manage access to secure digital and bodily systems through security.

KEYWORDS: utility work, multi-factor authentication (MFA), Lineman Security System, smart locks, access control mechanisms, encryption, password hashing, salting.

I. INTRODUCTION

The circuit breaker is an essential part of electrical systems, preventing overloads and short-circuits. Nowadays, the conventional circuit breaker has been replaced by microcontroller-based circuit breaker. Microcontroller-based circuit breaker detects overload, short-circuits, and ground faults and allows for remote monitoring and control of the circuits. The password-based multi-microcontroller networking system is an easy-to-use system that employs multi-microcontrollers as a network to control and monitor multiple circuits. All data is shared with a password-based security system to ensure that only authorized personnel can control each individual circuit.The password-based multi-microcontroller networking system allows for remote monitoring and control, which is helpful when a user is not physically at the system site. Our system also offers real-time monitoring and fault detection; faults are detected real-time and addressed before any major issues arise. The system is highly reliable, efficient and scalable, allowing for updating by adding more circuits and microcontrollers when needed.

II. METHODOLOGY

Methodology used:

1. Research and Requirement Analysis

• Literature Review: Review of NFC-based security systems that exist or technical papers that develop research on NFC Applications to understand typical function/characteristics, user requirements and limitations.
• Stakeholder Consultation: Meet with potential users to acquire requirements and expectations of the user interface (UI).
• Define Objectives: Clearly define objectives for UI development. Focused usability, accessibility, and aesthetics.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304231

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. User Interface Design Plan/Wireframing

• Wireframing: Wireframes to visualize the layout of the application. This will include drawing out the most important screens and the associated flow of navigation. This ensures the person using the UI can do so in an intuitive manner.

• Prototyping: Obtain a LO-FI prototype to demonstrate UI. This will encourage early feedback and opportunity for iteration in the design phase.

• Usability Testing: After user engagement, conduct usability testing to obtain improvement feedback on navigation, design, and overall user experience.

3. User Interface (UI) Development

• Technology Stack Selection: Identify the relevant technologies and frameworks to involve in UI development e.g., Android ADK for mobile development.

• Implementation: Begin writing the code for every UI component based on the design specifications. This includes ensuring that the UI remains responsive and compatible on multiple device screen sizes.

.• Integration with NFC Functionality: Collaborate with the backend developers in implementing the NFC-enabled software components and user interfaces that can communicate with one another to support the NFC-related tasks for scanning and authentication.

4. Documentation

• Technical Documentation: Documenting the development processes, implementations, and design that were involved in the further development will help with directing future development.

• User Guide: A user guide will be created to explain to the users how to interact with and operate the coffee security system which relies on NFC technology.

III. LITERATURE REVIEW

[1] In their work titled "Design and Implementation of an IoT-Based Smart Home Security System," Mohammad Asadul Hoque and Chad Davidson present a practical approach to building a smart home security setup using affordable hardware like Raspberry Pi and Arduino. The system monitors door access using RF communication and stores events in a MongoDB database. Additionally, an Android app was developed to alert users of any suspicious activity, like unauthorized door openings. While the concept is effective and budget-friendly, there are a few downsides. The 433 Hz RF signal used can face interference from other household devices. The Android app is also quite basic and lacks advanced features like time zone handling or detailed data visuals. Moreover, the paper doesn't go into how well the system would scale for larger or more complex home setups.

[2] "NFC: Advantages, Limits, and Future Scope," authors Garima Jain and Sanjeet Dahiya explore the possibilities of Near Field Communication (NFC) technology. They highlight how NFC can make our daily tech interactions more seamless by enabling contactless payments, enhancing convenience, and improving security. While the paper does a good job covering the general benefits of NFC, it's more focused on theoretical discussion than real-world application. It lacks technical depth and doesn't offer many case studies. Also, it only briefly touches on potential security and privacy concerns, which are crucial areas that deserve deeper investigation. The authors suggest that more research is needed to address these issues and fully understand NFC's impact.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] "Home Automation and Security System Using Android ADK," authors Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar, and May present a cost-effective and adaptable home automation solution. Their research primarily focuses on making daily life easier for elderly and differently-abled individuals by helping them control household appliances more conveniently and securely. The system showcases how automation can significantly improve quality of life. However, the work mainly revolves around a basic prototype, and the control is limited to a few devices. It also lacks depth in terms of scalability and how it could integrate with systems beyond the Android platform, leaving room for improvement in future developments.

[4] "Home Security System Using Internet of Things," by A. Anitha, explores the use of IoT technology to develop an efficient home security setup. The system allows users to receive real-time alerts in case of break-ins and also offers the ability to control the alarm system remotely through a smartphone. The proposed solution proved to be user-friendly and effective in enhancing home security. On the downside, the paper doesn't discuss how well the system would perform in larger or commercial spaces. It also leaves out important aspects such as how to address potential security vulnerabilities and how to make the system more resilient to threats, which are crucial considerations in any IoT-based security setup.

IV. RESULTS AND DISCUSSION

In recent years, a number of IoT-based smart home systems have been proposed to improve residential security and automation. One such system is presented in the paper titled “Home Security System Using IoT”, where the authors developed a basic intrusion detection mechanism using a PIR sensor connected to a Node MCU. The setup sends intrusion alerts through the Blynk app to notify the user. While this approach is cost-effective and relatively easy to implement, it lacks any kind of user authentication or secure access control. The system focuses solely on motion detection and alerting, making it suitable for simple security needs but insufficient for more sensitive or high-risk environments.

Another notable project, “IoT-Based Smart Security and Home Automation System”, takes a step further by introducing facial recognition using a Raspberry Pi. This provides a visual authentication mechanism for controlling door locks. However, while facial recognition does enhance access control, the paper does not address data protection through encryption, nor does it incorporate any system to handle or prevent electrical faults. Furthermore, the scalability of the system is not clearly discussed, potentially limiting its practical implementation in larger home networks.

A third paper, titled “Smart Home Automation and Security System Using Arduino”, focuses on basic home automation and security using an Arduino Uno. This system uses PIR sensors for motion detection and allows some automation features via Bluetooth or Wi-Fi modules. Although it serves as a decent low-cost prototype for entry-level home automation, it lacks features such as secure user identification, remote access logs, or any kind of integration with electrical circuit protection mechanisms. Its limited processing power and lack of encryption make it vulnerable from a security standpoint.

The fourth system, described in “Real-Time Home Automation with Voice Command”, explores voice-based control through integration with Google Assistant and IFTTT. This setup allows users to control home appliances via voice commands, offering a user-friendly experience. However, the system lacks any kind of access authentication or protection against electrical mishaps. It also does not provide any logging or monitoring functionality, which are important in smart home environments where accountability and real-time feedback are crucial.

In contrast to the systems described above, the proposed project in this study provides a more advanced and secure framework by combining NFC-based authentication, encrypted password handling, and automated circuit control. The use of the PN532 NFC module allows users to unlock access points only through encrypted credentials, which are verified via a Flask server. This significantly improves security, especially when compared to systems that rely solely on motion or voice triggers. Furthermore, the integration of a multi-microcontroller circuit breaker system enables real-time detection of electrical faults such as overloads and short-circuits. These faults can be addressed immediately through remote commands, reducing the risk of electrical damage or fire hazards.

Another key strength of this project is its Android application, which serves as a centralized control hub. Through the app, users can receive real-time alerts, monitor access logs, and manage user credentials remotely. This not only improves user convenience but also ensures better control and tracking of access events. Moreover, the system is designed to be scalable: additional circuits and microcontrollers can be added as needed, allowing for expansion in larger home or building environments. Overall, the proposed system successfully fills several gaps observed in the referenced works by integrating security, safety, usability, and scalability into a single cohesive platform.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. CONCLUSION

A system based on NFC (Near Field Communication) access security is a secure and trustworthy way to manage access conveniently. It is trustworthy by providing fast and easy remote authentication, due to quick responsiveness to the program-optimized process. Sensitive data is protected by advanced encryption protocols while minimizing unauthorized access. High unlock cases and good availability maximize performance and make a level of reliable access control other users can achieve based on models of satisfaction. The system has consistent data backup and restoration practices to uphold data integrity so that speed and restore follow any hardware failures or security breaches. Efficiency for restore and trouble with minimal interference further contribute to business resiliency. Planning for extensiveness and sound project planning in addition to offsets of likely costs from risks associated with hacking or supply chain lagging infers a level of tipping stability for cost and timing related to the system being deployed. A well planned security system based on NFC access security is a cost effective, scalable and appropriate for current access control, with related issues of security and availability addressed and suitable for all home and/or business needs.

REFERENCES

1. Mohammad Asadul Hoque & Chad Davidson, “Design and Implementation of an IoT-Based Smart Home Security System”, International Journal of Networked and Distributed Computing, 2019.
2. Garima Jain, Sanjeet Dahiya, “NFC: Advantages, Limits, and Future Scope”, International Journal on Cybernetics & Informatics (IJCI), 2015.
3. 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.
4. A Anitha, “Home Security System Using Internet of Things”, IOP Conference Series: Materials Science and Engineering, 2017.
5. 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
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. Panyaram, S., & Kotte, K. R. (2025). Leveraging AI and Data Analytics for Sustainable Robotic Process Automation (RPA) in Media: Driving Innovation in Green Field Business Process. In Driving Business Success Through Eco-Friendly Strategies (pp. 249-262). IGI Global Scientific Publishing.
13. Dr. Seth James Nielson, Christopher K. Monson, “Practical Cryptography in Python”, Springer Link, 2019.
14. Ivo Haring, “Technical Safety, Reliability and Resilience: Methods and Processes”, Springer Link, February 2021.
15. Lawrence Fennelly, “150 Things You Should Know about Security”, ScienceDirect, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details