IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Access Control System Using Raspberry Pi And RFID

[1]Bhoodevi Bhandare, [2]Sunita Kheman

[1]Assitant Professor, [2]Assitant Professor
[1]Department of physics, [2]Dept. of Electronics & Communication
[1] PDA College of Engineering Kalaburagi, Karnataka, India.
ORCID: 0009-0009-1096-2581, 0009-0002-7023-2854

Abstract: In the present digital era, security has become one of the most critical concerns across various domains such as educational institutions, corporate offices, research laboratories, industrial environments, residential complexes, and government organizations. Conventional access control mechanisms based on physical keys, passwords, or manual verification methods are increasingly proving to be inefficient, unreliable, and vulnerable to unauthorized access, duplication, theft, and human error. These traditional systems also lack flexibility, scalability, and real-time monitoring capabilities. To overcome these challenges, there is a growing need for intelligent, automated, and secure access control systems that can provide accurate authentication with minimal human intervention.

This paper presents the design and implementation of an Access Control System using Raspberry Pi and Radio Frequency Identification (RFID) technology. The proposed system offers a contactless, reliable, and cost-effective solution for managing access to restricted areas. RFID technology is used for user identification and authentication, where each authorized user is provided with a unique RFID card or tag containing a distinct identification number. The Raspberry Pi acts as the central processing unit, responsible for reading RFID data, validating credentials, controlling access mechanisms, and maintaining entry logs.

When an RFID card is scanned near the reader, the system captures the unique identification code and sends it to the Raspberry Pi for verification. The Raspberry Pi compares the scanned data with a pre-stored database of authorized users. If the credentials match, access is granted by activating the door locking mechanism through a relay module, and a visual or audio indication is provided. In case of unauthorized access attempts, the system denies entry and displays an alert message. This real-time decision-making process ensures high accuracy and improved security.

The experimental results demonstrate that the proposed access control system is efficient, reliable, and responsive. It successfully authenticates authorized users within a short time and effectively blocks unauthorized access attempts. The system operates with low power consumption and minimal hardware complexity, making it suitable for small-scale as well as large-scale deployments. Overall, the proposed solution provides a secure, scalable, and user-friendly access control mechanism that can significantly enhance safety and automation in modern infrastructures.

Index Terms - Access Control System, Raspberry Pi, RFID Technology, Embedded Systems, Security Systems, Authentication, Authorization, IoT-Based Security, Contactless Access, Smart Door Lock, RFID Reader, Solenoid Lock, Relay Module, Python Programming, Real-Time Monitoring, Data Logging, Automation, Smart Infrastructure, Digital Security, User Identification.

I. INTRODUCTION

In recent years, rapid technological advancements and increasing security threats have made access control systems an essential component of modern infrastructure. Access control refers to the selective restriction of entry to a place, system, or resource based on predefined authorization policies. It plays a crucial role in safeguarding physical assets, confidential information, and human safety in environments such as educational institutions, corporate offices, industrial facilities, residential complexes, data centers, and government organizations. Traditional access control methods, including mechanical keys, passwords, and manual verification, are gradually becoming obsolete due to their inherent limitations and security vulnerabilities.

Conventional key-based systems are prone to issues such as key duplication, loss, theft, and unauthorized usage. Similarly, password-based systems suffer from problems related to memorability, password sharing, brute-force attacks, and lack of accountability. Manual security mechanisms depend heavily on human intervention, making them inefficient, time-consuming, and susceptible to errors and manipulation. These limitations have led to the growing demand for automated, intelligent, and secure access control solutions that ensure reliability, accuracy, and ease of operation.

Radio Frequency Identification (RFID) technology has emerged as a promising solution for modern access control applications. RFID enables contactless identification and authentication of users through unique identification codes stored in RFID cards or tags. The contactless nature of RFID technology enhances convenience, reduces wear and tear, and minimizes authentication time. Moreover, RFID-based systems offer improved security by assigning unique identifiers to each user, making unauthorized duplication difficult.

The Raspberry Pi, a compact and powerful single-board computer, has gained significant popularity in embedded system and Internet of Things (IoT) applications. Unlike traditional microcontrollers, Raspberry Pi supports multitasking, advanced programming, database integration, and network connectivity. These features make it an ideal platform for developing intelligent access control systems with enhanced functionality, scalability, and future expansion capabilities. The combination of Raspberry Pi and RFID technology provides a robust foundation for building smart security systems.

This paper focuses on the design and implementation of an **Access Control System using Raspberry Pi and RFID**, which aims to provide secure, efficient, and automated access management. The proposed system verifies user identity by comparing RFID card data with stored authorized credentials. Upon successful authentication, the system grants access by activating a locking mechanism, while unauthorized attempts are rejected and recorded. Additionally, the system supports data logging, allowing administrators to monitor access activities and maintain digital records.

The proposed solution emphasizes affordability, ease of deployment, and adaptability. It can be implemented in small-scale environments such as homes and offices, as well as large-scale infrastructures like campuses and industrial facilities. By integrating hardware components with software-based decision-making, the system enhances security while reducing operational complexity. This research highlights the importance of smart access control systems in modern security frameworks and demonstrates how embedded computing platforms can be leveraged to address real-world security challenges effectively.

II. LITERATURE REVIEW

The development of access control systems has been widely explored by researchers and engineers, resulting in various approaches using different technologies such as RFID, biometric authentication, keypad-based systems, and IoT-enabled security frameworks. This section reviews existing research work related to RFID-based access control systems and highlights their advantages and limitations.

Early access control systems primarily relied on mechanical locks and manual supervision, which were later replaced by electronic locking mechanisms using microcontrollers. Several researchers proposed RFID-based access systems using microcontrollers such as Arduino and PIC, where RFID cards were used for user identification. These systems demonstrated improved efficiency over traditional methods; however, they often lacked advanced features such as data storage, real-time monitoring, and scalability.

Subsequent studies introduced RFID-based door locking systems integrated with microcontrollers and relay modules. These systems focused on basic authentication, where access was granted or denied based on card validity. While effective, many of these solutions did not provide logging mechanisms or remote access capabilities. Additionally, limited processing power restricted their ability to support advanced security features.

With the rise of embedded computing and IoT technologies, researchers began incorporating single-board computers into access control systems. Raspberry Pi–based access systems gained attention due to their ability to support operating systems, databases, and network communication. Several studies proposed Raspberry Pi and RFID-based security systems capable of maintaining user databases and recording access logs. These systems improved traceability and accountability by storing entry records for analysis.

Some researchers extended RFID-based systems by integrating GSM modules to send alerts during unauthorized access attempts. Others explored cloud-based access control solutions, enabling administrators to monitor and manage access remotely through web dashboards. Although these systems enhanced security, they introduced additional complexity and dependency on network availability.

Hybrid authentication systems combining RFID with biometric technologies such as fingerprint recognition, facial recognition, or iris scanning have also been studied. These systems provide higher security by implementing multi-factor authentication. However, they often increase system cost and computational requirements, making them less suitable for low-budget or small-scale deployments.

Recent literature highlights the importance of scalable and modular access control systems that can be easily upgraded and integrated with smart infrastructure. Researchers emphasize the need for systems that balance security, cost, performance, and ease of implementation. Despite significant advancements, many existing solutions lack flexibility, real-time data analysis, or user-friendly interfaces.

The proposed system in this paper builds upon existing research by leveraging the processing capabilities of Raspberry Pi and the simplicity of RFID technology. It aims to overcome the limitations of earlier systems by offering improved authentication accuracy, efficient data management, and potential for future IoT integration. By addressing security, scalability, and cost-effectiveness, this work contributes to the ongoing development of intelligent access control systems suitable for modern applications.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed Access Control System using Raspberry Pi and RFID is designed to provide a secure, automated, and efficient mechanism for controlling access to restricted areas. The system architecture integrates both hardware and software components to perform user authentication, access decision-making, and physical control of the locking mechanism. The overall design emphasizes simplicity, reliability, and scalability, making it suitable for various real-world applications such as offices, laboratories, institutions, and residential buildings.

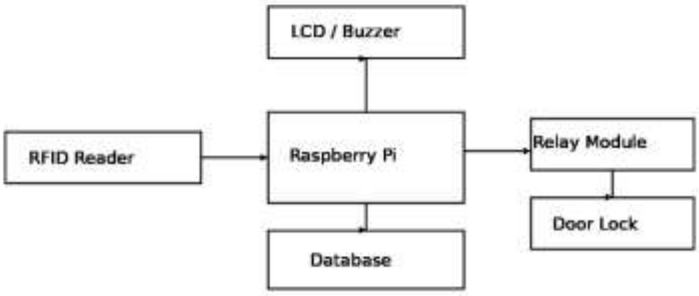

Fig. 1. Block diagram of proposed access control system using Raspberry Pi and RFID

The architecture primarily consists of an RFID reader, Raspberry Pi, database unit, relay module, door locking mechanism, and user notification components such as an LCD display or buzzer. The RFID reader serves as the input device, while the Raspberry Pi functions as the central processing and control unit. All authentication decisions are handled by the Raspberry Pi based on the data received from the RFID reader and the stored user credentials.

When a user presents an RFID card near the RFID reader, the reader captures the unique identification number (UID) embedded in the card. This UID is transmitted to the Raspberry Pi through a serial or SPI communication interface. The Raspberry Pi processes the received data and compares it with the list of authorized card IDs stored in a local database. The database may be implemented using SQLite or MySQL, enabling efficient storage and retrieval of authentication records.

If the scanned RFID card matches an authorized entry in the database, the Raspberry Pi generates a control signal to activate the relay module. The relay module, acting as an electrical switch, controls the door locking mechanism such as a solenoid lock or electromagnetic lock. Upon activation, the lock opens for a predefined duration, allowing the authorized user to gain access. Simultaneously, the system provides visual or audible feedback through an LCD display or buzzer indicating successful authentication.

In the case of an unauthorized RFID card, the Raspberry Pi denies access by keeping the door lock in a closed state. An alert message such as “Access Denied” is displayed, and the attempt can be logged for security auditing purposes. The system also records access details such as date and time for every authentication attempt, enabling effective monitoring and analysis of user activity.

The modular architecture of the proposed system allows for easy expansion and future upgrades. Additional features such as IoT-based remote monitoring, cloud data storage, biometric authentication, or mobile notifications can be integrated without major changes to the existing framework. Overall, the proposed system architecture ensures secure access control, efficient data management, and reliable system performance.

IV. HARDWARE REQUIREMENTS

The hardware components form the physical backbone of the proposed Access Control System using Raspberry Pi and RFID. Each component plays a crucial role in ensuring accurate authentication, reliable control of the locking mechanism, and smooth system operation. The hardware architecture is designed to be cost-effective, modular, and scalable, making it suitable for deployment in various environments such as offices, institutions, laboratories, and residential complexes.

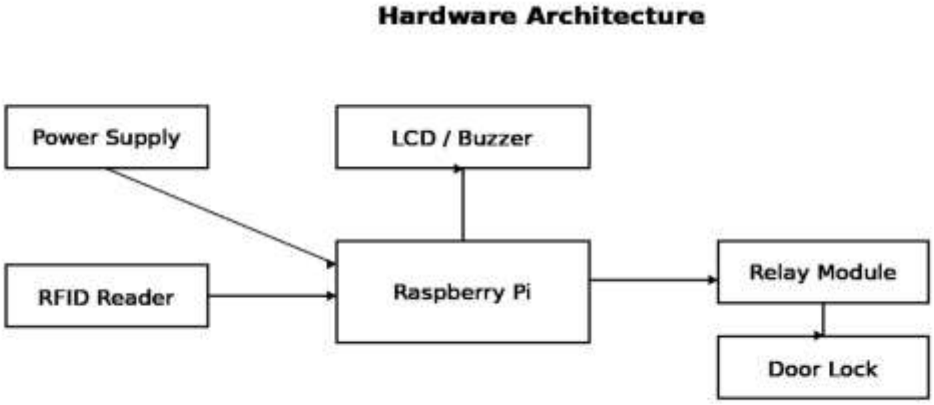

Fig. 2. Hardware block diagram of Raspberry Pi and RFID-based access control system.

1. Raspberry Pi

The Raspberry Pi acts as the central processing and control unit of the system. It is a single-board computer capable of running a full-fledged operating system and handling complex tasks such as database management, authentication logic, and peripheral control. The Raspberry Pi processes the RFID data received from the reader, compares it with stored credentials, and controls the relay module accordingly. Its GPIO pins enable direct interfacing with hardware components, while its processing power supports future integration with IoT platforms and advanced security modules.

2. RFID Reader (RC522)

The RFID reader is responsible for detecting and reading RFID cards or tags. It operates on radio frequency communication to extract the unique identification number (UID) stored in the RFID card. The reader communicates with the Raspberry Pi using SPI protocol, ensuring fast and reliable data transfer. Its contactless operation enhances convenience and minimizes wear and tear compared to physical contact-based systems.

3. RFID Cards / Tags

RFID cards or tags store unique identification codes assigned to authorized users. Each card acts as a digital key, allowing the system to distinguish between authorized and unauthorized users. These cards are durable, easy to carry, and difficult to duplicate, thereby improving system security.

4. Relay Module

The relay module functions as an electrically operated switch that enables the Raspberry Pi to control high-voltage devices safely. Since the Raspberry Pi operates at low voltage levels, the relay acts as an interface between the control logic and the door locking mechanism. When activated, the relay allows current to flow to the lock, enabling access.

5. Door Lock (Solenoid / Electromagnetic Lock)

The door locking mechanism physically restricts or permits access. Upon receiving a signal from the relay module, the lock disengages for a predefined duration, allowing authorized users to enter. Solenoid and electromagnetic locks are commonly used due to their fast response time and reliability.

6. LCD Display / Buzzer

These components provide real-time user feedback. The LCD display shows messages such as “Access Granted” or “Access Denied,” while the buzzer alerts users during unauthorized access attempts. These indicators improve user interaction and system transparency.

7. Power Supply

A regulated power supply is essential for providing stable voltage to all hardware components. The Raspberry Pi typically requires a 5V power source, while other peripherals may require additional voltage regulation.

V. SOFTWARE REQUIREMENTS

The software components govern the logical operation of the access control system. They are responsible for reading RFID data, authenticating users, controlling hardware components, managing databases, and providing real-time feedback. The software architecture is designed to be flexible, efficient, and easy to maintain.

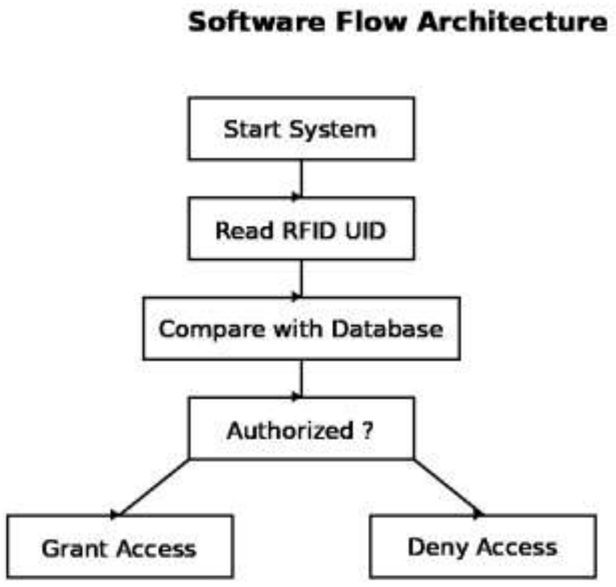

Fig. 3. Software flow diagram for RFID-based access control system.

1. Operating System

The Raspberry Pi runs on a Linux-based operating system such as Raspbian OS. This OS provides a stable environment for executing Python programs, managing hardware interfaces, and supporting database operations. It also enables networking capabilities for future remote access and monitoring.

2. Programming Language (Python)

Python is used as the primary programming language due to its simplicity, readability, and extensive library support. Python scripts handle RFID data acquisition, UID comparison, GPIO control, and user feedback mechanisms. Its modular structure allows easy enhancement and debugging.

3. RFID Interface Libraries

Specialized Python libraries such as MFRC522 and SPI enable communication between the RFID reader and the Raspberry Pi. These libraries simplify low-level hardware interactions and ensure reliable data transmission.

4. GPIO Control Libraries

GPIO libraries allow the Raspberry Pi to control external devices such as relays, LCD displays, and buzzers. These libraries manage pin configuration, signal generation, and timing operations.

5. Database Management System

A lightweight database such as SQLite or MySQL is used to store authorized RFID card IDs and access logs. The database ensures secure storage, fast retrieval, and structured management of authentication data. Logging features support monitoring and auditing.

6. Development Environment

Python IDEs such as Thonny or IDLE are used for program development and testing. These tools provide debugging support and facilitate efficient code development.

7. System Workflow

The software workflow begins with system initialization, followed by RFID scanning, UID comparison, access decision-making, and hardware control. Each step is executed sequentially to ensure accurate and secure operation.

VI. SYSTEM IMPLEMENTATION

The implementation of the proposed Access Control System using Raspberry Pi and RFID involves the integration of both hardware and software components to achieve secure and automated access management. This section explains the step-by-step implementation process, including hardware interfacing, software configuration, authentication logic, and system operation. The implementation is designed to ensure reliability, accuracy, and ease of maintenance.

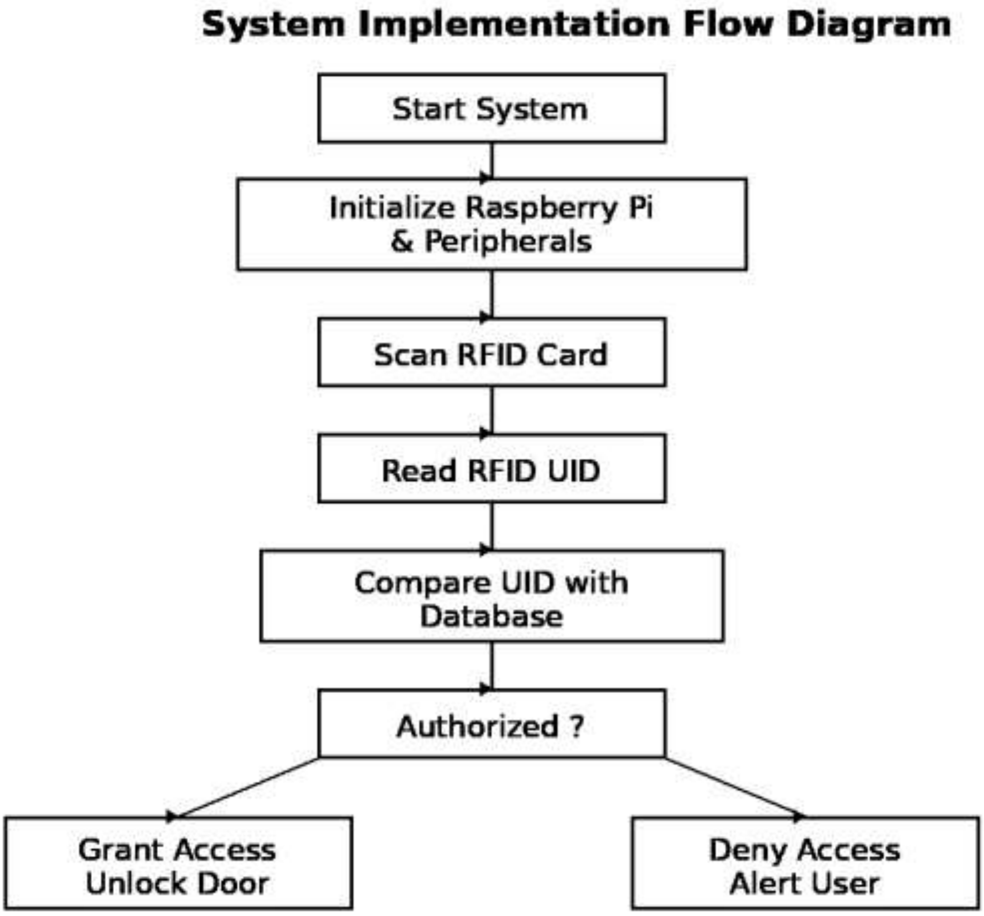

Fig. 4. System implementation flow diagram for Raspberry Pi and RFID-based access control system.

A. Hardware Integration

The hardware implementation begins with interfacing the RFID reader, relay module, locking mechanism, and user feedback devices with the Raspberry Pi. The RFID reader (RC522) is connected to the Raspberry Pi using the SPI communication protocol. Proper pin configuration is performed to ensure accurate data transmission between the RFID reader and the Raspberry Pi.

The relay module is connected to one of the GPIO pins of the Raspberry Pi. Since the Raspberry Pi operates at low voltage, the relay module acts as an intermediary, enabling the control of the door locking mechanism without damaging the controller. The solenoid or electromagnetic lock is connected to the relay output, allowing the system to physically lock or unlock the door based on authentication results.

An LCD display and buzzer are interfaced with the Raspberry Pi to provide real-time feedback to users. The LCD displays messages such as “Access Granted” or “Access Denied,” while the buzzer produces an alert sound during unauthorized access attempts. A regulated power supply is used to ensure stable voltage to all components, preventing system malfunction due to power fluctuations.

B. Software Setup and Configuration

The Raspberry Pi is configured with a Linux-based operating system, and necessary software packages and libraries are installed. Python is used as the primary programming language due to its simplicity and extensive support for hardware control and database management.

RFID interface libraries are installed to enable communication between the RFID reader and the Raspberry Pi. GPIO libraries are configured to control the relay, LCD display, and buzzer. A local database is created to store authorized RFID card IDs and maintain access logs. This database plays a crucial role in authentication and monitoring.

The software is modularly designed, with separate modules handling RFID reading, database operations, access control logic, and output control. This modular approach simplifies debugging, testing, and future enhancements.

C. Authentication and Access Control Logic

The system implementation follows a sequential authentication process. When the system is powered on, the Raspberry Pi initializes all connected peripherals and loads the authorized user database. The RFID reader continuously waits for a card to be scanned.

Once an RFID card is detected, the reader extracts the unique identification number (UID) and transmits it to the Raspberry Pi. The received UID is then compared with the stored authorized entries in the database. If a match is found, the system identifies the user as authorized and proceeds to grant access.

Upon successful authentication, the Raspberry Pi activates the relay module, which unlocks the door for a predefined time interval. During this period, the LCD displays an “Access Granted” message. After the time expires, the door automatically locks again, ensuring controlled access.

If the scanned UID does not match any authorized entry, the system denies access. The door remains locked, an “Access Denied” message is displayed, and the buzzer is activated to alert security personnel or users. Unauthorized access attempts are recorded in the database for further analysis.

D. Data Logging and Monitoring

A key feature of the implementation is the ability to log access data. Each authentication attempt—successful or unsuccessful—is recorded with the corresponding RFID UID, date, and time. This data logging capability enables administrators to monitor user activity, analyze access patterns, and detect suspicious behavior.

The stored logs can be reviewed locally or integrated with remote monitoring systems in future upgrades. This feature enhances accountability and strengthens overall security.

E. System Testing and Validation

After implementation, the system is tested under various conditions to ensure reliable operation. Multiple RFID cards are tested to verify correct authentication and rejection. The relay response time, door locking mechanism, and feedback indicators are carefully observed. The system demonstrates quick response, accurate authentication, and stable operation over extended usage.

F. Implementation Advantages

- The implemented system offers several advantages:
- Automated and contactless access control
- Reduced human intervention
- Accurate authentication and logging
- Low hardware complexity
- Easy scalability and maintenance

Summary

The successful implementation of the proposed access control system demonstrates the effectiveness of combining Raspberry Pi with RFID technology for secure and automated access management. The system operates efficiently, provides real-time feedback, and ensures reliable access control. Its modular design and robust implementation make it suitable for deployment in various real-world environments while allowing future expansion with advanced security features.

VII. RESULTS AND DISCUSSION

The proposed **Access Control System using Raspberry Pi and RFID** was implemented and tested under various operating conditions to evaluate its performance, reliability, and effectiveness. The system was assessed based on parameters such as authentication accuracy, response time, system stability, and user interaction. Multiple RFID cards, both authorized and unauthorized, were used during the testing phase to validate the system’s functionality.

The results indicate that the system successfully identifies authorized RFID cards and grants access within a very short response time. Upon scanning a valid RFID card, the Raspberry Pi processes the unique identification number and verifies it against the stored database. The relay module is activated almost instantaneously, allowing the door lock to open for the specified duration. This quick response enhances user convenience and ensures smooth operation in real-time environments.

Unauthorized access attempts were effectively detected and blocked by the system. When an invalid or unregistered RFID card was scanned, the system denied access and maintained the locked state of the door. Simultaneously, a warning message was displayed on the LCD, and an alert was generated using the buzzer. These features provide immediate feedback and improve security by discouraging unauthorized usage.

The data logging functionality performed reliably throughout the testing process. Each access attempt, whether successful or unsuccessful, was recorded with the corresponding RFID UID and timestamp. These logs proved useful for monitoring user activity and analyzing access patterns. The stored data can be utilized for attendance tracking, security audits, and behavioral analysis in institutional and organizational environments.

From a stability perspective, the system operated continuously without noticeable failure or malfunction. The Raspberry Pi handled multiple authentication requests efficiently, demonstrating its suitability for access control applications. The hardware components such as the RFID reader, relay module, and locking mechanism worked in coordination without signal delays or synchronization issues.

The discussion of results highlights that the proposed system offers a practical balance between security, cost, and performance. Compared to traditional key-based systems, the RFID-based approach provides higher security and ease of use. Unlike biometric systems, it avoids high computational complexity and cost, making it suitable for low- and medium-scale deployments. Overall, the experimental results confirm that the system is reliable, efficient, and capable of enhancing access control in real-world scenarios.

VIII. ADVANTAGES

The proposed **Access Control System using Raspberry Pi and RFID** offers several advantages over traditional security mechanisms. The system provides **contactless authentication**, which improves user convenience and reduces wear and tear associated with physical keys. The use of RFID technology ensures faster access verification and minimizes human involvement, thereby reducing the chances of error.

Another major advantage is **enhanced security**. Each RFID card contains a unique identification number, making unauthorized duplication difficult. The system also prevents access by unregistered users and records every access attempt, ensuring accountability. The ability to maintain access logs improves monitoring and security auditing.

The system is **cost-effective and energy-efficient**, as it uses readily available hardware components and consumes low power. The use of Raspberry Pi enables advanced features such as database storage, networking capability, and easy software updates. Additionally, the modular design allows easy scalability and future expansion without major changes to the existing system architecture.

IX. APPLICATIONS

The proposed system can be deployed in a wide range of real-world applications where controlled access is required. It is suitable for **educational institutions** to manage entry into classrooms, laboratories, and libraries. In **corporate offices**, the system can restrict access to authorized employees and maintain attendance records.

The system is also applicable in **industrial environments**, where access to restricted zones must be limited to trained personnel only. In **residential complexes and smart homes**, it enhances security by allowing only authorized individuals to enter. Additionally, the system can be used in **government offices, hospitals, data centers, and research laboratories**, where security and access tracking are critical.

X. CONCLUSION

This paper presented the design and implementation of an **Access Control System using Raspberry Pi and RFID** that provides a secure, efficient, and automated solution for managing access to restricted areas. The system successfully authenticates users based on RFID credentials and grants or denies access accordingly. The integration of Raspberry Pi enables advanced processing, data logging, and scalability, making the system suitable for modern security requirements.

Experimental results demonstrated that the system operates reliably with quick response time and accurate authentication. Unauthorized access attempts were effectively blocked, and access logs were successfully maintained. The proposed system overcomes the limitations of traditional access control mechanisms by offering improved security, ease of use, and flexibility. Overall, the solution proves to be practical and effective for real-world deployment.

XI. FUTURE SCOPE

Although the proposed system provides reliable access control, several enhancements can be incorporated in future developments. The system can be extended by integrating **biometric authentication** methods such as fingerprint or facial recognition to enable multi-factor authentication. **IoT-based cloud integration** can allow remote monitoring and control of access activities through web or mobile applications.

Additional features such as **SMS or email notifications** for unauthorized access attempts can further improve security. The system can also be enhanced with **mobile-based authentication**, QR codes, or smart card technology. Integration with **centralized security management systems** and artificial intelligence-based analytics can provide advanced monitoring, predictive security insights, and improved decision-making.

References

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 3rd ed., Wiley, 2016.

[2] M. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing*, vol. 15, no. 1, pp. 25–33, 2016.

[3] S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*, Addison-Wesley, 2016.

[4] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 381–394, 2016.

[5] Raspberry Pi Foundation, "Raspberry Pi Documentation," Raspberry Pi Foundation, UK, 2016.

[6] J. Landt, "The History of RFID," *IEEE Potentials*, vol. 35, no. 4, pp. 8–11, 2016.

[7] P. Kumar and S. R. Lee, "RFID-Based Security System," *International Journal of Engineering Research and Applications*, vol. 6, no. 5, pp. 21–26, 2016.

[8] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 22–34, 2017.

[9] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications*, vol. 5, no. 9, pp. 164–173, 2017.

[10] N. Singh and P. Mahajan, "Smart Door Lock System Using RFID and Raspberry Pi," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 6, no. 2, pp. 234–238, 2017.

[11] A. Al-Ali, R. Al-Rousan, and M. Qasaimeh, "Smart Home Automation Using IoT," *IEEE International Conference on Consumer Electronics*, pp. 1–6, 2017.

[12] T. Kumar and A. Verma, "Design and Implementation of RFID Based Security System," *International Journal of Emerging Technology and Advanced Engineering*, vol. 7, no. 3, pp. 112–116, 2017.

[13] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 28–34, 2017.

[14] S. Bhattacharya, S. K. Saha, and S. Dey, "Embedded System Based Access Control Using RFID," *International Journal of Computer Applications*, vol. 165, no. 6, pp. 18–22, 2017.

[15] M. S. Hossain and G. Muhammad, "Cloud-Based IoT Security Framework," *Future Generation Computer Systems*, vol. 70, pp. 77–86, 2017.