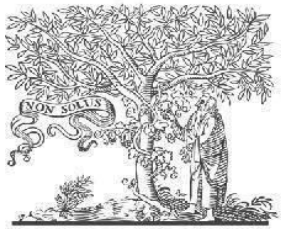
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 18th Dec 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13&issue= Issue12

DOI:10.48047/IJIEMR/V13/ISSUE12/37

Title: " SMART DOOR ACCESSING SYSTEM USING RFID"

Volume 13, ISSUE 12, Pages: 285 - 291

Paper Authors
Mr. G. Venkataswamy, Ms. G. Pradeepthi, Ms. P. Charitha, Ms. K. Uma Devi

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SMART DOOR ACCESSING SYSTEM USING RFID

Mr. G. Venkataswamy[1], Ms. G. Pradeepthi[2], Ms. P. Charitha[3], Ms. K. Uma Devi[4]

[1]Assistant Professor, Department of ECE, CMR Institute of Technology, Medchal, Hyderabad
[2,3,4]Bachelor's Student, Department of ECE, CMR Institute of Technology, Medchal, Hyderabad.

ABSTRACT-Security is the foremost matter that must be tackled in the present world. IoT has been proven to be the Progressive technology unraveling many security associated issues. Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The entrance plays an significant role in room safety. So, furnishing a protected door system for houses, offices, etc has turn out to be a essential research. The purpose is to carry out a security system by combining mobile phone and IOT using RFID. Here is a Room security solution based on IoT using RFID. We are going to build an RFID Based Access Control System using Node MCU. The same system can be named like Smart Lock System using RFID. If you have been to big hospitals or companies, you might have seen how they used RFID based locks to restrict access to certain areas. To establish a smart locking system which will only accessible for users with authorized cards and to maintain track of users entering and exiting the room through an online interface. As the device is connected to Internet it can be controlled from any place with internet connectivity. Thus one can monitor any room/property from anywhere.

Key words: Arduino UNO, RFID cards, EM-18 RFID Reader Module, Servo motor, Buzzer

1.INTRODUCTION

Safeguarding homes has turn into one of the concerning topic. Today homes are being farther open to numerous threats mainly being burglarised. Hence home security is required. Home security obliquely requires a protected system for the door. As stated, the purpose of this work is to resolve one of the security problems existing in the present world. It has been very tough for people to ensure effective security solutions even however in the enriched technological situations. Internet of Things is becoming a trend in many of the big cities and creating lots of revolutionary effects.

So the idea of Smart door lock system has been proposed. You are given a card and you just need to put it in front of a RFID Reader box, and the lock gets unlocked with a Beep and a Blink of LED. This RFID Door Lock can be made easily at your home and you can install it in any door. These Door lock is just electrically operating door lock which gets open when you apply some voltage (typically 12v) to it. With this system, only the legitimate persons can acquire the clearance to access the doors [1]. By using RFID the system will be able to differentiate a valid user with an invalid one. Also. The system can be monitored from anywhere in the world due to the continuous updating of the status of the door. With this system, only the

authorized individuals can gain the permission to access the doors [2]. Thus one can monitor his/her house from anywhere. A digital door locking system is also implemented and governed by RFID reader which authenticate and validate the user and open the door automatically.

It also keeps the record of check-in and check-out of the user. It's very important to authenticate the user before entering into a secure space and RFID provide this solution [3]. The system enables user to checkin and check-out under fast, secure and convenient conditions. The system include door locking system which open when the user put their tag in contact with reader and the user information matched with the information already stored in database [5]. The RFID controls the opening and closing of the door. In this study we utilize RFID technology to provide solution for secure access of a space while keeping record of the
user.

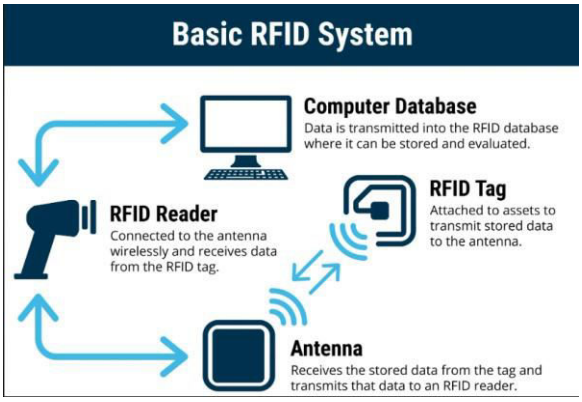


Fig 1: Diagram showing basic introduction of RFID system

2.LITERATURE REVIEW

The advancements in access control technologies have significantly improved security systems, with RFID-based smart door lock systems gaining prominence for their convenience, reliability, and enhanced security features. RFID, or Radio Frequency Identification, is widely used in modern access control to replace traditional methods such as keys or PINs. Several researchers have explored the integration of RFID technology into door locking systems, demonstrating its potential to improve security while maintaining ease of use [7].

Lia Kamelia et al. (2014) developed a Bluetoothbased door automation system that integrated RFID with Android mobile phones, enabling users to control and monitor access remotely. Similarly, Sedhumadhavan and Saraladevi (2014) presented an optimized locking system using Arduino, showcasing RFID as a primary means of user authentication. These systems highlighted the superiority of RFID over traditional locks and keypads by eliminating risks such as key duplication or password compromise [4]. RFID based systems have proven to be faster and more secure, making them a preferred choice for modern applications.

The integration of IoT (Internet of Things) has further expanded the capabilities of RFID-based door lock systems. IoT to provide remote monitoring and control of access events. Their work demonstrated how cloud-based services allow users to manage privileges and receive real-time notifications, making these systems suitable for residential, commercial, and industrial environments. Similarly, IoT's role in enhancing user experience through real-time monitoring and automation. By combining RFID with IoT, these systems provide a more robust and versatile solution for access control [6].

Cost and flexibility are additional factors contributing to the popularity of RFID-based systems. Unlike biometric systems that rely on expensive sensors or GSM-based systems that require network availability, RFID systems are cost-effective and operate independently. Lia Kamelia et al. (2014) noted that RFID-based locks can be installed without significant modifications to existing infrastructure, making them ideal for retrofitting. The simplicity of these systems further enhances their appeal, especially for users seeking affordable yet reliable solutions [8].

Emerging trends in access control systems suggest further advancements in RFID-based door locks. Future developments are likely to incorporate additional features such as voice recognition, facial authentication, and AI-driven behavior analysis to enhance security further [9]. The combination of RFID with biometric systems can provide multi-factor authentication, addressing concerns about advanced security threats [10]. Additionally, advancements in low-power devices and edge computing are expected to improve the efficiency and scalability of these systems, enabling them to handle large-scale deployments effectively.

In conclusion, the literature highlights the significant advantages of RFID-based smart door lock systems, including ease of use, cost effectiveness, and improved security. The integration of IoT has enhanced their functionality by enabling real-time monitoring and control. However, challenges such as scalability, data privacy, and protection against sophisticated attacks remain areas for further research. By addressing these issues and leveraging emerging technologies, RFID-based systems can continue to evolve and play a critical role in modern access control solutions.

3.SYSTEM MODEL

The RFID-based Door Lock System is designed as a secure, automated solution for access control, combining RFID technology with a microcontroller-based system to manage user authentication and door operations. The system comprises both hardware and software components that work together to ensure only authorized individuals can gain access. At the core of the system is the RFID reader, which detects and reads the unique identification numbers stored in RFID tags or cards when placed within its range. These tags serve as digital keys, eliminating the need for physical keys or PIN codes that can be easily lost or compromised.

The microcontroller, such as an Arduino or Raspberry Pi, acts as the central processing unit, orchestrating the system's functionality. Upon receiving data from the RFID reader, the microcontroller compares the scanned tag's ID against a pre-configured database of authorized IDs stored in its memory. If the ID matches an authorized entry, the system grants access by triggering the locking mechanism,such as a servo motor or electronic lock, to unlock the door.

Simultaneously, feedback is provided to the user through an LCD display, which shows messages like "Access Granted" or "Access Denied," ensuring clarity in system interactions.

This combination of hardware reliability and software intelligence makes the RFID-based Door Lock System a cost-effective and

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

scalable solution for securing residential, commercial, and industrial spaces.

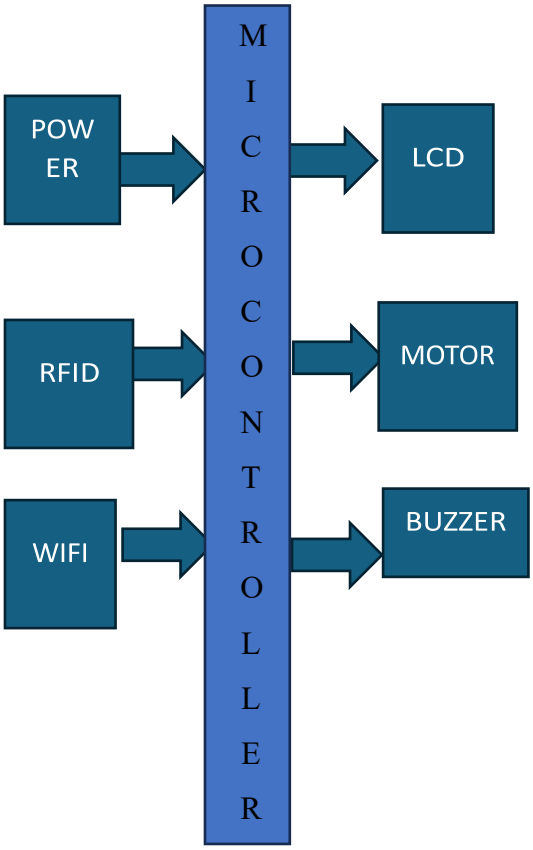


Fig 2: Block diagram showing the steps involved in RFID based door lock system

4.PROPOSED SYSTEM

The proposed system for finger vein recognition employs a deep learning architecture (DenseNet) to enhance the accuracy and robustness of biometric identification. The working process is divided into sequential steps, each contributing to the final recognition or verification result. Here's a step-by-step explanation of the proposed working:

Input Stage

The input stage of the RFID-based door lock system begins when the user presents an RFID card or tag near the RFID reader. The RFID card contains a unique identification (UID) that the system uses to verify the user's identity. The reader captures the UID from the card using electromagnetic signals, converting it into a digital format that can be transmitted to the microcontroller for processing. This step is the first point of interaction between the user and the system, enabling the system to detect an attempt to access the door. The RFID reader continuously scans for RFID tags, ensuring the system is always ready to respond to valid requests.

Processing Stage

Once the UID is scanned, the microcontroller processes the information to determine if the user is authorized to access the door. The microcontroller compares the received UID against a list of authorized IDs that are stored in the system's memory or an external database. If the UID matches one of the authorized entries, the system moves to the next step of granting access. If the UID is not recognized or does not match any of the authorized IDs, the microcontroller denies access. The processing stage is crucial because it ensures that only legitimate users can unlock the door, providing security by preventing unauthorized entry. The microcontroller also sends control signals to the door lock mechanism and status indicators (like LEDs or buzzers) based on the result of the authentication process.

Features

The RFID-based door lock system comes with a variety of features that enhance security, convenience, and flexibility. One of

its main advantages is secure access control, as only users with authorized RFID cards can unlock the door. The system also provides visual feedback through LEDs—green for granting access and red for denial—ensuring that the user is immediately aware of the system's decision. Additionally, the system includes automatic re-locking; once access is granted, the door remains unlocked only for a set period before automatically re-locking to prevent unauthorized access. The system is scalable, meaning it can easily accommodate additional users by simply adding their RFID cards to the authorized list. For enhanced security, the system can integrate dual authentication methods, such as a keypad for PIN input or biometric systems. Furthermore, the option for IoT integration allows remote control and monitoring of the system via mobile devices or web applications. The system can also include a battery backup to ensure continued operation during power outages.

Output Stage

The output stage of the system occurs after the microcontroller has processed the UID and made a decision. If the UID is valid and matches an authorized user, the microcontroller sends a signal to unlock the door. This action is accompanied by the illumination of the green LED, indicating that access has been granted. Additionally, a buzzer may sound to provide auditory feedback to the user. The door remains unlocked for a set period, ensuring that the user has enough time to enter. After this time expires, the microcontroller sends a signal to re-lock the door, restoring the system to its initial locked state. If the UID is invalid, the system triggers the red LED to blink and optionally sounds a buzzer, alerting the user that access is denied. This output stage ensures that the door is either securely unlocked for authorized users or remains locked for unauthorized attempts, maintaining the security of the premises.

Fig 3: Picture showing basic range of RFID

5.RESULT

The RFID-based door lock system operates seamlessly to provide secure and efficient access control. When a user presents an RFID card or tag to the RFID reader, the reader scans the unique identification (UID) stored on the card. The system then sends this UID to the microcontroller for verification. The microcontroller compares the received UID with a stored list of authorized IDs. If a match is found, the system sends a signal to the electronic door lock, triggering it to unlock. At the same time, a green LED lights up to indicate that access has been granted.

If the UID does not match any authorized entry, the microcontroller denies access by keeping the door locked. In this case, the system activates a red LED to signal that the access attempt was unsuccessful, and optionally, a buzzer can sound to alert the user of the invalid attempt.

Once access is granted, the door remains unlocked for a predefined period, after which

the microcontroller sends a signal to re-lock the door. The system then resets and returns to idle mode, waiting for the next RFID card scan. This process ensures smooth operation with real-time feedback and automatic locking for enhanced security.

Overall, the RFID-based door lock system works by securely verifying users, providing instant feedback, and ensuring the door remains locked when not in use, offering a reliable and user-friendly solution for access control.

The future of RFID-based door lock systems holds exciting possibilities for enhanced security and functionality. One major advancement could be the integration with IoT and smart home systems, allowing users to control their locks remotely and create a more automated environment, such as syncing with lighting and heating systems. Additionally, combining RFID with biometric authentication, such as fingerprint or facial recognition, could improve security by adding multi-factor authentication.

Another potential development is the use of smartphones as RFID cards, eliminating the need for physical tags and streamlining access. Cloud-based management systems would also enable administrators to remotely manage access permissions and track entry logs across multiple locations. Furthermore, incorporating voice recognition or AI could enhance user interaction, allowing for voice commands or advanced threat detection.

Blockchain could also play a role in securing access logs, providing tamper-proof data storage for sensitive environments. With these advancements, RFID-based systems will become even more secure, user-friendly, and integrated with broader technology ecosystems.

7.CONCLUSION

In this paper, a smart lock system is presented which is a novel access control system using IOT which includes the online monitoring. The smart lock system provides a convenient way to automate the access control feature thereby enhancing security and enabling the owner of the property carefree. It is a low cost, flexible, and a very easy to install system with no overhead like planning, cabling, and construction works.

REFERENCES

1. K. Radhakrishna, D. Satyaraj, H. Kantari, V. Srividhya, R. Tharun and S. Srinivasan, "Neural Touch for Enhanced Wearable Haptics with Recurrent Neural Network and IoT-Enabled Tactile Experiences," 2024 3rd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1-6,
2. Karne, R. K., & Sreeja, T. K. (2023, November). Cluster based vanet communication for reliable data transmission. In AIP Conference Proceedings (Vol. 2587, No. 1). AIP Publishing.
3. Karne, R., & Sreeja, T. K. (2023). Clustering algorithms and comparisons in vehicular ad hoc networks. Mesopotamian Journal of Computer Science, 2023, 115-123.
4. Karne, R. K., & Sreeja, T. K. (2023). PMLC-Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 477-483.

5. Mohandas, R., Sivapriya, N., Rao, A. S., Radhakrishna, K., & Sahaai, M. B. (2023, February). Development of machine learning framework for the protection of IoT devices. In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1394-1398). IEEE.
6. Kumar, A. A., & Karne, R. K. (2022). IIoT-IDS network using inception CNN model. Journal of Trends in Computer Science and Smart Technology, 4(3), 126-138.
7. Karne, R., & Sreeja, T. K. (2022). Routing protocols in vehicular adhoc networks (VANETs). International Journal of Early Childhood, 14(03), 2022.
8. Karne, R. K., & Sreeja, T. K. (2022). A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER, 10(4), 1092-1098.
9. RadhaKrishna Karne, D. T. (2021). COINV-Chances and Obstacles Interpretation to Carry new approaches in the VANET Communications. Design Engineering, 10346-10361.
10. RadhaKrishna Karne, D. T. (2021). Review on vanet architecture and applications. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(4), 1745-1749.