IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SMART CARD BASED DOOR ACCESS SYSTEM WITH LCD

Pushpak Kishor Chaudhari
Department of Electronics & Telecommunication,
AISSMS Institute of Information Technology, Pune, India

## Abstract:

This paper presents the design and implementation of a smart card-based door access system with an LCD. The system ensures enhanced security for restricted areas, such as banks and offices, by allowing access only to authorized users. The design leverages a contact smart card reader interfaced with a microcontroller to validate user credentials. Unauthorized access triggers an alarm system, while valid users are granted entry through a motorized door. The system is designed to be cost-effective and user-friendly while maintaining high reliability. Additionally, the system demonstrates scalability and can be adapted to include features such as IoT integration and multi-factor authentication, making it suitable for modern security needs.

## I. Introduction

Unauthorized access poses significant security risks in both commercial and residential spaces. Conventional access methods, such as mechanical keys and simple passcodes, are susceptible to duplication and breaches. Advanced technologies such as biometric systems and RFID offer promising alternatives but often come with higher costs and complex implementation requirements. This paper explores the use of a smart card-based door access system that employs microcontroller technology for authentication and control. The integration of an LCD ensures user feedback, enhancing the overall functionality and usability of the system. This project aims to provide a secure, efficient, and user-friendly alternative to conventional access systems. The focus is on creating a system that balances cost, reliability, and ease of use while offering high security. By leveraging the advantages of smart cards, the system provides a non biometric solution that avoids the pitfalls of false acceptance or rejection inherent in biometric methods.

## II. LITERATURE REVIEW

Several access control mechanisms have been studied extensively, each offering unique benefits and limitations. Biometric systems, for instance, provide high levels of security through unique identifiers such as fingerprints, facial features, or iris patterns. However, these systems often face challenges related to cost, processing time, and user acceptance. RFID-based systems, on the other hand, are widely used in commercial settings but may lack robustness against sophisticated attacks such as signal interception or spoofing. Smart card-based systems present a middle ground, combining the reliability of physical tokens with the computational capabilities of embedded systems. Previous studies highlight the effectiveness of smart card-based systems in environments requiring high security and user convenience. For example, Sehgal et al. (2008) demonstrated the utility of embedded controllers for smart card access systems, emphasizing their adaptability to various applications. Similarly, Farooq et al. (2014) explored RFID and smart card integration, showcasing the potential for enhanced security when combined with networked systems.

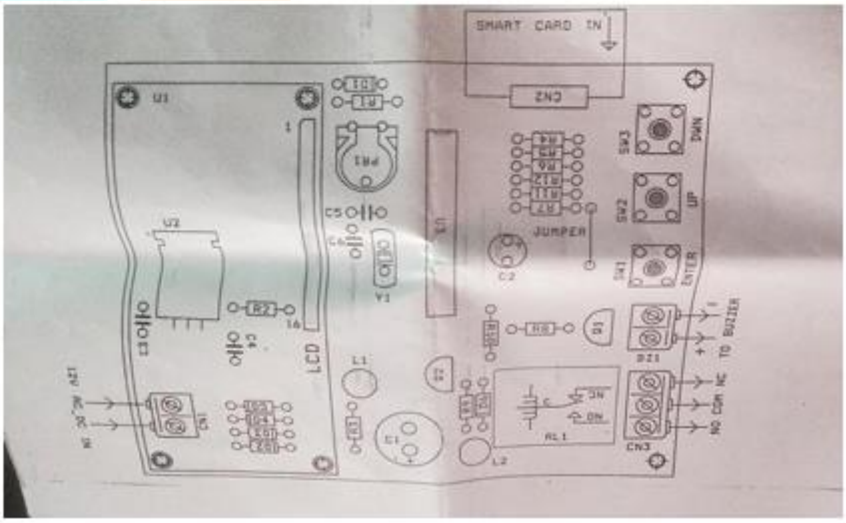
Despite these advancements, many systems suffer from limitations such as lack of scalability, high costs, or complexity in implementation. The proposed system addresses these gaps by utilizing a contact smart card reader and microcontroller, providing a cost-effective and efficient solution tailored for small to medium-scale applications.

## III. SYSTEM DESIGN AND METHODOLOGY

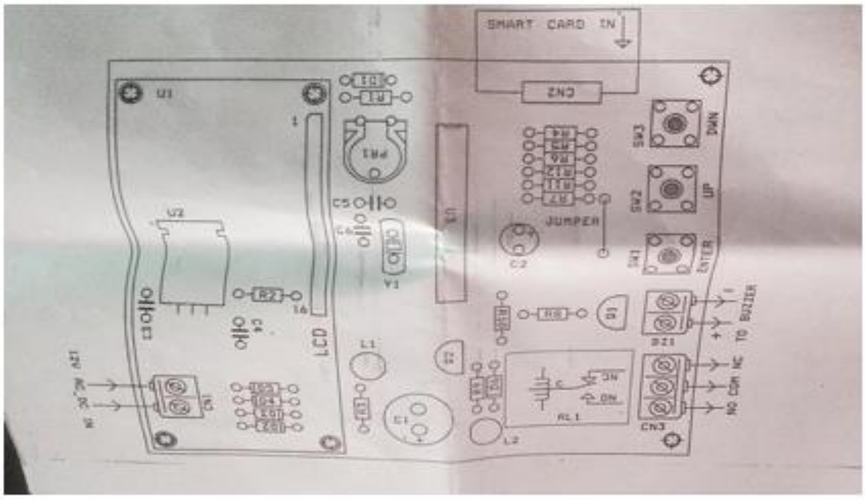
Block Diagram

The system consists of the following components:

1. Smart Card Reader: Reads data from the contact smart card.
2. Microcontroller (PIC16F72): Processes card data and determines access authorization.
3. LCD Display (16x2): Provides feedback to the user.
4. DC Gear Motor: Controls the door mechanism.
5. Power Supply Unit (5V/12V): Powers the system components.
6. Buzzer: Alerts for unauthorized access. The block diagram of the system illustrates the seamless integration of hardware and software components, ensuring efficient operation and robust security. The smart card reader interfaces directly with the microcontroller, which acts as the central processing unit, analyzing input data and triggering the appropriate responses.



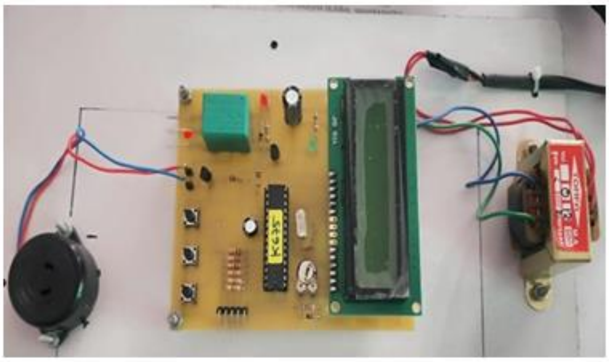
[2] PCB diagram Smart card



[2] PCB diagram Smart card

## **IV.** Hardware Design

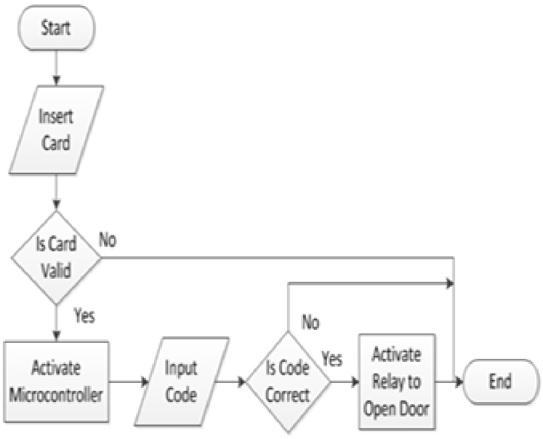
The hardware design focuses on simplicity and reliability. The smart card reader communicates with the microcontroller via a serial interface. The reader retrieves data stored in the card’s EEPROM and transmits it to the microcontroller. The microcontroller compares this data with pre-stored credentials in its memory. For authorized users, the microcontroller activates the motorized door mechanism and displays an "Authorized" message on the LCD. For unauthorized attempts, the buzzer is triggered, and an "Unauthorized" message is displayed. Key hardware specifications include: • Microcontroller: PIC16F72, chosen for its processing power and ease of integration. • Smart Card Reader: SR-90 SDK, supporting 1KB memory capacity and high read/write reliability. • Power Supply: 5V and 12V regulated supplies, ensuring stable operation of all components.



[3] Hardware design photo

## V. Software Design

The software design follows a structured approach to ensure robustness and reliability. The algorithm is implemented as follows: 1. Initialize system components, including the LCD, smart card reader, and buzzer. 2. Continuously monitor the card reader for insertion events. 3. Read data from the inserted card and validate it against stored credentials. 4. If credentials match, activate the motorized door mechanism and display an "Authorized" message. 5. If credentials do not match, trigger the buzzer and display an "Unauthorized" message. 6. Reset the system for the next user interaction.

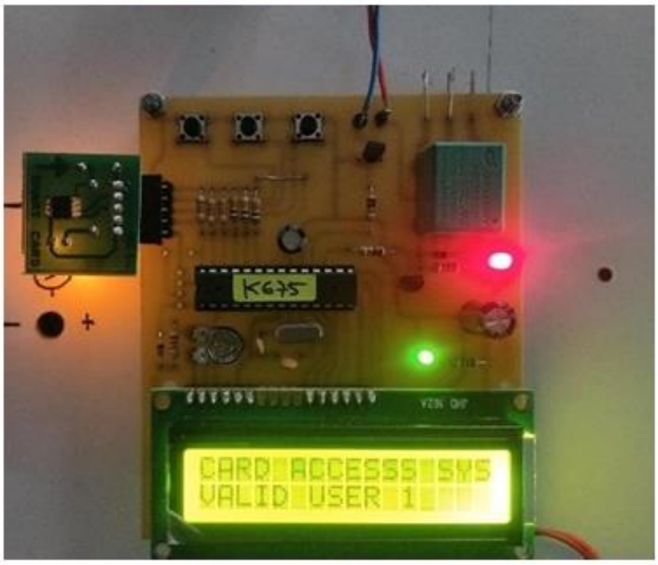


[4] Software flow chart

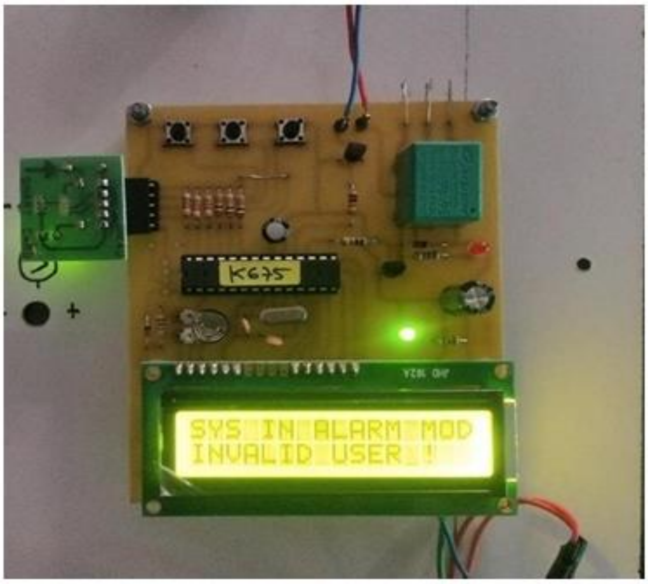
The system software is written in C, utilizing modular functions to facilitate debugging and future enhancements. The program also incorporates error handling to address scenarios such as invalid card data or hardware malfunctions.

## VI. RESULTS AND ANALYSIS

The system was rigorously tested under various scenarios to evaluate its performance and reliability. Key tests included: • Authorized Access: Multiple smart cards with valid credentials were tested to ensure seamless operation. The door mechanism consistently responded within one second of card insertion. • Unauthorized Access: Cards with invalid or corrupted data were used to test the system's response. The buzzer activated immediately, and the LCD displayed an "Unauthorized" message as expected. • Power Interruptions: The system was tested for resilience against power failures. Upon restoration of power, the system resumed normal operation without data loss.



[5] Result photo 1



[6] Result photo 2

The results demonstrate the system's effectiveness in providing secure access control. Key performance metrics include: • Response Time: Less than one second for all operations. • Accuracy: 100% success rate for authorized access and unauthorized detection. • Reliability: Continuous operation over extended testing periods without failures. These findings validate the system's suitability for practical applications in environments such as offices, banks, and restricted areas.

## VII. CONCLUSION AND FUTURE SCOPE

The smart card-based door access system offers a practical, low-cost solution for secure access control. Its design addresses common limitations of existing systems, such as high costs and complexity, while maintaining robust security and user convenience. By leveraging smart card technology, the system provides a reliable alternative to biometric and RFID-based methods.

Future developments could focus on: 1. IoT Integration: Enabling remote monitoring and control of the system via internet connected devices. 2. Multi-Factor Authentication: Incorporating additional security layers, such as PIN codes or biometric verification. 3. Hardware Miniaturization: Reducing the size and power consumption of system components to expand its applicability to portable and wearable devices. 4. Enhanced User Interfaces: Developing intuitive mobile or desktop applications for system management and configuration. The system's scalability and adaptability ensure its relevance in addressing evolving security challenges. With further enhancements, it has the potential to become a cornerstone technology in modern access control solutions.

## VIII. REFERENCES

[1] K.W. Ko, J. Lee, M. Ahmadi, and S. Lee, "Development of Human Identification System Based on Simple Finger Vein Pattern Matching Method for Embedded Environments," International Journal of Security and Its Applications, vol. 9, no. 5, pp. 297 306, 2015. [2] R. Kaur and R. Rani, "An Identity Authentification Using Finger Vein and Texture Images Using NN," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, pp. 983-988, July 2014. [3] I. Sarkar, Alisherov F., T. Kim, and D Bhattachayya, "Palm Vein Authentication System: A Review," International Journal of Control and Automation, vol. 3, no. 1, pp. 27-34, March 2010. [4] A. S. Falohun, E.O. Omidiora, O.A. Fakolujo, O.A. Afolabi, and A.O. Oke, "Development of a biometrically- controlled door system (using iris), with power backup," American Journal of Scientific and Industrial Research, vol. 3, no. 4, pp. 203-207, 2012. [5] O. Omidiora, M. Olaniyi, and A.A. Ipadeola, "Development of Security System Using Facial Recognition,"

Pacific Journal of Science and Technology, vol. 9, no. 2, pp. 377-386, 2008. [6] S. Achankunju and C. Mondikathi, "Voice Based Security System Using Matlab& Embedded System," International Journal of Scientific Research, vol. 4, no. 5, pp. 770-773, May 2015. [7] W.A. Wahyudi and M. Syazilawati, "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for Building Security," Journal of Computer Science , vol. 3, no. 5, pp. 274-280, 2007 [8] L. Osadciw, P. Varshney, and K. Veeramachaneni, "Improving Personal Identification Accuracy Using Multi sensor Fusion for Building Access Control Application," in Proceedings the Fifth International Conference for Information Fusion, 2002, pp. 1176- 1183 [9] U. Farooq, M. Hasan, M. Amar, and A. Hanif, "RFID Based Security and Access Control System," IACSIT International Journal of Engineering and Technology, vol. 6, no. 4, pp. 309-314, August 2014 [10] N. Saparkhojayev, A. Nurtayev, and G. Baimenshina, "Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Keys," Middle-East Journal of Scientific Research, vol. 21, no. 7, pp. 1130-1135, 2014. [11] V.K. Sehgal, Nitin, and D.S. Chauhan, "Embedded Controller Based Smart Card Access," in Proceedings of the World Congress on Engineering and Computer Science, San Francisco, 2008. [12] J.L. Raheja, S. Nayak, and A. Gupta, "RFID Based Networked Gate Entry Control System (GECS)," International Journal of Computer Networks & Communications (IJCNC), vol. 1, no. 3, pp. 34-44, October 2009.