J Euro Eco His.
ISSN : 0391-5115
Volume 7, Isue 3 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Improving Security in Health care Appliances Using a Secret code Based Organizer System

D. Saravanan
School of Computer Science and Artificial Intelligence
SR University
Warangal, Telangana, 506371, India

Faculty of Operations & IT
ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.

S. Vairachilai
School of Computer Science and Artificial Intelligence
SR University
Warangal, Telangana, 506371, India
vairachilai2676@gmail.com

Sai Suheer Volety
Visiting Faculty
ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.

Abstract: The proposed research work focuses on how systems are protected using user authentication techniques. The system utilizes a microcontroller-based approach to gives the secure admittance control to controlled areas. The main components of the system include a keypad for entering the secret code, a microcontroller unit for processing inputs and controlling the locking mechanism, and an electronic lock for physically securing the door. The secret code entry process involves the user inputting a predefined combination using the keypad. Upon receiving the input, the microcontroller compares it with the stored secrete code in its memory. Based on the authentication provided by the user, the system verifies the stored datasets. If both match, the system immediately generates pulses, the corresponding lock is released, and the user is allowed to access the information securely.

If the users enter the wrong credentials or unauthorized access, the system may in corporate features such as timeout delays or alarm triggers to enhance security. The system design emphasizes simplicity, reliability, and cost-effectiveness. This makes it suitable for various applications, covering most day-to-day home applications as well as industrial applications. Additionally, the modular nature of the design allows for easy integration with existing door systems and scalability for future expansions or enhancements. Overall, the secret code-based door lock system offers an efficient and practical solution for access control, providing peace of mind for property owners and occupants alike.

Keywords: Secrete code-based, Door Lock System, Microcontroller, Keypad, Electronic lock, Access control, Security.

1. Introduction

The main motivation of the proposed work is to substitute the old-fashioned key and lock mechanism where we use the physical locking system are used to lock the needed source or using the resource based locking system. Overall, the motivation for implementing a secret code-based lock system using Existing setup or similar platforms lies in its ability to provide robust security, convenience, flexibility, and cost-effectiveness while also offering opportunities for learning and customization in the realm of modern access.

Protecting sensitive information from third parties is one of the major concerns in day-to-day life. With the rapid increase in applications, threats are also increasing; therefore, security mechanisms must continuously improve. Traditional systems that rely on text-based or similar protection methods are easy to break and easy for crackers to guess. Hence, there is an urgent need for a stronger mechanism to protect information from third-party threats. This requirement is not limited to commercial applications alone; it is also applicable to industrial environments. Protection of information from all possible sources must be enhanced. The main focus of this development is on improving lattice-level protection, because existing structural mechanisms can be easily breached. Even systems protected by conventional lock-and-key methods or sensor-based security can be compromised by attackers, allowing unauthorized access. Therefore, it is essential to develop a new security mechanism that can effectively prevent threats and control unauthorized access.

In many cases, unauthorized access may be noticed only after the breach has occurred. To address this issue, the proposed mechanism triggers a siren whenever an unauthorized attempt is detected. This approach provides improved authentication compared to existing lock-and-key-based systems. The proposed mechanism works based on a combination of resource-based and code-based security. The user is required to enter a secret code using the provided input mechanism. This input is compared with the stored data, and access is granted only if both values match. If the user enters an incorrect code more than twice, a siren is immediately activated to alert the owner. Additionally, necessary alerts are sent to inform the owner about the unauthorized attempt.

This proposed system offers better performance than existing security systems. In future developments, the resource-based components can be completely replaced by a fully code-based system, making it difficult for attackers to identify where the resources are installed. This further enhances system security and ensures highly secure information protection. The system provides tension-free security for the owner and eliminates the need to carry physical keys or related security items. The system setup is simple and user-friendly. It consists of a resource module, a code input keypad, a trigger unit, an engine, and a display screen to show user input. The resource-based system maintains full control over the security process. User input received through the keypad is processed by the system code and verified against stored data. Based on the verification, access is either granted or denied. In the case of an incorrect attempt, a trigger-based event is generated, activating the siren and immediately alerting the user. The developed device enhances security in areas where unauthorized entry is restricted

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Isue 3 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

2. System Design:

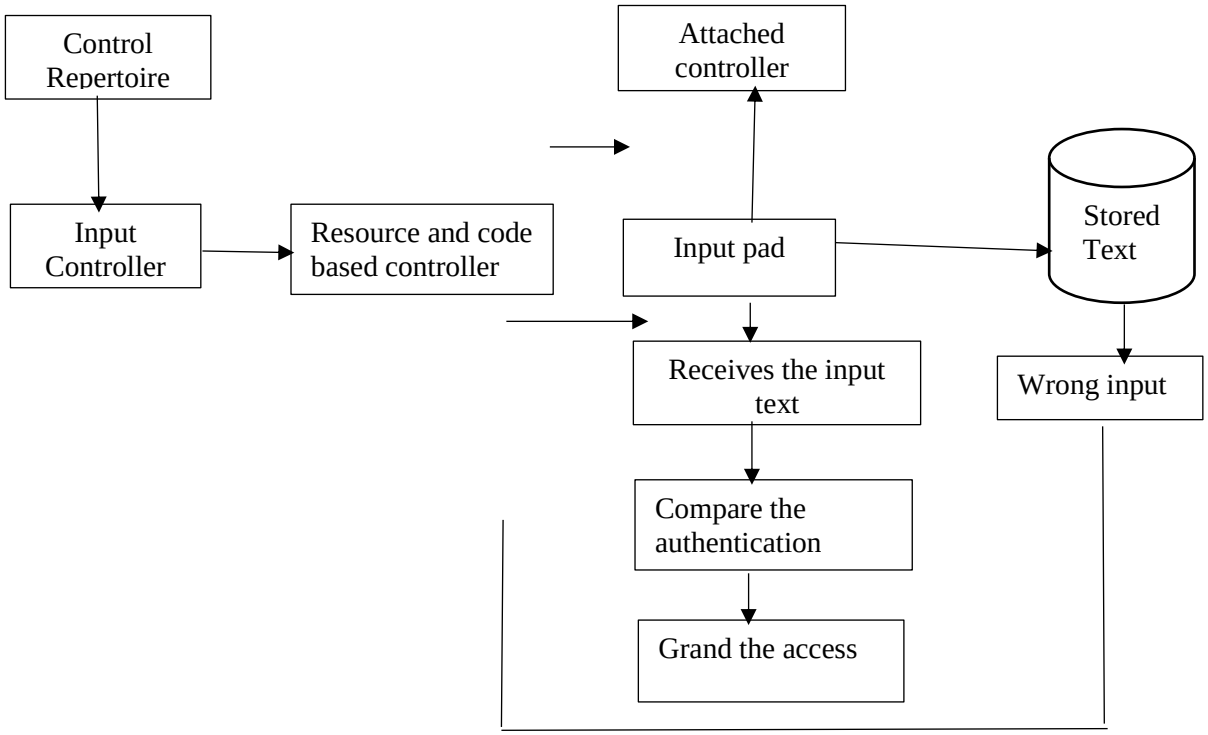

Fig 1 Proposed Architecture

The proposed architecture is shown in **Figure 1.** The working mechanism consists of a control module, an input controller, a resource- and code-based controller, an input keypad, and a display monitor to show the input entered by the user. The system operates on a simple logic. Using the input controller, the user enters a key, which is received by the resource- and code-based controller and forwarded to the stored database. The database is created earlier based on user input choices, where all possible permitted inputs are collected and stored. The received input is compared with the stored data. If both values match, a signal is generated through the resource controller and sent to the attached control mechanism. This mechanism generates and transmits a permission signal that allows user access, thereby authorizing the transaction.

Each user input is verified every time, and authentication is initiated only after successful verification. A maximum of two incorrect attempts is permitted. To address unauthorized access, the proposed mechanism triggers a siren whenever an invalid attempt is detected. If the user enters an incorrect code more than twice, the siren is immediately activated to alert the owner, and necessary alerts are sent regarding the unauthorized attempt. This approach provides improved authentication compared to existing lock-and-key-based systems and offers better performance than conventional security mechanisms. In future developments, the resource-based components can be completely replaced with a fully code-based system, making it difficult for attackers to identify the location of security resources and further enhancing overall system security. The details of each function will be described further below

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Isue 3 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

2.1 Motivation:

Security and safety considerations for a secret code-based lock system are critical to protect against unauthorized access and ensure user privacy. Here are some detailed points to consider:

2.2 Input text control:

In many authentication systems, users are required to set an authentication input using a combination of alphanumeric characters. However, users often choose easily memorable credentials such as their date of birth, marriage date, or important personal milestones like their child's birth date, joining date, or graduation date. Such credentials are highly predictable and can be easily guessed by secret code crackers. In many cases, attackers closely observe users' activities and social behavior, making it possible to collect this information within a short period of time. To address this vulnerability, the proposed system strongly recommends the use of authentication inputs that include a secure combination of letters, numbers, and special characters. This approach makes it significantly more difficult for unauthorized users to track or guess the authentication credentials.

The proposed system restricts access attempts by allowing only two incorrect entries. Upon the third incorrect attempt, the system immediately triggers a siren, creating an alert environment and notifying the owner about a possible security breach. This mechanism enhances protection against repeated unauthorized attempts. Additionally, the system enforces strict rules for setting the secret key. Easily guessable words, sequential numbers or letters, and secrete codes consisting solely of alphabets or numerals are not permitted. By enforcing these constraints, the authentication input becomes more complex and resistant to brute-force and guessing attacks, thereby improving overall system security.

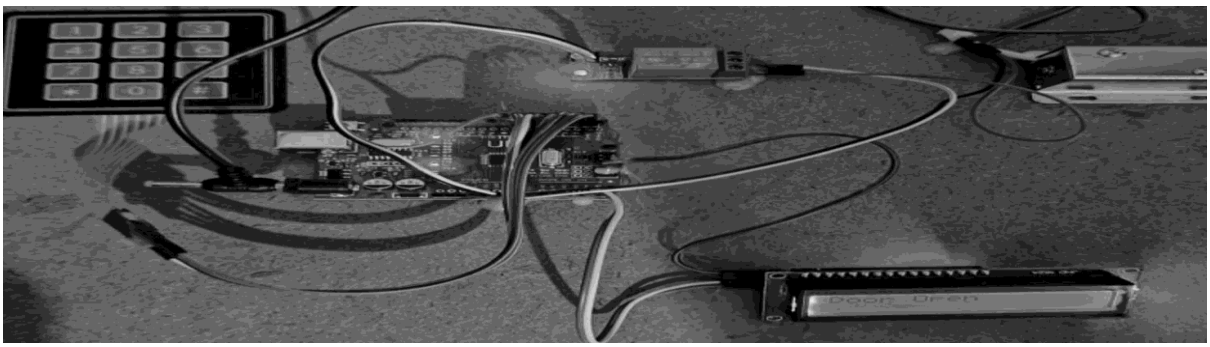

Fig 2. Users input feeding system.

2.2.1 Draw back of the present system

Safekeeping Liabilities: If the secret code is not strong or is easily guessable, the system can be bypassed. Additionally, if the code handling the secret code is not well- secured, it might be susceptible to attacks like brute force or code injection.

Incomplete Loading and Dispensation Power: Existing systems have limited memory a

process in power, which can limit the complexity and the number of features you can implement. This can make the system less robust and more susceptible to hacking.

Operator Suitability: Remembering and entering a secret code every time can be inconvenient for users. If the secret code is forgotten, it can be difficult to reset or recover without proper mechanisms in place.

Physical Sidestep: As an Existing setup is a physical device, it can be tampered with physically. Someone with access to the hardware could potentially reset the Existing setup and access the system.

Requirement on Control Source: The system relies on a continuous power supply. Any interruption in power can reset the system, potentially leading to loss of data or requiring the system to be reconfigured.

2.3 User input confirmation system:

Many existing systems operate on single-source authentication, where the user provides credentials and the system verifies them before immediately granting access. Since permission is based on only one level of verification, such systems are vulnerable to attacks and make it easier for unauthorized individuals to steal information. To overcome this limitation, the proposed system implements multi-stage authentication. In this approach, the user initially provides authentication input in the form of text, pattern, or another primary method. After successful verification at the first level, the system requires an additional layer of authentication. This second-level verification may be in the form of a one-time input a system-generated token, a confirmation message, or any other secure mechanism.

Multi-level authentication significantly improves system security. In single-source verification systems, unauthorized access may go unnoticed, especially if the owner is not present at the location. However, with multiple authentication techniques, alerts or verification messages are sent to the user through alternate channels, increasing awareness and vigilance regarding system access attempts. In the proposed system, multi-stage authentication is strictly enforced. After successful completion of the first verification stage, the second-stage authentication is performed. Access to data is granted only when both stages are successfully verified. This multi-stage verification mechanism provides higher security compared to single-stage authentication and ensures that information is protected in a highly secure manner.

2.4 Protecting the secreted code on the system repository

The proposed system operates using a multi-stage verification technique. Each time a user attempts to access the information, they are required to enter a secret key through a keypad. The entered credentials are verified against the stored credentials, and access is granted only if both matches. The system permits only two incorrect attempts. On the third incorrect attempt, the system immediately triggers a siren, alerting the surroundings about the unauthorized access attempt and encouraging users to enter the correct credentials. Before access is granted, the system generates the required authentication key based on predefined security rules. To address common vulnerabilities, the proposed system strongly enforces the use of authentication inputs that consist of a secure combination of letters, numbers, and

special characters. This significantly reduces the possibility of unauthorized users tracking or guessing the credentials.

Strict rules are enforced while creating the secret key. Easily guessable words, sequential letters or numbers, and secret codes containing only alphabets or numerals are not permitted. These constraints increase secrete code complexity and make the system resistant to brute-force and guessing attacks, thereby enhancing overall security. Additionally, once the authentication credentials are created, they are converted into an unreadable format before being stored in the system repository. This ensures that even if the system is compromised, attackers cannot interpret or misuse the stored credentials. The secure storage of encrypted credentials serves as an additional layer of protection and is a key advantage of the proposed system.

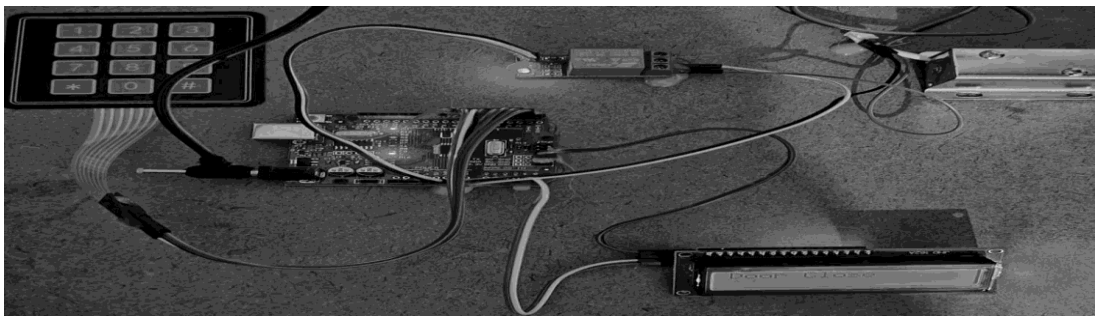

Fig 4. Display shows the input accept and action initiated.

2.5 Generate privilege control to the user

This proposed system offers better performance than existing security systems. Protecting sensitive information from third parties is one of the major concerns in day-to-day life. With the rapid growth of applications, security threats are also increasing; therefore, authentication mechanisms must continuously evolve. In many conventional authentication systems, users are required to set access credentials using a combination of alphanumeric characters. The proposed system limits access attempts by allowing only two incorrect entries. Upon the third incorrect attempt, the system immediately triggers a siren, creating an alert environment and notifying the owner of a potential security breach. This mechanism significantly enhances protection against repeated unauthorized access attempts.

Each time a user attempts to access the system, they are required to enter a secret key through a keypad, enabling a multi-stage security process. The system maintains a record of authorized users and their permitted access levels. This information is updated and controlled within the system, which is configured to monitor usage patterns and access privileges. If any unauthorized individual attempts to access the system, the event is immediately detected, and notifications are sent to the owner and relevant authorities. This ensures proactive security monitoring and effective prevention of unauthorized access.

2.6 Functional Flow:

The user enters the secret code through a keypad. The microcontroller retrieves the stored secret codes from its memory. A comparator module then compares the entered secrete code

with the stored data. Based on the comparison result, the control logic determines whether the authentication is successful. If the authentication is successful, the control logic activates the lock mechanism to unlock the system and updates the display to indicate authorized access. If the authentication fails, the lock mechanism remains locked, and the display shows an error message. The block diagram provides an overall view of the system, explaining the working principle and illustrating how various components are interconnected within the circuit. It clearly demonstrates the signal flow, control logic, and functional relationship between hardware modules.

3.Working principle:

The proposed system will work as follows 12-volt input is given to input controller by adaptor and the controller converts the 12 volts into 5 volts and it is sent to the display output at the same time 5volts supply is given to the relay. A single pole double throw relay. Why we are using relay means we are using a solenoid lock. The solenoid lock runs with 12volts DC and 1 ampere of current the controller can't able to drive the 12 volts so to give the 12volts of supply to solenoid lock we are using a driver. To work all these things, we are using a keypad. In this secrete key based lock system were using a secrete key to exposed the access and another secrete code to close the door The keypad is 3/4 keypad we are not giving any power supply to the keypad we are giving only ground so when we press the button the ground supply will be activated for particular pins. We are using display screen as I2C protocol to reduce the pins. I2C protocol is nothing but it stands for inter integrated circuit

If the secrete key is given in the right way then the output is directed to the relay the relay operates with the 5 volt DC when signal sent to the relay the current flows in the coil the current that flows in the coil generates the magnetic field and the current finally when we enter the secrete key if the input was correct then the lock will be open.

3.1 Advantage of the proposed system:

Cost-Effective: The proposed system setup and initialization are much cheaper than the present system. It uses very limited resources, and its working style does not consume much power or resources compared to the existing one.

Sustainability: The present system is easy to install and easy to enhance; it allows users to modify the existing setup and add more resources whenever required.

3.2 Usages of the proposed system

The system will work for various applications few of them listed below:

Homebased Safety Organizations: This type of setup ensures that users other than authorized users are not allowed to enter the location without proper authentication.

Workplace Admittance Regulator: Similarly, in the workplace, user entry is restricted; only authorized users are allowed to enter the premises, and others without access are denied by our proposed technique

Safe or Storeroom Schemes: In many financial organizations such as banks and other locations, users' documents or other relevant information are kept in safe locker systems. This proposed system helps users protect their information more effectively compared to existing techniques**.**

Vending Technologies: Secure vending machines or other automated dispensing systems, safeguarding that only official users can admittance or top-up the mechanism

Manufacturing Equipment: Control access to machinery or equipment in industrial settings, ensuring safety and preventing unauthorized use.

Individual Schemes: Hobbyists and makers can use Existing setup-based secrete code lock systems for various personal projects, such as securing toolboxes, drawers, or other personal items.

These applications utilize the Existing setup board in conjunction with components like keypads, display screens, and servo motors or electronic locks to create a functional and secure secrete code based locking mechanism

4. Conclusion:

The system utilizes a microcontroller-based approach to provide secure access control to restricted areas. The main components of the system include a keypad for entering the secret code, a microcontroller unit for processing inputs and controlling the locking mechanism, and an electronic lock for physically securing the door. The proposed system operates using a multi-stage verification technique. Each time a user attempts to access the system, they are required to enter a secret key through the keypad. The entered credentials are verified against the stored data, and access is granted only when both values match. The system permits a maximum of two incorrect attempts. On the third incorrect attempt, a siren is immediately triggered, alerting the surroundings of an unauthorized access attempt and prompting corrective action.

The system enhances security by requiring a valid secret code, thereby reducing the risk of unauthorized entry. It can be easily reprogrammed to update secret codes or to integrate additional security features such as radio frequency, biometric authentication, or two-factor authentication. Furthermore, the system can be scaled to control multiple locks or integrated into a larger security network. With a simple and user-friendly interface, users can easily enter and manage secret codes, making the system accessible to a wide range of users. Overall, a secret code–based lock system using Existing setup provides a practical and efficient solution for modern security requirements. Future enhancements may include implementing stronger encryption algorithms for secure code storage and transmission, incorporating biometric verification such as fingerprint or facial recognition in conjunction with secret codes, developing low-power operating modes to extend battery life, and expanding the system to manage multiple doors or access points.

5. References:

1. Lahart, Justin (27 November 2009). "Taking an Open-Source Approach to Hardware". The

Wall Street Journal. Retrieved 2014-09-07.

2. Yuvaraj singh rathore, Sourabh kumar, Prashant Saini, Ritik Jangid, Er. Mohit Mishra, Dr.Vishal Shrivastava, Dr.Ashok Kajala, Dr.Akhil Pandy, "Advanced IOT Based smart home security systems: Desing, Implementation, and future treads", International Journal on science and Technology , ISSN: 2229-7677, Pages 1, 14, 2015.

3. Barragán, Hernando (2016-01-01). "The Untold History of Existing setup". Existing setuphistory.github.io. Retrieved 2016-03-06.

4. Rami Nahas, "Samart home security systems", International journal of engineering research & technology, ISSN:2278-0181, Pages 62-67, 2020

5. How many Existing setups are "in the wild?" About 300,000". Adafruit Industries. May 15, 2011. Retrieved 2013-05-26.

6. Nandhini PK, " Securing smart homes:Challenges and solutions in IOT Cybersecurity", International journal of science engineering and technology, ISSN:2348-4098, Pages 01-07, 2024

7. Existing setup FAQ – With David Cuartielles". Malmö University. April 5, 2013. Archived from the original on 2017-09-06. Retrieved 2014-03-24.

8. Anwer, M., & Hassen, S. "Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology". https://doi.org/10.21271/ZJPAS.35.4.08, 2023.

9. Allan, Alasdair (6 March 2015). "Existing setup Wars: Group Splits, Competing Products Revealed?". makezine.com. Maker Media, Inc. Retrieved 21 April 2015.

10. Akashdeep Bhardwaj, Salil Bharany, Anas W. Abulfaraj, Ashraf Osman Ibrahim, Wamda Nagmeldin, Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities, Egyptian Informatics Journal, Volume 25, 2024.

11. J. V. Harris, "Legal implications of automated emergency calls from private security devices," IEEE Technol. Soc. Mag., vol. 40, no. 1, pp. 55–62, Mar. 2021.

12. K. R. Delgado, "Comparative study of CCTV and sensor-based systems in burglary prevention," IEEE Trans. Ind. Informat., vol. 18, no. 8, pp. 5671–5682, Aug. 2022.

13. Banzi, Massimo (19 March 2015). "Massimo Banzi: Fighting for Existing setup". makezine.com. Maker Media, Inc. Retrieved 21 April 2015.