

Patternized Secret Knock Detecting Smart Door Lock System

P A Harsha Vardhini¹, P Pavan Kumar¹, M. Sreya Bhavani², B. Prasanna², B. Tapan kumar², M. Bhargav²

¹Department of ECE, Vignan Institute of Technology & Science, Yadadri, Bhuvanagiri Dist., India

²UG Student, Department of ECE, Vignan Institute of Technology & Science, Yadadri, Bhuvanagiri Dist., India

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.140500077>

Received: 31 May 2025; Accepted: 06 June 2025; Published: 19 June 2025

Abstract: The Patternized Secret Knock Detecting Door Lock is an advanced security solution that combines simplicity and innovation by using acoustic signal recognition for access control. This system captures vibrations from knocks using a piezoelectric sensor, processes them through a microcontroller, and compares the detected pattern with a pre-programmed secret knock. Only when the knock sequence matches is the lock mechanism activated, ensuring secure and personalized access. The design is user-friendly, allowing customization of knock patterns and providing an alternative to traditional locks or keypads. It prioritizes energy efficiency, ease of installation, and resistance to tampering or false triggers. By eliminating the need for physical keys or cards, this solution minimizes the risk of unauthorized duplication and offers a discreet, reliable locking mechanism suitable for homes, offices, and restricted areas. The work highlights the practical application of embedded systems and signal processing in modern access control technologies.

Keywords: Secret Knock, Door Lock, Acoustic Signal Recognition, Piezoelectric Sensor, Microcontroller, Knock Pattern, Access Control, Security Solution, Embedded Systems, Signal Processing.

INTRODUCTION

The Patternized Secret Knock Detecting Door Lock is an innovative security solution that combines the principles of pattern recognition and acoustic signal processing to enhance access control. Traditional locking systems, such as key-based or keypad locks, are prone to risks like key duplication, code breaches, or unauthorized access. This work addresses these vulnerabilities by introducing a discreet and customizable locking mechanism that relies on detecting and recognizing a specific knock pattern as the unlocking signal. The system employs a piezoelectric sensor to detect vibrations generated by knocking on the door. These vibrations are processed by a microcontroller, which analyzes the knock sequence and compares it with a pre-programmed pattern. If the detected sequence matches the stored pattern, the system activates the door lock, granting access. This ensures a secure and user-friendly mechanism, eliminating the need for physical keys or memorizing complex passwords. Designed for ease of installation and use, the lock can be customized to recognize unique knock patterns, enhancing personalization and security. Its energy-efficient design and resistance to tampering make it suitable for residential, commercial, and restricted environments. By blending technology with convenience.

The concept of knock-based access control has been explored in various studies as a novel alternative to traditional locking mechanisms. prior works have demonstrated the use of piezoelectric sensors for vibration detection and microcontrollers for signal processing. researchers have investigated pattern recognition algorithms, such as Dynamic Time Warping (DTW) and Fast Fourier Transform (FFT), to accurately identify predefined knock sequences. studies emphasize the system's adaptability, allowing users to personalize knock patterns, enhancing security against unauthorized access. challenges like environmental noise, sensor sensitivity, and false positives have been addressed through optimized hardware and algorithmic tuning. the integration of such systems with IoT has also been explored, enabling remote monitoring and control. this survey provides insights into advancements shaping this innovative locking solution.

SMART DOOR LOCK SYSTEM

The proposed system Patternized Secret Knock Detecting Door Lock integrates a knock-based access mechanism to enhance security and user convenience. It employs a piezoelectric sensor to detect and capture knock vibrations on the door. These vibrations are converted into electrical signals and processed by a microcontroller equipped with a pattern recognition algorithm. The system allows users to set a unique sequence of knocks as the "secret pattern." When a knock is detected, the system compares the input pattern with the stored sequence. If the patterns match, the door lock mechanism is triggered to grant access; otherwise, access is denied. Key features include ease of use, energy efficiency, and high customization. The design is resistant to tampering, minimizes false positives, and eliminates reliance on physical keys or cards. This proposed system aims to offer an affordable, user-friendly, and secure alternative for residential and commercial access control.

The implementation of the Patternized Secret Knock Detecting Door Lock system involves the integration of hardware and software components to create a secure, intuitive access control solution. The core of the system consists of a microcontroller, typically an Arduino or similar embedded platform, which processes data from a piezoelectric sensor placed on the door. The sensor detects vibrations produced by knocking and converts these into electrical signals. The system is programmed to recognize specific patterns of knocks, such as the number of taps and the timing between them. These characteristics are crucial for creating a unique and customizable access pattern, which serves as the "secret knock" that unlocks the door. The microcontroller captures the signal from

the sensor and processes it using an algorithm that analyzes the pattern's duration, intervals, and frequency. This data is compared to a pre-stored pattern, stored in the microcontroller's memory. If the detected knock matches the stored pattern, the system sends a signal to a relay or motor that activates the locking mechanism, unlocking the door. If the knock sequence is incorrect, the system remains locked and does not respond. The system can also allow for the easy reprogramming of the knock pattern, providing flexibility for the user. For added security, the system includes features such as debounce algorithms to prevent false triggers caused by environmental vibrations, and an optional time-out function to temporarily lock out users after several failed attempts. The design ensures that the device is energy-efficient and easy to install. The work combines concepts of signal processing, embedded programming, and practical hardware interfacing to create a unique and effective door locking system based on secret knock patterns.

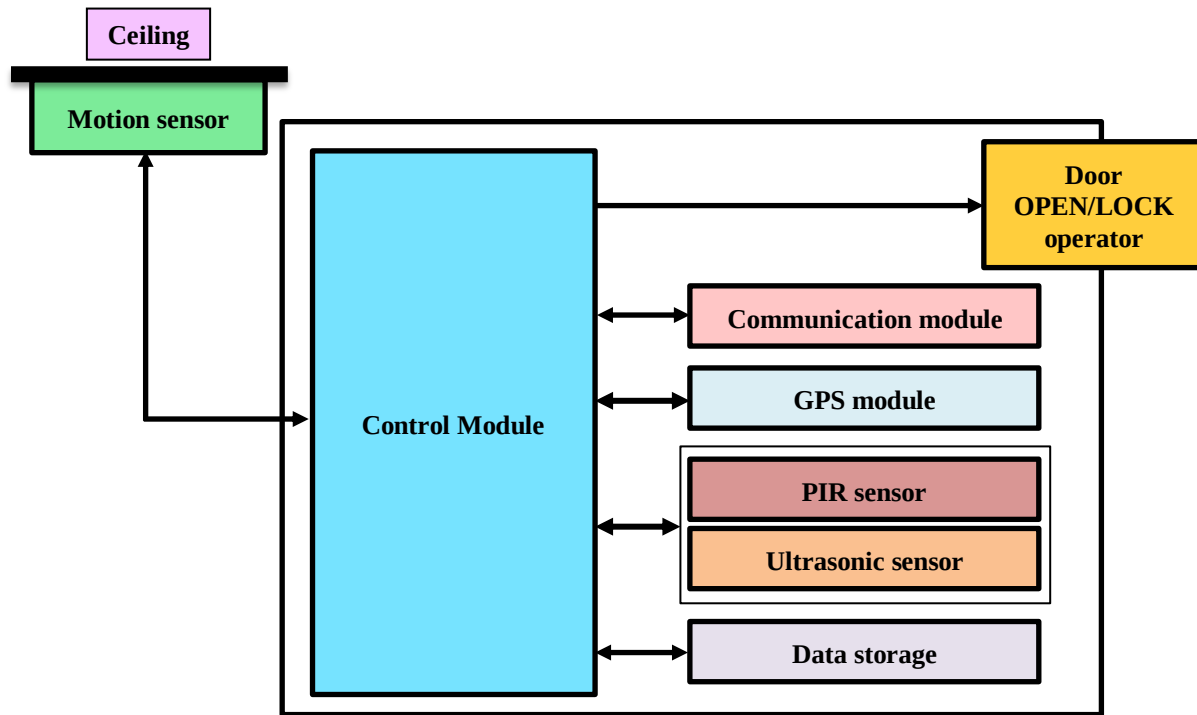


Fig 1. Smart Door Lock System

METHODOLOGY

The development of the Patternized Secret Knock Detecting Door Lock involves a multi-step approach that combines hardware design, signal processing, and software development. The methodology is outlined as follows:

System Design and Hardware Selection:

The primary components for the system include a microcontroller (e.g., Arduino or Raspberry Pi), a piezoelectric sensor to detect knocks, a motorized lock mechanism, and a power supply. The piezoelectric sensor is chosen for its sensitivity to mechanical vibrations, ensuring accurate knock detection. The microcontroller processes the input from the sensor and controls the locking mechanism based on the detected knock pattern.

Knock Detection:

The piezoelectric sensor is placed on the door frame to detect knock vibrations. These vibrations are converted into electrical signals, which are sent to the microcontroller. The microcontroller is programmed to analyze the frequency, duration, and timing of the knock signals. An algorithm is implemented to recognize and differentiate between different knock patterns, allowing the system to identify whether the knock sequence matches the pre-programmed "secret" pattern.

Pattern Recognition and Validation:

The knock pattern is recorded by the system during an initial setup phase. The user programs their unique knock pattern into the system by tapping a sequence on the door. The system stores this pattern in memory, and during subsequent knock events, it compares the detected sequence with the stored pattern. If the pattern matches, the system sends a signal to the motorized lock to unlock the door.

Security and False Trigger Prevention:

To enhance security, the system incorporates a delay mechanism to prevent false triggers from accidental knocks. Additionally, a counter for unsuccessful attempts is included, which can trigger an alarm or temporarily disable the system after a set number of failed attempts.

User Interface and Customization:

A simple interface is developed, allowing users to set, reset, or change their secret knock pattern through a mobile app or physical buttons on the device. The system provides ease of use and flexibility in adjusting security settings.

Overall, this methodology combines signal processing, embedded systems, and mechanical design to create a user-friendly yet secure locking solution based on patternized acoustic signals.

RESULTS

The Patternized Secret Knock Detecting Door Lock successfully demonstrated secure, convenient access control by accurately detecting and verifying custom knock patterns. The system reliably activated the lock mechanism only after matching the predefined sequence, ensuring high security and minimal false triggers, proving its effectiveness in real-world scenarios.

Advantages of the Patternized Secret Knock Detecting Door Lock

The Patternized Secret Knock Detecting Door Lock offers several significant advantages over traditional locking systems, making it a highly innovative and secure solution for modern access control.

Enhanced Security: The system relies on a unique and customizable secret knock pattern, which significantly reduces the likelihood of unauthorized access. Unlike conventional locks, which can be easily picked or copied, the knock pattern adds an additional layer of security that is difficult to replicate.

User-Friendly: The system eliminates the need for physical keys, access cards, or PIN codes, making it more convenient for users. The user can set and change their secret knock pattern at any time, offering both flexibility and ease of use.

Discreet and Stealthy: The knock-based entry method is discreet, preventing onlookers from detecting or guessing the unlock pattern. This feature is particularly useful in sensitive or private environments.

Customization and Personalization: Users can customize the knock pattern to their liking, offering greater personalization for different individuals or security needs.

Tamper Resistance: The system's design is resistant to traditional bypass methods like lock picking or key duplication, enhancing the overall robustness and reliability of the door lock.

Cost-Effective: With fewer hardware components and a focus on acoustic sensing technology, the system can be produced at a relatively low cost, offering affordable security without sacrificing quality.



Fig 2: prototype of patternized secret knock detecting door lock & working demonstration

CONCLUSION

In conclusion, the Patternized Secret Knock Detecting Door Lock offers a unique and secure solution for access control, combining convenience with advanced technology. By using acoustic signal processing to detect personalized knock patterns, the system provides an intuitive and tamper-resistant alternative to traditional locking mechanisms. Its ease of use, customization options, and energy efficiency make it a practical choice for enhancing security in various settings. This work demonstrates the potential of

integrating embedded systems and pattern recognition to create innovative, reliable security solutions that reduce risks and improve user experience.

REFERENCES

1. Singh, S., & Rani, K. (2019). Internet of Things in Smart Homes: Security and Privacy Challenges. *International Journal of Security and Its Applications*, 13(6), 13-24.
2. Patel, K., & Desai, S. (2020). Authentication Protocols in Smart Locks and IoT Systems. *Journal of Security Engineering*, 18(1), 45-57.
3. Hussain, M., & Xu, X. (2021). Securing IoT-Based Smart Homes: A Review of Current Trends and Solutions. *Journal of Internet Technology*, 22(2), 361-370.
4. Harivardhagini, S. (2017). LabVIEW based greenhouse automation. *CVR Journal of Science and Technology*, 13, 79-82.
5. Hussain, S. J., & Ramyasri, G. (2019). Security enhancement for devices using restapi, middleware iot gateway. *International Journal of Engineering and Advanced Technology (IJEAT)*, 2249-8958.
6. Vardhini, Palagiri Anjani Harsha, et al. "Design and development of cost-effective fingerprint-based exam hall corroborate system." *AIP Conference Proceedings*. Vol. 3157. No. 1. AIP Publishing LLC, 2025.
7. Javvaji, K. S. S., Nelakuditi, U. R., & Dadi, B. P. (2020, July). IoT based cost effective home automation and security system. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.
8. Vardhini, P. H., & Babu, K. M. C. (2017). Implementation of low cost IOT based home automation system on SPARTAN FPGA. *Recent Advances in Electronics and communications RAECE-2K17/Special issue. International Journal of Recent trends in engineering and Research*, 513-516.
9. Xie, J., & Zhang, Y. (2019). IoT Security for Smart Locks: Vulnerabilities and Countermeasures. *Computer Science Review*, 32, 55-68.
10. Vardhini, P. H., & Babu, K. M. C. (2018). Home Automation System with Remote Android Smart Device for Physically Challenged. *Journal of Applied Science and Computations*, 5(8), 967-972.
11. Krishna, A. Sai, et al. "Design & Development of Embedded Application Software for Interface Processing Unit (IPU)." *International Journal of Research in Engineering and Technology (IJRET)* 3.9 (2014): 212-216.
12. P. A. H. Vardhini, R. Pavan Kumar, T. Singh, H. V. R. Puliyala and S. Chamarthy, "Efficient IoT based Smart Home Assistance System with Electrical Control Unit," *2022 International Mobile and Embedded Technology Conference (MECON)*, Noida, India, 2022, pp. 475-479, doi: 10.1109/MECON53876.2022.9752276.
13. K. M. Chandra Babu and P. A. Harsha Vardhini, "Brain Computer Interface based Arduino Home Automation System for Physically Challenged," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, 2020, pp. 125-130, doi: 10.1109/ICISS49785.2020.9315999.
14. B. Sricharan, J. U. Sanjana, T. V. Vani and C. N. Sujatha, "RFID Based ATM Security System Using IOT," *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*, Hyderabad, India, 2022, pp. 1-6, doi: 10.1109/ICICCSP53532.2022.9862486.
15. Raju, N., et al. "IoT-based Door Access Control System using ESP32 CAM." *International Journal of Engineering Inventions* 11.12 (2022): 9-15.
16. Vardhini, P. H., Sai, M. H. V., & Matta, B. (2022, March). Human footstep power harvesting systems using piezoelectric sensor technology. In *2022 international mobile and embedded technology conference (MECON)* (pp. 450-454). IEEE.
17. Krishnaveni, S., Harsha Priya, M., & Harsha Vardhini, P. A. (2022). LabVIEW Implemented Smart Security System Using National Instruments myRIO. In *Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021* (pp. 129-136). Singapore: Springer Nature Singapore.
18. Vardhini, P. H., Sreenidhi, A., & Sai, M. H. V. A Smart Asset Tracking System with IoT for Women and Child Safety Applications.
19. Vardhini, P. A. H., Swaraja, K., Sai, M. H. V., Vignesh, N. A., Narsaiah, M. N., Rawat, B., & Vafaeva, K. M. (2025, April). Design and development of cost-effective fingerprint-based exam hall corroborate system. In *AIP Conference Proceedings* (Vol. 3157, No. 1, p. 040004). AIP Publishing LLC.
20. Ananthula, N., & Vardhini, P. H. (2021, November). Design and Implementation of Internet of Things based Spybot. In *2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT)* (pp. 63-67). IEEE.
21. Ramalatha, M., Ramkumar, A. K., Selvaraj, S., & Suriyakanth, S. (2014). RFID based personal medical data card for toll automation. *Elysium Journal Engineering Research and Management*. Volume1, ISSN, 2347-4408.