ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR814

A 2-Way Verification Process using One Time Password Key for Home Authentication System

M. Premalatha[1] (Assistant Professor)
Department of ECE, Guru Nanak
Institute of Technology, Hyderabad

Dr. N. Srinivas[2] (Associate Professor)
Department of ECE, Guru Nanak
Institute of Technology, Hyderabad

Narendar Reddy S[3]
Department of ECE, Guru Nanak
Institute of Technology, Hyderabad

Prashanth Reddy T[4]
Department of ECE,Guru Nanak
Institute of Technology, Hyderabad

Sahithi Y[5]
Department of ECE, Guru Nanak
Institute of Technology, Hyderabad

Abstract:- The goal of this research project is to make it possible to implement extra security measures in place of employment and residence.In the suggested system, A 2-way verification technique is applied. First, the data is stored in the Electrically Erasable Programmable Read Only Memory (EEPROM) password for security. If the user enters the correct password, a randomized verification One Time Password or key is sent via paired Bluetooth and user device which is smartphone for 2 -way verification. If the entered key or OTP matches, the system will be opened and the required job may be begun. If either the key or the OTP is entered incorrectly, access is denied and the user can have a few attempts--three chances under the suggested approach. The main objective is to develop a complete home security system using wireless devices and embedded (micro controller) technology.

Keywords:- *One Time Password , EEPROM , Micro Controller.*

I. INTRODUCTION

Over the years, a variety of control systems have been meticulously designed to counteract unauthorized access, with locks serving as the front line defence for our homes, schools, offices, and buildings. The core objective of deploying locks is undeniably the security of lives and property. The prevalence of automatic door systems in contemporary structures has become a standard feature, offering a seamless and convenient means of achieving security.

The relentless increase in crime rates has elevated home security to a paramount concern, prompting a collective desire for effective measures against unauthorized access. This escalating need has fueled the development of sophisticated electronic devices dedicated to fortifying security. In this context, the micro controller-based digital lock emerges as a beacon of modern access control systems.

This innovative digital lock serves as a guardian for restricted areas, allowing entry exclusively to authorized individuals. Tailored for diverse environments, it finds optimal utility in corporate offices, automated machines like ATMs, and homes seeking enhanced security measures. By limiting access to designated personnel, this digital lock aligns with the contemporary emphasis on precision security solutions, offering a practical response to the evolving challenges associated with unauthorized access in a world increasingly conscious of safeguarding its occupants and possessions.

II. EXISTING SYSTEM

The existing systems provide only single factor authentication that leads to less secure system. In this prototype Device Tampering: Physical tampering with the lock system, such as attempting to manipulate or hack into the OTP plays major role in providing security. The micro controller-based digital lock offers a cost-effective and highly secure solution, aligning with the prevalence of OTP- based authentication methods, including those used in Aadhar and banking systems. As nearly 90% of authentication relies on OTP, the system leverages this widespread approach to provide a low-cost service without compromising on security. By integrating OTP technology, it ensures robust authentication comparable to or exceeding existing security systems. This dual advantage of affordability and high security makes the micro controller-based digital lock a compelling choice in the landscape of access control systems.Code Interception: Cyber attackers may attempt to intercept or eavesdrop on the communication between the micro controller and connected devices, potentially gaining unauthorized access to OTPs. Micro controller, poses a security risk. Robust tamper detection mechanisms are essential to mitigate this risk.3. Weak Encryption: If the communication channels or stored data are not adequately encrypted, there is a risk of attackers deciphering sensitive information, including user credentials and access logs. Software Vulnerabilities: Bugs or vulnerabilities in the software running on the micro controller may be exploited by attackers to compromise the security of the system. Regular software updates and security audits are crucial to address such issues. Insufficient User Authentication:

Inadequate user authentication measures, such as weak PINs or easily guessable OTPs, can make it easier for attackers to gain unauthorized access.6. Lack of Two-Factor

Authentication: Relying solely on OTPs without additional authentication factors can leave the system vulnerable. Limited Physical Security: In scenarios where the physical security of the lock hardware is insufficient, attackers may exploit weaknesses in the casing or installation to gain access to critical components. Power Source Vulnerabilities: If the power source is not adequately secured, attackers may disrupt the power supply, potentially leading to a loss of functionality or unauthorized access during power outages.

Addressing these challenges requires a comprehensive approach, involving regular security updates, encryption protocols, user education on secure practices, and the implementation of robust physical and cyber safeguards. Regular security assessments and staying informed about emerging threats are essential to maintaining the effectiveness of micro controller-based OTP lock systems.

III. PROPOSED SYSTEM

The proposed system employs a robust A 2- way verification approach, integrating both password and OTP mechanisms to enhance security. In this system, a randomized verification One Time Password or key is transmitted via paired Bluetooth and user device which is smartphone, constituting the second layer of verification. The user initiates the process by inputting the correct password, and upon successful entry, the OTP is sent for 2-way verification. If the entered OTP matches the generated code, the system grants access, enabling the user to perform necessary actions. By combining these elements, the system not only achieves heightened security but also aligns with the modern trend of utilizing smart and interconnected technologies to fortify access control in residential environments. Enhanced Encryption: Implement advanced encryption protocols to secure communication channels, preventing unauthorized access and eavesdropping. Utilizing algorithms for encryption which are highly standard for data protection. Supervision of Key: Implement supervision of key performs to safeguard cryptographic keys used for OTP generation and verification. Bio metric Authentication: Integrate biometric authentication, such as fingerprint or facial recognition, as an additional layer of user verification. This adds a unique and secure identifier beyond traditional PINs or OTPs. Continuous Security Audits:Conduct regular security Auditsto identify and address vulnerabilities in both hardware and software components. This proactive approach helps in staying ahead of potential threats. Two-Factor Authentication: Enforce two-factor authentication, combining OTPs with another authentication factor like biometrics or a hardware token. Secure Boot and Firmware Updates: Implement secure boot processes to ensure the integrity of the firmware. Enable secure over-the-air firmware updates to address vulnerabilities promptly and keep the system up-to- date. Physical Security Enhancements: Strengthen the physical security of the lock system by using tamper-resistant casings, anti-drill components, and secure mounting mechanisms to deter and detect physical tampering attempts. Advanced Tamper Detection: Integrate advanced tamper detection mechanisms that can identify and respond to various physical tampering methods, triggering alarms and preventing unauthorized access. Multi-User Permissions: Allow for granular control over user permissions, specifying different access levels for various users. This ensures that each user has the appropriate level of access based on their roles and responsibilities.10. Secure Mobile App Communication: If applicable, secure the communication between the micro controller and the mobile app, using encryption and secure protocols to prevent potential attacks on the app interface. Power Source Redundancy: implement power redundancy solutions, such as backup batteries or alternative power sources, to ensure the system remains operational during power outages or disruptions. By incorporating these proposed features, the micro controller-based OTP Lock system can significantly enhance its overall security posture, providing a robust and resilient solution for integrated home security. Regular updates, user education, and collaboration with cyber security experts can further contribute the system's effectiveness in thwarting potential threats.

IV. METHODOLOGY

The proposed system employs a robust A2- way verification approach, integrating both password and OTP mechanisms to enhance security. In this system, a randomized verification code is transmitted through paired bluetooth and user device which is smartphone, constituting the second layer of verification. The user initiates the process by inputting the correct password, and upon successful entry, the OTP is sent for 2- way verification. If the entered OTP matches the generated code, the system grants access, enabling the user to perform necessary actions. To discourage unauthorized attempts, the system imposes restrictions on access after a certain number of incorrect password or OTP entries. This multi-layered verification system ensures a comprehensive and secure home security setup, leveraging embedded micro controller technologies and wireless communication devices. By combining these elements, the system not only achieves heightened security but also aligns with the modern trend of utilizing smart and interconnected technologies to fortify access control in residential environments. User Authentication Request: When a user approaches an entry point, they initiate the authentication process, typically by entering a code or triggering a sensor. Input Verification; The micro controller receives the input (e.g., entered code) and verifies it against stored user data. This can include comparing the entered OTP with the one generated by the system. OTP Generation: If OTP- based, the system generates a unique, time-sensitive OTP based on algorithms and predefined parameters. This OTP is sent to the user or displayed on a keypad or screen. User Confirmation: The user confirms their identity by entering the received OTP into the system, either through a keypad or touchscreen. Authentication Process: The micro controller compares the entered OTP with the generated one. If they match within the predefined validity period, authentication is successful. Lock Control: Upon successful authentication, the micro controller triggers the locking mechanism, allowing access to the secured area. In case of failure, access is denied. Status Monitoring: Sensors continuously monitor the status of entry points. Any unauthorized access attempts or unusual activities trigger an alert or alarm. Communication and Logging: The system communicates the authentication status to external devices or a central monitoring station. Access logs are updated with details of each access attempt, providing a record for security monitoring. Emergency Access: In case of system malfunctions or emergencies, authorized personnel can use backup mechanisms, such as emergency codes or physical keys, to gain access. Power Management: The system manages power efficiently, and low power consumption mechanisms may be implemented, especially if using battery-powered setups. Tamper Detection: Tamper detection mechanisms identify and respond to any attempts at physical tampering, further securing the system. The working principle emphasizes secure user authentication, real-time monitoring, and response mechanisms to ensure the integrity of the home security system. The integration of OTPs, sensors, and communication modules enhances the overall effectiveness of the system in providing a reliable and robust security solution.

➢ *Flow Chart*

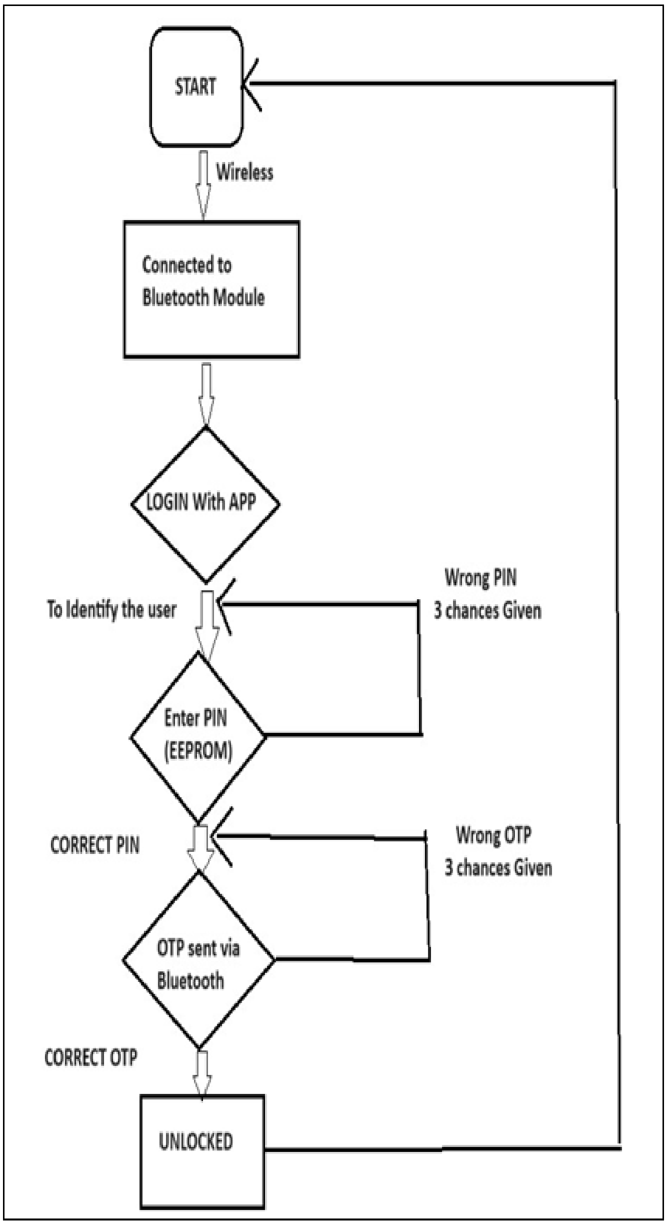

Fig 1 Flowchart of Working

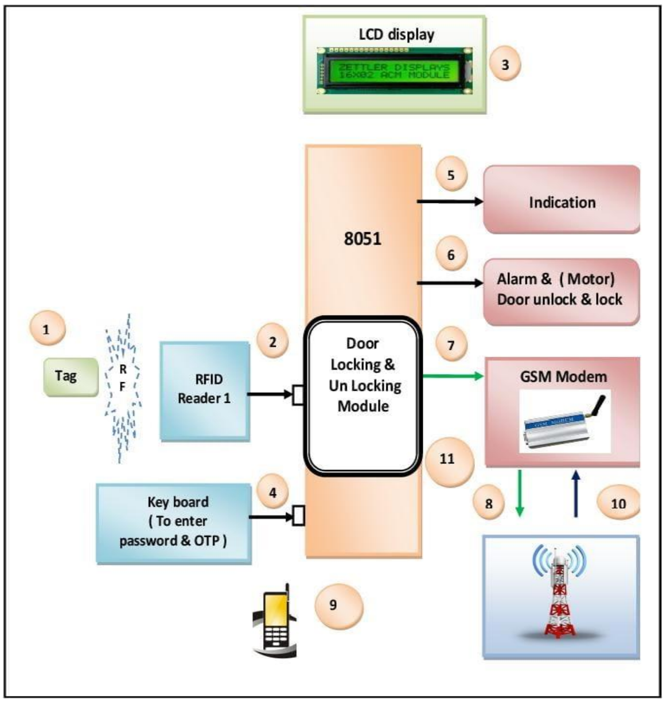
LCD display
3
8051
5
Indication
6
Alarm & (Motor) Door unlock & lock
1
Tag
R F
RFID Reader 1
2
Door Locking & Un Locking Module
7
GSM Modem
11
4
Key board (To enter password & OTP)
8
10
9

Fig 2 Hardware Model Development

➢ *Block Diagram*

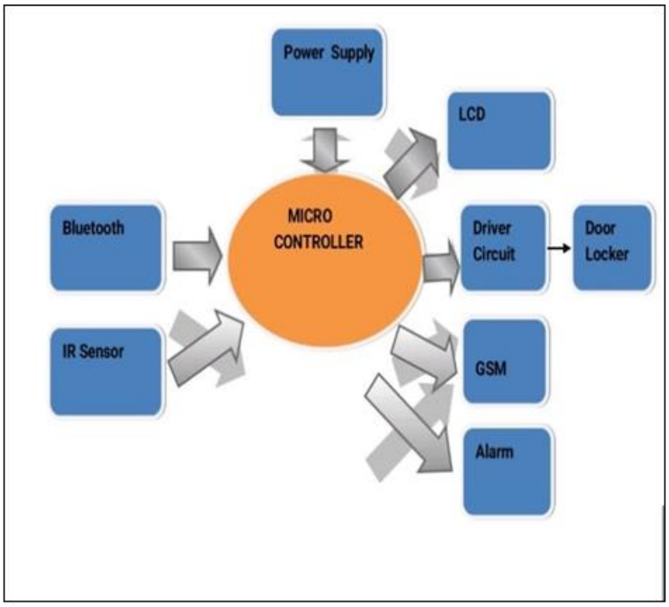

Fig 3 Block Diagram

➢ *Applications*

- *Access Control*
- *Remote Authorization*
- *Multi-Level Security*
- *Emergency Access*
- *Low Power Consumption*
- *Residential Security*
- *Office Security*
- *Rental Properties*
- *Smart Homes*
- *Security-sensitive Areas*

V. HARDWARE DETAILS

The ATmega16 is a low-power CMOS 8-bit micro controller based on the AVR enhanced RISC Architecture. The ATmega16 is a versatile 40-pin micro controller with significant memory capabilities. It features 16 KB of programmable flash memory, allowing users to store and execute program code. Additionally, it possesses 1 KB of static RAM, providing temporary data storage during program execution, and 512 Bytes of EEPROM, offering non-volatile memory for critical data storage that persists even when the power is off. The micro controller is equipped with 32 1/0 (input/output) lines, which are divided into four 8-bit ports named PORTA, PORTB, PORTC, and PORTD. These ports facilitate communication with external devices and sensors, enabling the micro controller to receive inputs and produce outputs. The flexibility of having multiple ports allows for efficient interfacing with various components, enhancing the overall functionality and adaptability of the ATmega16 in embedded systems and micro controller-based projects. The Pin is saved in the EEPROM. This Pin could be reset when required. If the Pin is wrong then the user is prompted to enter the Pin again (3 Chances given). If the user fails to enter the correct Pin for more than 3 times the system is disabled. If the entered Pin is correct then for 2–way verification, an OTP is sent on the user's device via.The HC-05 Bluetooth Module has 6 pins- EN, Vcc, GND, TX, RX and State [4]. The HC-05 Bluetooth Module serves as a versatile solution for wireless communication, supporting both Master and Slave configurations. This flexibility makes it suitable for various applications where reliable wireless data transfer is essential. The typical range for Bluetooth communication with the HC-05 is around 30 meters or less, making it suitable for short-range wireless connections.

An LCD screen is an electronic display module that provides visual output. A 16×2 LCD, as mentioned, can display 16 characters per line across two lines. Each character is represented by a 5x7 pixel matrix. The LCD features two registers - the Command register, storing instructions for the LCD, and the Data register, storing the ASCII values of characters to be displayed. This configuration allows for control and customization of the displayed content.

For user input, a Keypad 4x4 is utilized to load numeric data into the micro controller. This keypad consists of 16 buttons arranged in a 4x4 array, forming four lines and four columns. It requires only one port pin to read a digital input into the micro controller. The matrix arrangement of the keypad efficiently reduces the pin count, making it practical for scenarios with numerous digital inputs.

In summary, the combination of the HC-05 Bluetooth Module, LCD screen, and Keypad 4x4 provides a comprehensive solution for wireless communication, visual output, and user input in micro controller-based systems.

The hardware components for a micro controller-based One Time Password Key For Home Authentication System typically include: Micro controller: The heart of the system, responsible for processing and controlling operations. Common choices include Arduino, Raspberry Pi, or specialized micro controllers with integrated security features. Locking Mechanism: Physical hardware responsible for securing entry points, such as an electronic lock, electromagnetic lock, or motorized deadbolt. Keypad or Touchscreen: Input interface for users to enter their OTPs or additional authentication credentials. Can be a physical keypad or a touchscreen display. OTP Generator: The component responsible for generating one-time passwords based on algorithms and time- sensitive parameters. This could be implemented within the micro controller or as a separate module. Sensor s: Various sensors like door/window sensors and motion detectors to monitor the status of entry points and detect any unauthorized access attempts. Communication Module: Enables communication between the micro controller and external devices, such as a Wi-Fi or Bluetooth module for remote access and monitoring. Power Supply: Provides the necessary power to the system, usually through batteries or a direct power source. Emergency Backup: A backup power source or alternative entry method (emergency codes, physical keys) for situations where the primary system may fail. Enclosure: Protects the components from environmental factors and tampering, ensuring the system's reliability and durability. Indicator Lights or Display: Visual indicators to communicate the status of the lock system, showing whether it's locked, unlocked, or in an alarm state. Microphone and Speaker (optional): For incorporating audio features, such as voice- based commands or alarms. Tamper Detection Mechanism: Detects and responds to any attempts at tampering with the lock system, enhancing overall security. The specific hardware details can vary based on the chosen micro controller, the complexity of the system, and the desired features. Integration of secure communication protocols and encryption mechanisms is essential to ensure the overall security of the home security system.

VI. DESCRIPTION OF SOFTWARE

Embedded C compiler based software is used to create a hex file from Embedded C code. Then simulation software is used to test the prepared code (fig. 2). After successful testing of prepared Embedded C code. Then another software is used to burn the hex file inside the MCU [10]. Using One Time Password Key For Home Authentication System is a software solution designed to enhance security by incorporating a one-time password (OTP) mechanism. This software enables communication between the micro controller and various components of the home security system to ensure secure access. Overall, the micro controller-based OTP Lock software provides a robust and adaptable solution for integrated home security, ensuring a high level of protection against unauthorized access. OTP Generation: The software generates unique, time-sensitive OTPs for user authentication, adding an extra layer of security. User Management: Allows administrators to add, modify, or remove users, assigning unique credentials for access control. Integration with Sensors: Interfaces with sensors like door/window sensors, motion detectors, ensuring real-time status updates. Mobile App Integration: Provides the ability to manage and monitor the lock system remotely through a dedicated mobile application. Logging and Reporting: Records access attempts, successful or otherwise, providing a detailed log for security monitoring and analysis. 6. Emergency Access: Implements a backup mechanism or emergency codes for authorized personnel to access the property in case of system malfunctions. Secure Communication: Utilizes encryption protocols to secure communication between the micro controller and connected devices, preventing unauthorized access. Multi-factor Authentication: Supports additional authentication factors, such as PIN codes, to enhance overall security. Tamper Detection: Incorporates mechanisms to detect and respond to any attempts at tampering with the lock system. Customization: Allows users to customize settings like OTP validity period, access permissions, and notification preferences.

- *Simulation Result*

Table 1 Comparison of Integrated and Manual Locking System

Feature	Integrated System	Manual System
Convenience	Integrated locks are more convenient because they can be opened and closed with a secured code i.e. OTP.	Manual locks require the user to physically unlock and lock the door.
Security	These are more secure because they can be controlled through additional security features.	Manual locks can be picked or forced open, making them less secure.
Maintenance	Requires regular maintenance.	Requires minimal maintenance.
Cost	More expensive because of their advanced technology.	Less expensive.

Table 2 Comparison of Existing System with Proposed System

Feature	Existing System	Proposed System
Lock Mechanism	Traditional key-based locks	Micro controller controlled lock with OTP
Integration	Limited integration with other devices	Seamless integration with home automation systems
Emergency Access	Limited options	Provision for emergency access protocols
Remote Access	Limited or absent	Remote access and control through mobile apps
User Authentication	Key possession-based	OTP generation for each access attempt.

- *Schematic Diagrams*

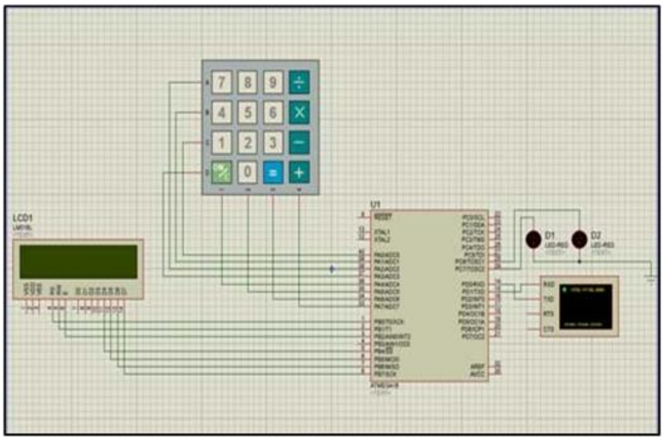

Fig 4 Proteus Simulation

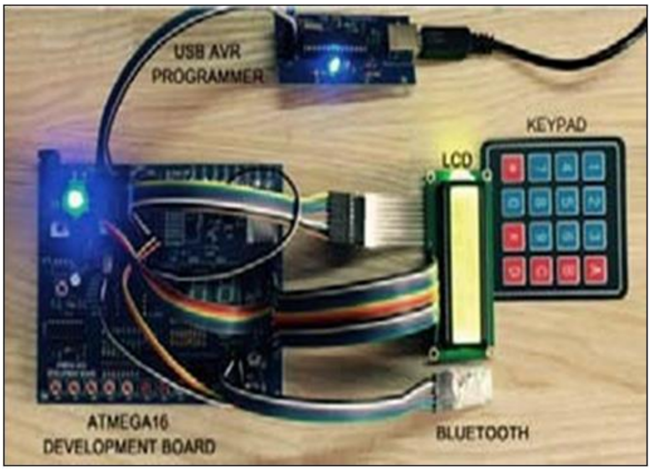

Fig 5 Hardware

VII. CONCLUSION

The project aims to address the common issue of forgetting keys or accidentally getting locked out of one's home. In such scenarios, gaining access can be challenging. The proposed solution offers a keyless entry system to alleviate these concerns while enhancing security.

By implementing a keyless entry system, individuals can access their homes without the need for traditional keys. This is particularly beneficial in situations where keys are forgotten or misplaced. Additionally, the system provides a secure alternative to conventional locks, reducing the risk associated with physical keys being lost or stolen. Project likely incorporates advanced technologies such as electronic locks, password or PIN-based entry, or even biometric authentication for enhanced security. The integration of such features not only ensures convenient access but also enhances the overall safety of the home.

In summary, the key less entry system serves as a practical and secure solution to the common problem of forgetting keys or accidentally getting locked out. It introduces modern and reliable methods of access control, providing individuals with a more convenient and secure means of entering their homes. In conclusion, the micro controller-based One Time Password Key For Home Authentication System offers a promising solution to enhance access control and safeguard residential spaces. While this technology provides advanced security features, it is crucial to address existing vulnerabilities and continuously improve the system's overall resilience. The proposed enhancements, including advanced encryption, biometric authentication, continuous security audits, and physical security measures, contribute to fortifying the system against cyber threats and unauthorized access. Implementing two-factor authentication, secure firmware updates, and multi-user permission controls further elevate the system's security posture. However, it's essential to recognize that security is an ongoing process, and staying vigilant against emerging threats is paramount. Regular updates, user education on secure practices, and collaboration with cyber security experts are key elements in maintaining the effectiveness of the micro controller-based OTP Lock. In deploying and utilizing this technology, a balanced approach that considers both the hardware and software aspects, as well as the human factor, will contribute to a robust and reliable home security solution. As advancements in technology continue, adapting the system to incorporate the latest security standards and practices will ensure its relevance and effectiveness in safeguarding homes in the ever-evolving landscape of security challenges.

ACKNOWLEDGMENT

This paper is an acknowledgement to the inspiration, drive and technical assistance contributed by many individuals. This project would have never seen light of this day without the help and guidance we have received. We would like to express our gratitude to all the people behind the screen who helped us to transform an idea into a real time application.

REFERENCES

[1]. S. Sreekanth, M. Sandeep, N. Santhosh, M.V. Devaraja and J.B. Kalaiah, "Design and Prototype Development of OTP based advanced digital Locking system", International Research Journal of Modernization in Engineering Technology and Science, vol. 03, no. 07, July 2021.

[2]. Chaitanya Rane, “Password Based Door Locking System Using GSM”, International Journal of Engineering Trends and Applications (IJETA), Volume 2 Issue 4, July-Aug 2015.

[3]. K. M. Pooja, K. G. Chandrakala, M. A. Nikhitha and P. N. Anushree, "Finger print based bank locker security system", Int. J. Eng. Res. Technol. (IJERT)NCESC, vol. 6, no. 13, pp. 1-5, 2018.

[4]. https://wiki.eprolabs.com/index.php?title=Bluetooth_Module_HC-05.

[5]. P. Deeksha, M.K. Mangala Gowri, R. Sateesh, M. Yashaswini and V. Ashika, "B. OTP Based Locking System using IOT", International Journal of Research Publication and Reviews, no. 2, pp. 352-356, 2021.

[6]. S.K.Dubey , “PASSWORD BASED SECURITY LOCK SYSTEM”, International Journal of Advanced Technology in Engineering and Science, Volume No.02, Issue No. 05, May 2014.

[7]. Hitachi, “LCD HD44780 datasheet”, Hitachi.

[8]. Muhanad Hayder Mohammed, "Secure Electronic Lock using PIC 16F628A Microcontroller". International Journal of Research in Computer Science, 2 (5): pp. 43-47, September 2012.

[9]. S. D. Nivethika, T. Nivethetha, P. Priyadharshini, V. T. Nithyasri, M. Senthil Pandian and R. Shiva prasad, "Design and Development of Pipe inspection Snake Locomotion Robot", 2022 International Conference on Power Energy Control and Transmission Systems (ICPECTS), pp. 1-5, 2022.

[10]. S. Daegyu, G. Hanshin and N. Yongdeok, Design and Implementation of Digital Door Lock by IOT KIISE Transactions on Computing Practices, vol. 21, no. 3, pp. 215-222, 2015.

[11]. Abhinav Kumar, Salil Choudhary, “Android Based Message Conveying System Using Bluetooth”, Elins International Journal of Science Engineering & Management (EIJSEM), Volume-1, Issue-1, May 2016.