NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 9, ISSUE 1, Jan. -2022

DESIGN AND IMPLEMENTATION OF OTP BASED DOOR LOCKING SYSTEM

Shravani Nerli
Department of Electronics and Communication,
REVA University, Banglore, India
*Shravani.nerli@gmail.com

Smita T. S.
Department of Electronics and Communication,
REVA University, Banglore, India
* Smitasudesh@gmail.com

N. Raksha
Department of CS, REVA University, Banglore, India
* Raksha.n2029@gmail.com

ABSTRACT
Vulnerability to criminality is emerging as a new social problem as the incidence of single-parent households rises rapidly. The fear of stranger visitors is known to be the main worry for single female households. The proposed system's goal is to give additional security measures that may be employed in both homes and offices. The secret word for security is first stored in the Electrically Erasable Programmable Read Only Memory [EEPROM] in this innovation. If the user inputs the proper password, a randomly generated OTP is delivered to the user's device via Bluetooth for two-way verification. The system will be unlocked and the required task can be started if the entered OTP matches. If either the password or the OTP is incorrect, access is prohibited, and the user is given a limited number of opportunities (3 chances in the proposed system). Our main goal is to use wireless (Bluetooth device) and embedded (Microcontroller) technology to create an integrated home security system. When compared to other security systems, the suggested solution delivers a low-cost service with guaranteed high security.

Keywords: OTP, Bluetooth, Security, EEPROM**.**

INTRODUCTION

Over the years, a variety of control methods have been developed to prevent unwanted users from gaining access. The primary goal of installing locks in our homes, schools, offices, and other structures is to ensure the safety of our lives and belongings. As a result, having an easy approach to accomplish this goal is critical. Many various types of buildings and homes now include automatic door systems as a basic feature. And developing effective electronic devices that provide security is getting increasingly popular. Because of the rise in crime, home security has become a big concern, and everyone wants to take steps to prevent unwanted access. This micro controller-based digital lock is an access control system that allows only authorised individuals to enter a limited area. This system is ideal for corporate offices, automated machines (ATMs), and home protection. Because of the rapid growth of the IOT market, businesses will increasingly focus on the chance to display and provide products as quickly as possible rather than developing a secure significant product. As a result, a variety of IOT devices now have adequate protection against a variety of malicious attacks. IOT security is a constantly evolving topic, and despite the fact that there has been a lot of research done on it, there hasn't been a lot of significant work done on executions or standardizations that

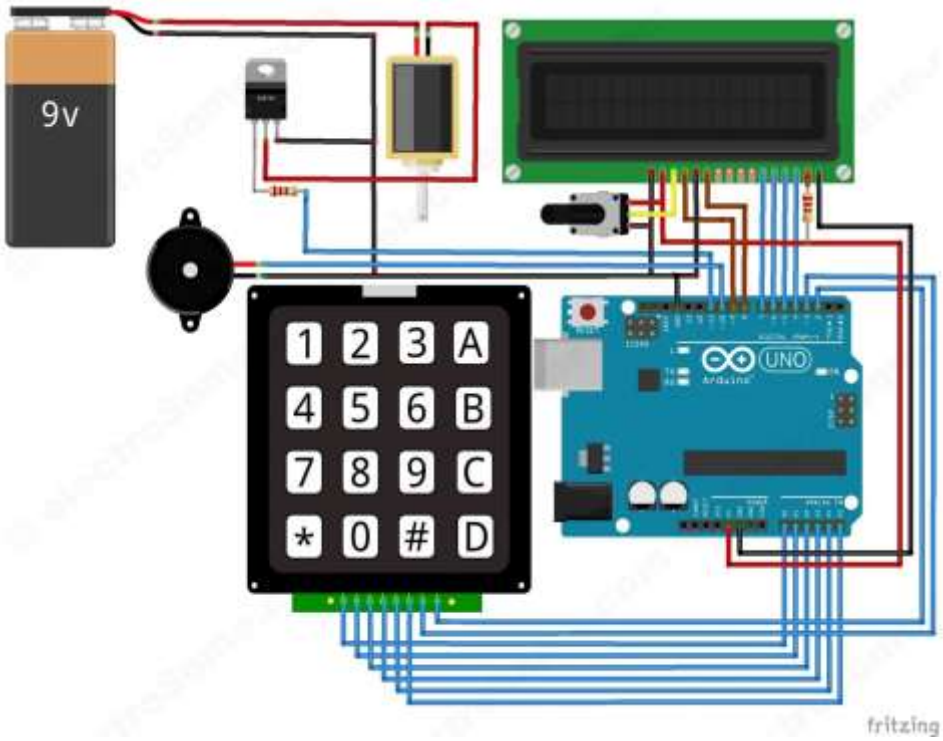
could address this issue. IOT security is extremely important since the consequences of security breaches in IOT can be catastrophic. In some exceptional circumstances, a breach in a smart automobile or clever entryway lock could result in the theft of valuables or even losses

METHODOLOGY

Software: To generate a hex file from Embedded C code, software based on the Embedded C compiler is utilized. The code is then put through its paces using simulation software. After the prepared Embedded C code has been successfully tested. The hex file is then burned inside the MCU using another piece of software.

Hardware: The ATmega16 is a low-power 8-bit CMOS microcontroller that uses the AVR enhanced RISC Architecture. The ATmega16 features 16 KB of programmable flash memory, 1 KB of static RAM, and 512 bytes of EEPROM. The ATmega16 microcontroller has 40 pins. There are 32 input/output (I/O) lines separated into four 8-bit ports labeled PORTA, PORTB, PORTC, and PORTD. EN, VCC, GND, TX, RX, and State [4] are the six pins on the HC-05 Bluetooth Module. The HC-05 Bluetooth Module is a wonderful solution for wireless communication because it may be used as a Master or Slave. Bluetooth communication typically has a range of 30 meters or less. A liquid crystal display (LCD) screen is a type of electronic display module. A 16x2 LCD can display 16 characters per line on each of its two lines. Each character is presented in a 5x7 pixel matrix on this LCD. Command and Data are the two registers on this LCD. The LCD command instructions are stored in the command register. The data to be displayed on the LCD is stored in the data register. The ASCII value of the character to be displayed on the LCD [6] is the data. The 4X4 keypad is used to program the microcontroller with numbers. It is made up of 16 buttons that are placed in an array with four lines and four columns. To read a digital input into the controller, one port pin is usually required. When there are a lot of digital inputs to read, allocating one pin for each of them is impractical. This is when a matrix keypad is used to reduce the number of pins.

BLOCK DIAGRAM



$$\alpha + \beta = \chi. \quad (1)$$

WORKING

To identify the user, the system prompts the user to log in using a Bluetooth-connected device. This is the initial stage in determining whether or not the user is authentic. Genuine users will be the only ones who know the password or verification code needed to connect the system to the device. After a successful login, the user is prompted to input a pin using the keypad. In the EEPROM, the pin is kept. When necessary, this pin can be reset. The user is prompted to input the Pin again if the Pin is incorrect (3 Chances given). The system will be disabled if the user fails to input the right Pin three times. If the user's Pin is accurate, an OTP is delivered via Bluetooth to the user's smart phone for two–way verification. The OTP is a 4-digit number that is chosen at random. Every time this number is generated, it is unique. The user is then instructed to use the keypad to input the OTP. If the OTP is wrong, the user's device receives a new OTP. The system is disabled if the user fails to input the correct OTP three times. If the OTP is right, the system will be opened, allowing you to do the required task.

CONCLUSION

The proposed architecture increased the ease of use while maintaining a high level of security. The enhanced lock framework's unchanging quality is based on the computerised lock framework assuming a significant role in the Internet of Things. It provides security and reduces HR in a wise manner situation with robotization at home and in buildings. The proposed framework's advanced methodology is implemented and improved. The convenience and consistent quality often ensures the security of the computerised lock system for a client who has been approved as well as a guest. The different climates have different security perspectives. It has dwindled human labour and it is given increased importance. For the wise house and building robotization there's security applications. The proposed framework increased the computerised lock framework's comfort and high unshakable quality by applying IOT. In the bright home and building computerization scenario, the computerised lock framework plays a significant role in providing security and lowering HR. The recommended technique entails implementing a computerised lock framework to ensure security for both approved and guest clients. We put the security angles to the test in a variety of climates. For shrewd house and building robotization applications, human labour has been reduced, and improved security has been provided.

REFERENCES

1) Mohammed, S.A., & Alkeelani, A.H. (2019). Locker Security System Using Keypad and RFID. 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), 1-5.
2) Shruti Jalapur, Afsha Maniya, “DOOR LOCK SYSTEM USING CRYPTOGRAPHIC ALGORITHM BASED ONIOT”, IJMTER Volume 04, Issue 2, [February– 2017] ISSN(Online):2349–9745.
3) Muhanad Hayder Mohammed, "Secure Electronic Lock using PIC 16F628A Microcontroller". International Journal of Research in Computer Science, 2 (5): pp. 43-47, September 2012.
4) Pradnya R. Nehete, J. P. Chaudhari, S. R. Pachpande, K. P. Rane, “Literature Survey on Door Lock Security Systems”, International Journal of Computer Applications (0975 – 8887), Volume 153 – No2, November 2016
5) Ilkyu Ha, “Security and Usability Improvement on a Digital Door LockSystem based on Internet of Things”, International Journal of Security and Its Applications, Vol.9, No.8 (2015)
6) 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.