IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

OTP Based Device Control System

Dr. Sreeja Mole SS[1], B Swathi[2], G Thriveni[3], B Pooja[4]
Professor, Department of Electronics & Communication Engineering[1]
UG Students, Department of Electronics & Communication Engineering[2,3,4]
Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Abstract: *OTP based wireless system is the advanced version of key based locking system the problem with the earlier key-based locking system is that every time need to carry a key to unlock the lock there is a high risk of losing a key if key is lost then, break the locking systemwhich also result in wastage of money and for old people it is difficult to open the key basedlock and there can only be one unique key for different locks having different keys. In project advanced version OTP based lock is used with high security. In project there is 3 layers security system. If someone tries to access it will generate a random OTP which was send toowner mobile & display for fraction of seconds. If the person entered a wrong OTP, it will bealert alarm buzz & generate a new OTP again. After successful enter the correct OTP will enter in 2nd layer protection which was asking us to enter password. Finally, we need to verifyour RFID tag at 3rd layer protection. So, by this way our project was very highly security system able to use at bank locker, Data rooms in companies, confidential areas etc.*

Keywords: OTP

I. INTRODUCTION

The OTP 3-layer based device control system is an advanced security mechanism designed to ensure secure and controlled remote access to devices. In today's interconnected world, where devices can be accessed and controlled remotely, ensuring the confidentiality, integrity, and authenticity of such interactions is crucial. This system employs a three-layer approach, combining user authentication, device verification, and One-Time Password (OTP) authorization to achieve a robust and reliable security framework. User Authentication Layer.This layer prevents unauthorized devices from accessing the system and ensures that only devices that have been pre-registered and authorized can communicate by combining these three layers, the OTP 3-layer based device control system significantly reduces the risk of unauthorized access, data breaches, and potential misuse of controlled devices [1].

. The main idea behind this project is to make your home and office where this project would be implemented to be more secured. But along with that, the system should be easy toaccess and also execute as fast as possible.[1] All the existing door lock systems mainly use key-based locks or outdated RFID chips. So there is a higher risk of keys being misplaced orgetting into the wrong hands. This where this project comes into the scene

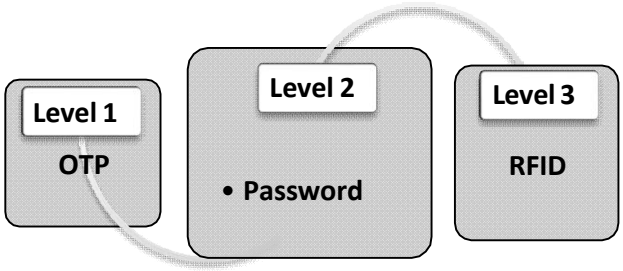


Fig 1 Proposed Three level Authentication

II. LITARATURE SURVEY

In OTP-based device control systems, including the use of OTP (One-Time Passwords), passwords, and RFID (Radio Frequency Identification) technology. Look for research papers, articles, and case studies that discuss the implementation, benefits, and challenges of such systems. Focus on understanding how OTPs work, their advantages in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

terms of security, andhow they can be integrated with passwords and RFID for enhanced access control. Explore the different authentication methods used in OTP-based systems and their effectiveness in preventing unauthorized access. Additionally, you can delve into the practical applications ofthese systems in various industries, such as home security, corporate access control, and evenonline transactions. Look for real-world examples and success stories to gain insights into thebenefits and potential limitations of OTP-based device control systems [2].

III. EMBEDDED SYSTEM

An embedded system is a special-purpose computer system designed to performone or a few dedicated functions, sometimes with real-time computing constraints. It is usually embedded as part of a complete device including hardware and mechanical parts. In contrast,a general purpose computer, such as a personal computer, can do many different tasks depending on programming. Embedded systems have become very important today as they control many of the common devices we use.

Since the embedded system is dedicated to specific tasks, design engineers can optimize it, reducing the size and cost of the product, or increasing the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale[5].

Physically embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, or the systems controlling nuclear power plants. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure.

An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is specifically designed for a particular kind of application device. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines, and toys (as well as the more obvious cellular phone and PDA) are among the myriad possible hosts of an embedded system. Embedded systems that are programmable are provided with a programming interface, and embedded systems programming is a specialized occupation. Certain operating systems or language platforms are tailored for the embedded market, such as Embedded Java and Windows XP Embedded. However, some low-end consumer products use very inexpensive microprocessors and limited storage, with the application and operating system both part ofa single program. The program is written permanently into the system's memory in this case,rather than being loaded into RAM (random access memory), as programs on a personal computer.[5]

IV. EXISTING SYSTEM

- Choose the hardware: Decide on the devices you want to control, such as lights, doors,or appliances.
- Setup the OTP generation: Implement a method to generate a One-Time Password for eachuser. This can be done using algorithms like Time-Based One-Time Password (TOTP) or Hash-Based Message Authentication Code (HMAC).
- Implement OTP verification: Develop a system to verify the OTP entered by the user. Thiscan be done by comparing the entered OTP with the one generated for that specific user.
- Connect devices and control system: Establish a connection between the control system andthe devices you want to control. This can be done using protocols like Wi-Fi, Bluetooth, or Zigbee.
- Develop a user interface: Create a user-friendly interface where users can enter their OTP, password, or use their RFID card to control the devices.
- Test and refine: Test the system thoroughly to ensure it works as expected. Make any necessary refinements based on user feedback. Remember, security is crucial, so make sure to implement encryption and secure communication protocols to protect user data[2]

V. PROPOSED METHOD

The OTP-based device control system is designed to enhance security and control access to devices by implementing a multi-factor authentication approach. The system utilizes three different methods for authentication: OTP (One-Time Password), password, and an RFID (Radio Frequency Identification) reader.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

The OTP serves as a temporary password that is generated and sent to the user's registered mobile device or email address. This password is valid for a single use and has a limited time window for verification.[3] By using OTP, the system ensures that only authorized individuals with access to the valid OTP can authenticate and gain entry to the devices.

In addition to OTP, the system also requires users to enter a password. This adds an extra layer of security by requiring individuals to provide a unique combination of characters known only to them. The password serves as a long-term authentication mechanism, ensuringthat only authorized users who possess the correct password can access the devices.

Furthermore, the system incorporates an RFID reader, which reads the unique identification information embedded in RFID tags or cards. Users are required to present theirRFID tag or card to the reader to gain access to the devices. This physical authentication method adds another level of security, as it requires individuals to possess the authorized RFID tag or card[3]

VI. WORKING PRINCIPLE

In an OTP-based device control system project, the OTP, or One-Time Password, plays a crucial role in ensuring secure access to devices. It generates a unique password for each login ortransaction, which adds an extra layer of security. The password layer involves using traditional passwords for authentication, providing an additional level of verification. Additionally, the RFIDtechnology is utilized for access control, allowing authorized users to interact with the devices [3].

By combining OTP password, and RFID technologies, we can create a comprehensive andsecure device control system User Initiation: The user initiates a request to control a device remotely. This could be done through a mobile app, a web interface, or any other means of communication[4]

- **OTP Generation:** The system generates a unique OTP for that specific control request. The OTPis usually a combination of random numbers and/or characters.
- **OTP Delivery:** The OTP is then delivered to the user through a secure channel. This can be done via SMS, email, push notification, or any other method that ensures the confidentiality of the OTP.**User Authentication:** The user receives the OTP and enters it into the device control system. The system verifies the OTP for authenticity.
- **OTP Validation:** The system validates the OTP by comparing it with the one generated for that specific control request. If the OTP matches, the user is granted access to control the device..
- **OTP Expiration**: To maintain security, the OTP has a limited lifespan. It is designed to expire after a certain period of time or after it has been used once. This ensures that even if someone interceptsthe OTP, they won't be able to use it after its expiration

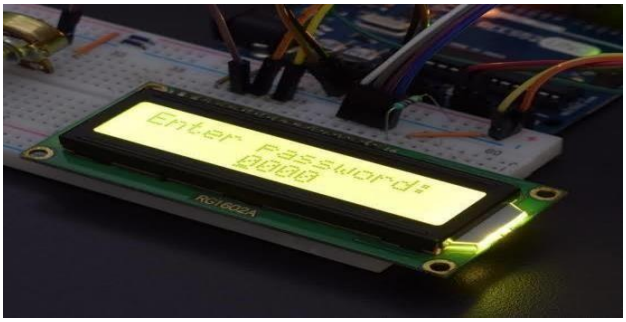


Fig 2 Display of Enter Password

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

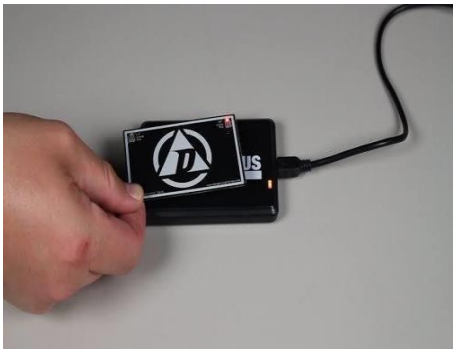


Fig 3 RFID Scanning

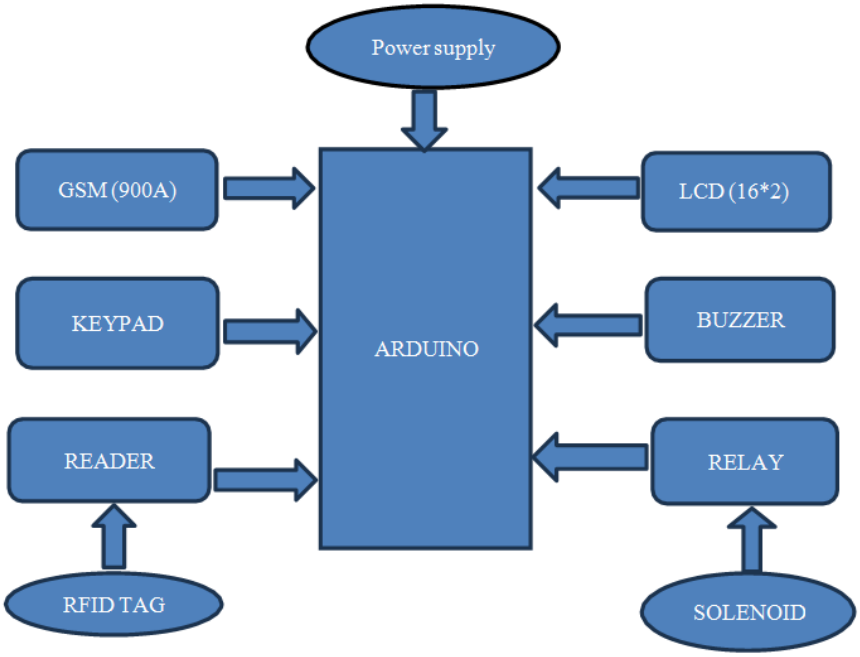


Fig 4: OTP Based Device Control System

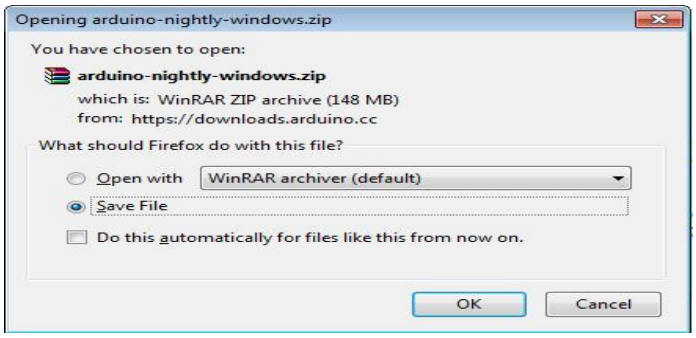
VI. SOFTWARE USED

Arduino is a prototype platform (open-source) based on an easy-to-use hardware and software. It consists of a circuit board, which can be programmed (referred to as a microcontroller) and a ready-made software called Arduino IDE (Integrated Development Environment), which isused to write and upload the computer code to the physical board.

The key features are:

- Arduino boards are able to read analog or digital input signals from different sensorsand turn it into an output such as activating a motor, turning LED on/off, connect to thecloud and many other actions.
- You can control your board functions by sending a set of instructions to the microcontroller on the board via Arduino IDE (referred to as uploading software).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024



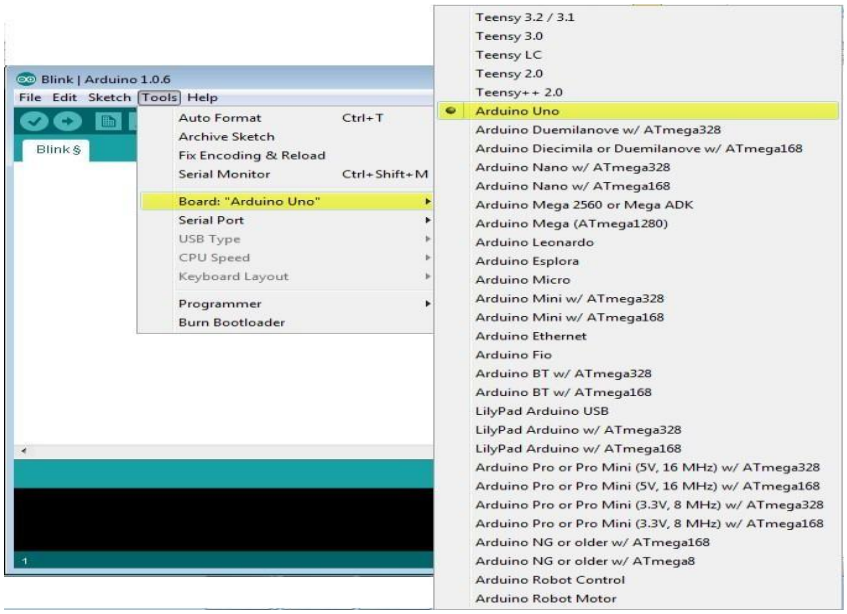


Fig 5 selection of Arduino Uno Board

VII. RESULT

This project can be used at residential places to ensure better safety and also at organizationsto ensure authorized access. Power consumption for implementation of this circuit is relatively less and it also uses commonly available components.It is a low-range circuit, so it is possible to only operate the circuit locally. If we forget the pass-word it is still possible to open the door since we have integrated extra measures. This project cannot be used by remote access. Since this project uses Solenoid Lock it requires a constant electric supply, if supply is cut it would not be possible to open the door provides security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

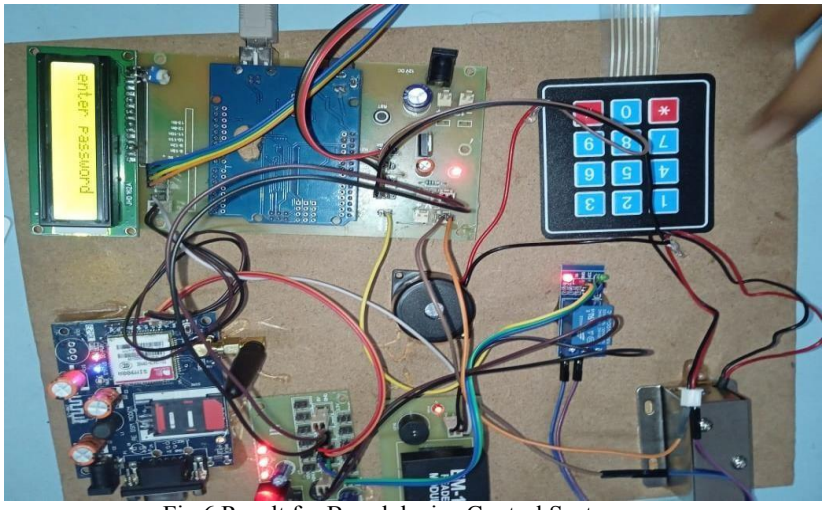


Fig 6 Result for Based device Control System

VIII. CONCLUSION

The combination of OTP, password, and RFID card authentication provides holistic anddynamic security solution that addresses various attack vectors and enhances overall protection. this approach is particularly valuable in high-security environments, critical infrastructure, financial institutions, and any scenario where safeguarding sensitive informationis paramount. Prevent unauthorized individuals from gaining access even if they manage to acquire a password or OTP. Regular system audits, updates, and employee/user education are crucial to maintaining the effectiveness of this triple-layer security approach.

REFERENCES

[1]. Kaustubh Dhondge Kaushik Ayinala Baek-Young Choi Sejun Song, "Infrared Optical Wireless Communication for Smart Door Locks Using Smart phones", 12th International Conference on Mobile Ad-Hoc and Sensor Networks, 2016.

[2]. Abdallah Kassem and Sami El Murr, "A Smart Lock System using Wi-Fi Security", 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) 2016.

[3]. 'Uno Revision 3", http://arduino.cc/en/Main/arduinoBoardUno, 2016.

[4]. M. Roland, "Software card emulation in nfc-enabled mobile phones: great advantage or security nightmare", in Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, 2012.

[5]. Edoardo Persichetti, "Secure and Anonymous Hybrid Encryption from Coding Theory", Springer-Verlag Berlin Heidelberg 2013.

[6]. "Access systems", https://www.security.honeywell.com/me/documents/Acces s Systems2011.pdf, 2011.