OMNILOCK-SMART DOOR LOCKING SYSTEMS

Dr. G Anand Kumar
Computer Science & Engineering
Dept. of Cyber Security & IoT
Malla Reddy University
Hyderabad, India
anandlife@gmail.com

Dr. M V N Srujan Manohar
Computer Science & Engineering
Dept. of Cyber Security & IoT
Malla Reddy University
Hyderabad, India
srujanmanohar.edu@gmail.com

Devansh Mishra
Computer Science & Engineering
Dept. of IoT
Malla Reddy University
Hyderabad, India
2211cs050023@mallareddyuniversity.ac.in

Kalla Thanmai Reddy
Computer Science & Engineering
Dept. of IoT
Malla Reddy University
Hyderabad, India
2211cs050040@mallareddyuniversity.ac.in

Kancharla Shivani
Computer Science & Engineering
Dept. of IoT
Malla Reddy University
Hyderabad, India
2211cs050046@mallareddyuniversity.ac.in

Abstract— **By integrating cutting-edge biometrics with the capabilities of the Internet of Things (IoT), Omnilock enhances access control. This creative solution uses an Arduino microcontroller and ESP32 combination to produce a reliable, easy-to-use smart lock application. With its integration of touchpad entry, fingerprint authentication, and remote access through the Web server. Omnilock goes beyond traditional methods to provide unmatched security and convenience. Each feature of the system may operate independently due to its modular architecture, which guarantees optimal performance and a consistent user interface. Omnilock places security first, users can choose from secure login methods like a fingerprint sensor or a simple touchpad for convenient access. Additionally, Omnilock offers remote access, allowing you to unlock the door for specified individuals even when you are not physically present. A buzzer that sounds when entry is denied serves as a barrier to unwanted attempts. In the end, Omnilock bills itself as a safe access control system that can be used in homes and other locations, giving consumers a smooth and adaptable interface.**

Keywords—Arduino, ESP32, fingerprint authentication, touchpad, remote access, buzzer

I. INTRODUCTION

These days security is a major threat faced by every individual when away from home or at home. The crime of theft at home often occurs from time to time this happens because the house is often inhabited or empty by the owner so the house becomes the main target for thieves [9]. And when it comes to security frameworks, it is one of the essential concerns in this active competitive world, where humans cannot discover ways to supply security to his/her private possessions physically. Besides, the traditional door lock uses a key that can easily be opened by an unauthorized person if he/she has the right key or a duplicate [1]. There are some more hassles that people might face when using keys or smart cards. That is when our Omnilock door lock system comes into play. Adarsh V Patil highlighted that their system works on pre-decided password concepts. It increases the security level to prevent an unauthorized unlocking done by an attacker. In case the user forgets the password, the system gives the flexibility to the user to change or reset the password [4]. Our design is implemented to provide better security as users get convenient and secure access choices, such as fingerprint scanning, and keypad entry. Furthermore, remote access features for convenience. Moreover, it doesn't need any sort of keys or cards that often get lost. Omnilock elevates your security from traditional locks to a state-of-the-art access control solution. It seamlessly integrates cutting-edge technologies with user-friendly design, offering unparalleled security and convenience. With Omnilock, your door becomes a sophisticated guardian instead of just a basic keyhole. Instead of using standard keys, which are easy to steal, misplace, or duplicate, this smart lock uses fingerprint and keypad authentication. The human detection and recognition field is very significant and has undergone rapid changes with time. An important and very reliable human identification method is fingerprint identification [5]. When access is refused, an audible buzzer sounds to discourage unwanted attempts. In contrast to RFID, which is clone-prone, Omni lock's biometric method provides more security. Additionally, the servo motor ensures flawless operation with your current door, saving you money on changes. The primary objective of the Omnilock project is to develop an advanced Smart Door Lock System that leverages cutting-edge biometric technologies and the capabilities of the ESP32 and Arduino microcontroller to provide unparalleled security and convenience. Omnilock aims to offer robust identity verification by integrating fingerprint scanning and keypad entry, significantly reducing the risk of unauthorized access. Moreover, Omnilock enables remote access for user convenience. The project seeks to address the shortcomings of traditional access control methods by delivering a comprehensive solution that is both secure and user-friendly. At its core, a high-accuracy fingerprint sensor provides quick and reliable individual identification, eliminating the need for physical keys. For those who prefer a traditional approach or situations where fingerprint scanning isn't ideal, a secure keypad interface allows access using a user-defined PIN code. Furthermore, remote access through the web server provides total control over the lock even when you're not there. The powerful ESP32 microcontroller serves as the system's brain, managing data processing, communication, and general control.

II. Literature Survey

[1] "Property Security Using a Biometric Based Door Lock System" was proposed by OnyanA and Enalume K. The paper is about the creation and implementation of a Biometric Based Door Lock System, which will automatically unlock a door when a registered fingerprint is detected. To achieve this, a fingerprint scanner R305 is used in conjunction with an ATMEGA 328 Arduino microcontroller to monitor the locking and unlocking process of a door. Access is given to the user after a recorded fingerprint is put on the sensor, the door slides open, and it closes after five seconds. The 16x2 Liquid Crystal Display (LCD) shows the individual's name along with the registered fingerprint during this process. Access is refused if an unregistered fingerprint is detected.

[2] A paper named "Secured password-based lock system" was put forward by "Arpita Mishra, Siddharth Sharma, Sachin Dubey, and S.K. Dubey". This strategy is focused on avoiding the opening of the entryway by obscure people. The arrangement of the domestic security benefit comprises the numeric keypad, the snare which is utilized for lifting, and a GSM module to set up reliable association for communication conferred with the MCU. The control board conferred with the gadget is utilized since the passcode gets to combination opens/closes the entryway.

[3] "A locks which operate by a secret knock" which was put forward by "Dr.M.Siva Sangari, Dhivakar. E, Gowthaam. K". To open and close the lock by burrowing out the thumps detected by the piezo sensor to open the entryway, a servo turns when it identifies the thumps and opens and closes the entryway.

[4] "Android Based Smart Door Locking System" which was proposed by "Adarsh V Patil, Sreevarsha Prakash, Akshay S, Mahadevaswamy, Chandan B Patgar, Sharath Kumar A J". The method executes on a pre-coded passcode idea. It moves forward the security prepares to halt an unathletically pulverizing done by a false.

[5] "SMART DOOR UNLOCK SYSTEM USING FINGERPRINT" was proposed by K. Rajesh, Asst.Prof. B.VenkataRao, P.AV.S.K.Chaitanya, and A.Ruchitha Reddy. In this paper, they have used a fingerprint sensor to read one's identity to operate the door of the car automatically. They used a microcontroller to enable the door to open or close if the matching between scanned data and the existing data is correct. Comparison is done inside the fingerprint module itself and its output is given to the microcontroller. The result is displayed on an LCD whether the user is authorized or not. LCD also helps to make troubleshooting easier. The alarming option is provided to warn about unauthorized usage. The microcontroller used is PIC16F877.

[6] "DOOR LOCKING USING KEYPAD AND ARDUINO" was put forward by Annmary Vadakkan, Athulya Babu V K, Christy Pappachan, and Prof. Ani Sunny. Password-based door lock systems allow authorized persons to access restricted areas in their security pattern. It is controlled by an Arduino. The password is entered using a keypad. The entered password is compared with the known password when setting a combination password and by using 1-6 digits. A correct password opens the door and displays the status on the LCD. If the password is wrong, the door remains closed and states "WRONG PASSWORD" on LCD. The buzzer will also activate when a password is entered incorrectly an indefinite number of times.

[7] "Smart Digital Door Lock for the Home Automation" was proposed by Yong Tae Park, Pranesh Sthapit, and Jae-Young Pyun. In this paper, they proposed a smart digital door lock system for home automation. In their proposed system, a ZigBee module is embedded in the digital door lock and the door lock acts as a central main controller of the overall home automation system. This door lock system proposed here consists of an RFID reader for user authentication, a touch LCD, a motor module for door opening and closing, sensor modules for detecting the condition inside the house, a communication module, and a control module for controlling other modules.

[8] In the paper "IoT and Fingerprint Based Door Looking System" which was proposed by Prof. Mohammad Nasirruddin, Prerna Kachhwaha, Ankita Balpande, Payal Bondre, and Mrunal Gawande. This door-locking system project suggests unlocking a door using a fingerprint. One of the most reliable biometric features having a wide range of applications is fingerprint. It provides tools to enforce reliable system transaction logs as well as protect an individual's privacy. To provide access to the facility used by multiple users, the fingerprints of the authorized users are enrolled and verified. A new user can be enrolled as well and an old user can also be removed from the system.

[9] A paper named "Door Security Design Using Fingerprint and Buzzer Alarm Based on Arduino" was put forward by Mario Junianto Manurung, Poningsih, Sundari Retno Andani, Muhammad Safii, and Irawan. In this paper they used a microcontroller Arduino as the main control center, assisted by a fingerprint sensor as a process for recording and identifying fingerprints and NodeMCU to connect to a wifi network where later on the door can also be controlled using Android via a wifi network as a remote control and an alarm buzzer which will function if when the fingerprint identification process fails, the alarm will sound as a warning sign, it will be concluded to design a safety device.

[10] "DOOR-AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE" proposed by Lia Kamelia, Alfin Noorhassan S.R, Mada Sanjaya and W.S., and Edi Mulyana. In this paper, a system called door locks automation system using Bluetooth-based Android smartphones is proposed and prototyped. First, the hardware design and software development are described, and then the design of a Bluetooth-based Smartphone application for locking/unlocking the door is presented. The hardware design for the door-lock system is the combination of an Android smartphone as the taskmaster, a Bluetooth module as the command agent, an Arduino microcontroller as the controller center/data processing center, and a solenoid as the door lock output.

III. SYSTEM ANALYSIS

A. Existing System

Traditional door locks that just require physical keys are vanishing from use. Their weaknesses are many: keys are easily lost, stolen, or even duplicated, putting your house or place of business's security at risk. A stolen key can provide an unauthorized entrance, while a lost key can leave you stranded outside. Sharing access also becomes problematic because it frequently necessitates giving out a physical key, which is dangerous and inconvenient, particularly for temporary visitors or service providers. Moreover, carrying around several keys is inconvenient since it adds extra weight to your pockets and causes you to constantly worry about losing them.

Traditional locks and keycards can be inconvenient or difficult for people with disabilities. There's no way to track who accessed the door and when with a traditional lock, making it difficult to monitor activity. Despite appearing to be a benefit, RFID technology raises additional issues. Because they rely on radio frequency transmissions, they can be copied, which could lead to unauthorized entry via intercepted communications.

Omnilock provides a multi-modal authentication system that balances ease and security, surpassing the drawbacks of conventional key-based access management. Physical keys are rendered obsolete by fingerprint scanners and secure keypads. The chance of physical keys being misplaced, stolen, or duplicated is eliminated, which dramatically lowers the risk of illegal access. Omnilock's possible interaction with the web server enables remote unlocking and access management. This improves security and peace of mind by enabling real-time entryway monitoring. When access is refused, a loud alarm also sounds to discourage unwanted attempts. More control and security are ensured by doing away with the need to issue actual keys, particularly for temporary access needs like deliveries or service visits.

B. Proposed System

Omnilock provides a multi-layered solution to access management, addressing the drawbacks of standalone biometric systems, RFID, and classic locks. Security can be compromised by physical keys, which are readily lost or stolen. By using biometrics (fingerprint technology) and secure keypads, Omnilock removes this risk and increases the difficulty of unwanted entry using lost or stolen credentials. Despite their ease, RFID technologies have a serious security vulnerability. Since they communicate by radio waves, they are vulnerable to copying and interception. With the correct tools, a malicious actor might be able to make a duplicate RFID card and obtain unauthorized access. Omnilock directly addresses this problem. Because biometrics are unique to each person, they greatly lessen the possibility of unwanted access through credential theft. The system may become inoperable due to a broken fingerprint scanner. The multi-modal approach of Omnilock provides users with additional techniques (remote access, keypad, or fingerprint) for user authentication, ensuring access even if one component malfunctions. The ESP32 may be utilized for remote access. However, its processing power and security features may be insufficient for the best results. Using an Arduino's advantages in communication and control,

Omnilock combines the ESP32 with it to create a more robust solution.

Advantages

- The primary advantage of Omnilock is its variety of authentication options. This makes it far more difficult than with single-factor systems for unauthorized people to obtain access.
- An increased degree of security is offered by biometric verification as opposed to conventional keys or RFID cards. Biometric authentication provides an additional degree of security, even if a user's PIN code is stolen.
- Depending on their comfort level and circumstances, users can select their preferred authentication method. While fingerprint gives a possibly speedier method, the keypad offers a more comfortable option. Even if a user is not available then they can use the remote access.
- Future integration with other technologies, such as smart home systems or innovative safety features, is made possible by the modular design.

IV. METHODOLOGY

A. Architecture
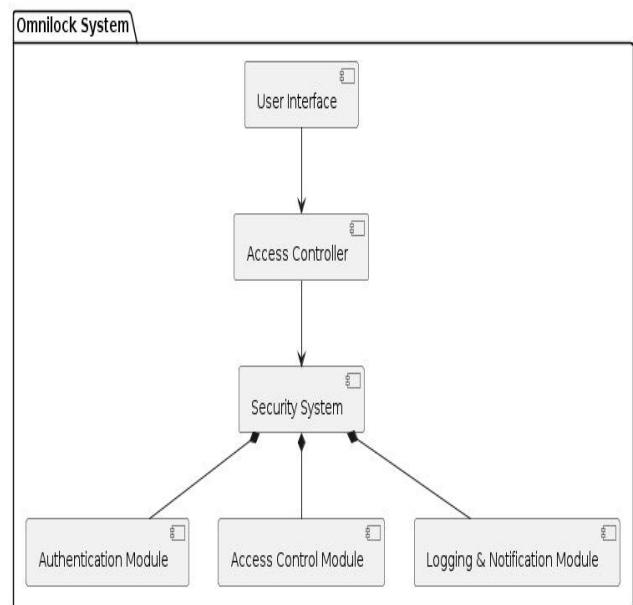
Algorithms Implemented: Fingerprint Verification and String Comparison.

Fingerprint Verification Algorithm:

The technology used in fingerprint sensors does more than just take a picture of your fingers. The actual magic of user identification is carried out by complex algorithms that are included in these sensors. These exclusive algorithms function directly on the sensor, guaranteeing a safe and effective procedure. Since the sensor vendor closely guards the specifics of these algorithms, they are frequently private. Because it becomes harder for potential hackers to exploit the underlying workings of the algorithms, this strategy maintains security. These sensor-specific algorithms also take advantage of the hardware's capabilities to optimize processing times and power consumption. The sensor's

fingerprint verification algorithms serve as the gatekeepers, carefully examining each characteristic of your fingerprint to provide safe and practical user identification.

String Comparison Algorithm:

PIN code protection is just one more way that Omnilock puts the security of its users first. An important vulnerability would be a straightforward string comparison between the entered PIN and a stored PIN code. A hacker might simply open the door if they managed to get the stored PIN codes. Omnilock uses hashing functions to solve this issue. These cryptographic functions create a unique, fixed-length string of characters termed a hash using the user's PIN code as input. The original PIN is securely represented by this hash. It's crucial to remember that the hashing function is one-way; the original PIN code cannot be recovered by mathematically reversing the hash.

B. Process

1) Module 1: User Interface Module
- Responsible for giving an interface for clients to associate with the system.
- Includes functionalities such as user authentication, access request submission, and viewing system status.
- Designed with a user-friendly interface for ease of use and accessibility.

2) Module 2: Access Controller Module
- Manages access requests from users and coordinates the authentication process.
- Acts as an intermediary between the user interface and the security system.
- Responsible for initiating the authentication process and handling access control decisions based on authentication results.

3) Module 3: Security System Module
- The central component is responsible for authentication and access control.
- Consists of sub-modules for various authentication methods such as fingerprint recognition, remote access, and PIN authentication.
- Implements access control policies based on authentication results and grants or denies access accordingly.

4) Module 4: Authentication Module
- Handles the authentication process for verifying the identity of users.
- Includes sub-modules for different authentication methods, such as biometric authentication (fingerprint technology), traditional methods (PIN authentication), and remote access via web server.

5) Module 5: Access Control Module
- Implements access control policies based on authentication results.

- Determines whether users are granted or denied access to secured areas based on authentication outcomes.
- Interfaces with the security system to enforce access control decisions and manage access permissions.
- The buzzer can be activated for a predetermined duration by a function that the Access Control Module may trigger in response to a "denied access" signal.

#### 6) Module 6: Logging & Notification Module

- Responsible for logging system events and generating notifications/alerts.
- Records access control activities, authentication attempts, and system errors for audit and monitoring purposes.
- Notifies administrators or users about security-related events, such as unauthorized access attempts or system malfunctions.
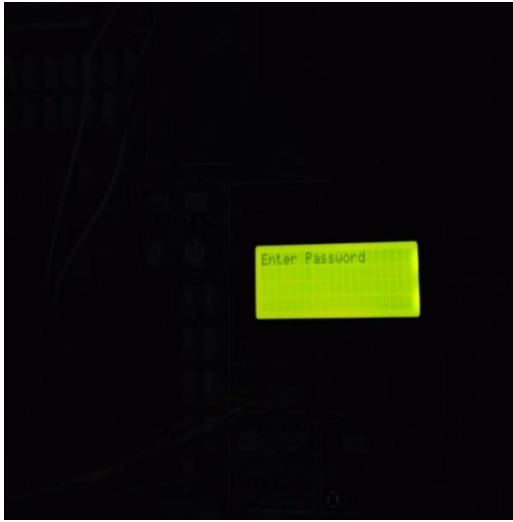
V. RESULTS

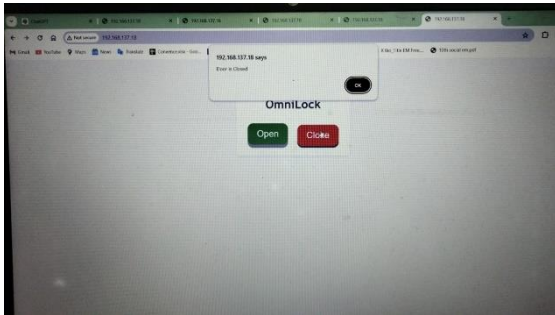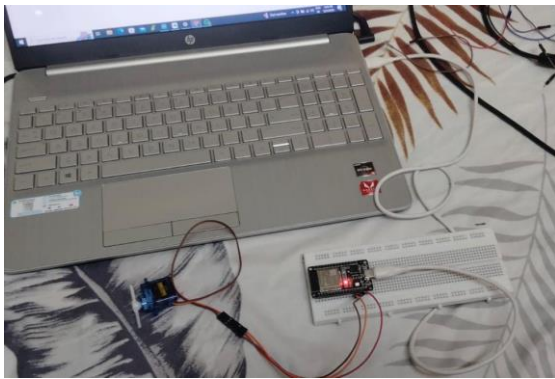### A. Figure 1: Integration with Fingerprint sensor

B. Figure 2: Integration of Keypad
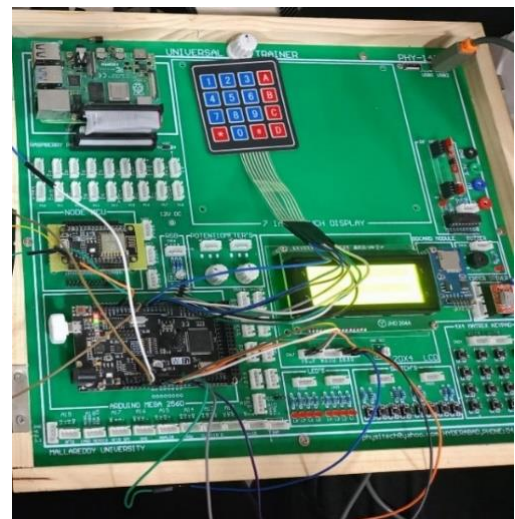
C. Figure 3: Remote Access

D. Figure 4: Integration of Fingerprint, Keypad, and Remote Access

VI. CONCULSION

By overcoming the drawbacks of conventional keys and single-factor authentication, Omnilock transforms access control. With its multi-modal approach, customers can select their favorite technique, be it a fingerprint scanner or secure keypad. Compared to readily misplaced, stolen, or duplicated keys or RFID cards that are susceptible to interception, this greatly improves security. Another level of comfort comes with the possibility of remote access control provided through the web server. Omnilock markets itself as a user-friendly, flexible, and safe access control system. With the use of potent microcontrollers, state-of-the-art biometrics, and the possibility of smart home integration, Omnilock users are in a new era of smart and practical door locks for homes and other locations.

VII. FUTURE WORK

Encouraging possibilities exist for enhanced security and user-friendliness in the future. Visualize a scenario where high-security regions require access to both a PIN code and a fingerprint scan as part of multi-factor authentication. When you get closer, geofencing might open the door for you, and time-based access might only allow certain users in during particular times. Voice authentication may even be made available as a convenient hands-free option.

VIII. REFERENCES

[1] OnyanA and Enalume K, "Property Security Using a Biometric Based Door Lock System" – 2018.

[2] Arpita Mishra, et al., "PASSWORD BASED SECURITY LOCK SYSTEM" International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Issue No. 05, May 2014 ISSN (online): 2348 – 7550.

[3] Dr. M. SivaSangari, et al., "Secret Knock Detecting Door Lock" Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 406-410 Received 15 April 2021; Accepted 05 May 2021.

[4] Adarsh V Patil, et al., "Android Based Smart Door Locking System" International Journal of Engineering Research & Technology (IJERT)

[5] K. Rajesh, et al., "SMART DOOR UNLOCK SYSTEM USING FINGERPRINT" Pramana Research Journal Volume 9, Issue 3, 2019 ISSN NO: 2249-2976.

[6] A.Vadakkan, et al., "DOOR LOCKING USING KEYPAD AND ARDUINO," International Research Journal of Modernization in Engineering Technology and Science, vol. 3, no. 11, p. 783, 2021.

[7] Park, et al., "Smart digital door lock for the home automation." In TENCON 2009-2009 IEEE Region 10 Conference, pp. 1-6. IEEE, 2009.

[8] NasarruddinM, et al., "IOT and fingerprint based door locking system" – 2018.

[9] Manurung, M. J., et al., (2021). "Door Security Design Using Fingerprint and Buzzer Alarm Based on Arduino". *Journal of Computer Networks, Architecture and High Performance Computing*, *3*(1), 42-51.

[10] LiaKamelia, et al., "DOOR-AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE" VOL. 9, NO. 10, OCTOBER 2014 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences.