Advanced Authentication System with Biometric and OTP Integration

Jeevan Kumar Vajja[1]; Polaki Pavan[2]; Dunga Sasi Kumar[3]; Kaniti Navya[4]; Srinu Kurimina[5]; Yogeshwar Rao Divvalasa[6]

[1;2;3;4;5;6]Department of Electronics and Communication Engineering,
Sri Sivani College of Engineering, Srikakulam,532402

Publication Date: 2025/04/11

Abstract: In the modern digital era, traditional key-based locks are highly vulnerable to duplication and unauthorized access, necessitating advanced authentication mechanisms. This research proposes a dual-layer authentication system using a Raspberry Pi Pico, integrating facial recognition and a secure OTP mechanism to enhance security. The system first captures and verifies facial features against an authorized database. An OTP is generated using secure algorithms and transmitted via encrypted channels if authentication fails. The user enters this OTP on a keypad for secondary verification. Additional security measures include OTP expiration, limited authentication attempts, and encrypted data transmission, ensuring robust protection against unauthorized access. Furthermore, the system incorporates a GSM module for real-time OTP delivery, ensuring accessibility even in network-restricted environments. The relay module and electronic solenoid lock coordinate to provide seamless and automated door control. This system is designed for smart homes, offices, and high-security zones, offering a scalable and reliable solution for modern access control systems.

Keywords: *Smart Authentication, Dual-Layer Security, Facial Recognition, OTP Verification, Raspberry Pi Pico, GSM Module, NFC, Biometric Authentication.*

How to Cite: Jeevan Kumar Vajja; Polaki Pavan; Dunga Sasi Kumar; Kaniti Navya; Srinu Kurimina; Yogeshwar Rao Divvalasa (2025). Advanced Authentication System with Biometric and OTP Integration. *International Journal of Innovative Science and Research Technology*, 10(4), 86-90. https://doi.org/10.38124/ijisrt/25apr160

I. INTRODUCTION

In an era where security breaches and unauthorized access are growing concerns, traditional key-based locking systems cannot provide robust protection. Conventional locks are vulnerable to duplication, theft, and unauthorized entry, posing significant security risks to homes, offices, and high-security areas. Modern authentication systems utilize biometric verification, OTP-based security, and encrypted communication protocols to tackle these challenges and strengthen access control mechanisms.

This research focuses on developing an Advanced Authentication System with Biometric and OTP Integration, incorporating a dual-layer security mechanism to prevent unauthorized access. The system utilizes facial recognition as the primary authentication method, leveraging computer vision algorithms to verify users. If facial authentication fails, a secondary OTP verification step is triggered, where a dynamically generated one-time password (OTP) is sent via a GSM module through an encrypted channel.

The user must enter this OTP on a keypad for final verification before granting access. Additional features such as OTP expiration, limited authentication attempts, encrypted data transmission, and relay-controlled door-locking mechanisms have been implemented to strengthen security. This system ensures high reliability, scalability, and adaptability for various applications, including smart homes, office security, and **highly restricted** areas. This research presents a cost-effective and efficient solution for modern access control systems by integrating biometrics and embedded system technologies.

II. LITERATURE REVIEW

In a study by Prof. N. A. Thorat, Sohan Sutar, Siddesh Bhandare, Shailaja Sathe, Pranav Ghate, and Saurabh Bhosale, " A Survey on 'Smart Authentication Door Locking-System, '" Published in International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume-3, Issue-4, May-2023. This study presents an advanced, bright door lock system designed to enhance security in homes and Offices.

The system integrates various authentication techniques, including biometric scanning, OTP verification via GSM modules, and keypad entry. It employs an Arduino Uno as the primary controller, IP cameras, relays, solenoid locks, and cloud-based monitoring. The paper highlights the advantages of replacing conventional locks with modern, flexible security mechanisms and discusses challenges such as power consumption, network reliability, and hacking vulnerabilities.[1]

“Access System Using Facial Recognition and NFC” by José Ignacio Vega Luna et al. Source: International Journal of Embedded Systems and Smart Innovations, 2022. Introduces a laboratory access control system integrating facial recognition with NFC technology for secure entry. The system employs an AI-based vision module and an NFC reader controlled by an Arduino UNO. Upon detecting a valid face, the system cross-verifies the NFC card ID before activating the electric lock. The research demonstrates a recognition time of 155.875ms with 87.5% accuracy, highlighting the potential of dual-authentication mechanisms in enhancing security.[2]

The Android-Based Smart Door Locking System by Adarsh V Patil et al.. presents an innovative door-locking system operated via an Android application. The system supports regular and multi-mode access, making it suitable for high-security areas like banks and corporate offices. The application ensures convenient access and system control for authorized users while providing robust security through password-based protection. The research demonstrates how mobile applications can enhance accessibility without compromising safety.[3]

III. PROPOSED SYSTEM

The proposed system is an Advanced Authentication System with Biometric and OTP Integration, designed to provide a highly secure and efficient access control mechanism. Traditional key-based locks are prone to duplication and unauthorized access, making them less reliable for high-security applications. To address these concerns, this system integrates facial recognition and OTP-based authentication, ensuring only authorized individuals can gain access.

When a user approaches the door, the PIR sensor detects motion and activates the ESP32-CAM module to capture the user's facial image. The captured image is compared with a pre-stored database of authorized users. If the system identifies a match, access is granted by unlocking the solenoid lock. If facial recognition fails, the system triggers a secondary authentication mechanism by generating a One-Time Password (OTP). This OTP is sent to the registered mobile number using the GSM module. The user then enters the OTP on the 4x4 Keypad, and if it matches the generated code, the relay module activates, unlocking the door.[4][5]

The system incorporates several advanced security features to enhance reliability. The LCD 16x2 display provides real-time feedback on authentication status, ensuring clarity for the user. OTPs are transmitted through encrypted channels to prevent unauthorized interception, further strengthening security. Additionally, the system enforces limited access attempts, reducing the risk of brute-force attacks. Integrating a GSM module ensures that the OTP- based authentication can function even in offline environments, making the system suitable for areas with limited internet connectivity.

The proposed system offers a scalable, efficient, and robust security solution combining biometric authentication and OTP verification. Its design makes it ideal for smart homes, offices, and high-security zones, providing a reliable, user-friendly, and technologically advanced access control method.

A. Components to be used:

- *Raspberry Pi Pico:*

The Raspberry Pi Pico is a microcontroller board based on the RP2040 chip, featuring dual-core ARM Cortex-M0+ processors. It is designed for embedded applications with flexible I/O options and supports programming in Micro Python and C/C++. In this project, it plays a crucial role in processing authentication logic and managing hardware components such as the relay, keypad, and sensors. Its low power consumption makes it suitable for continuous operation in security systems.

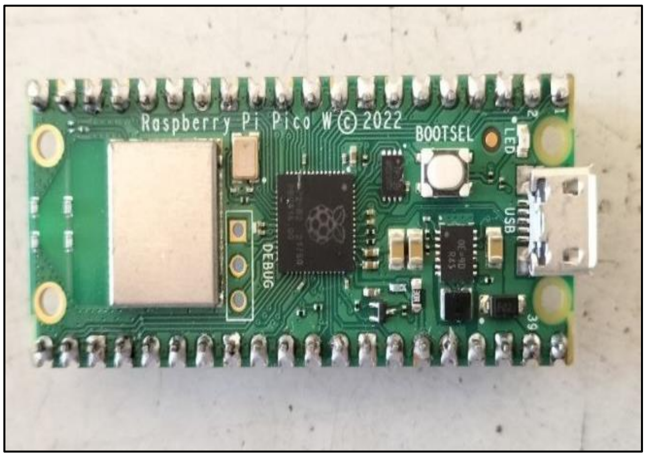

Fig 1 Raspberry Pi

- *ESP32-CAM Module:*

The ESP32-CAM Module is a compact camera module integrated with an ESP32 chip, enabling wireless image processing and transmission. It captures facial images and transmits them to the authentication system for verification. With built-in WiFi and Bluetooth capabilities, the ESP32-CAM allows remote monitoring and secure data communication. Supporting various image resolutions, it enhances the accuracy of face recognition, making it a key component in smart security applications.

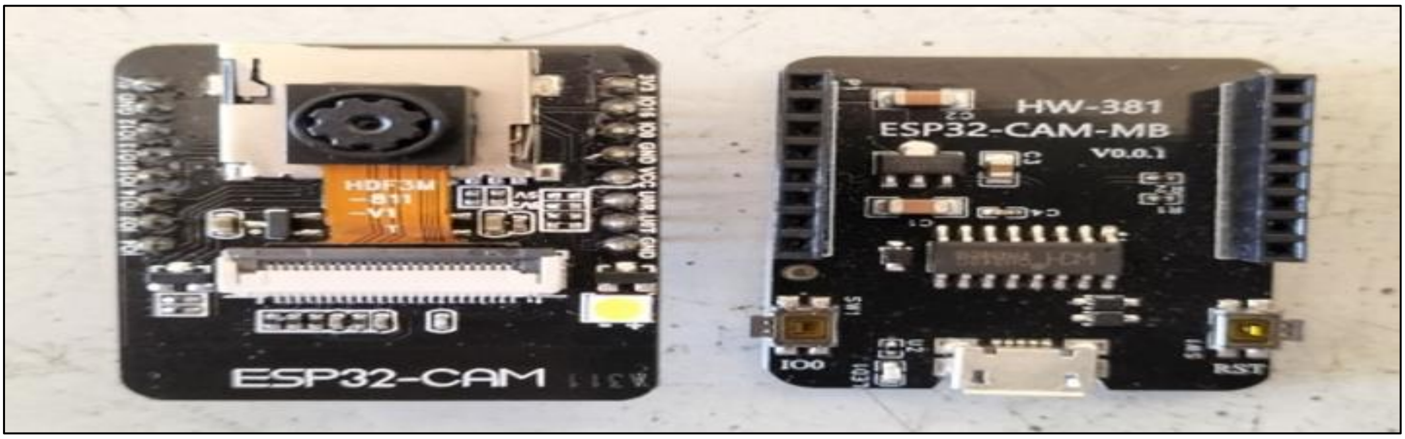

Fig 2 ESP32 CAM Module

- *GSM Module (SIM900A)*

The GSM Module (SIM900A) is used to send OTPs via SMS, enabling an additional layer of security. It operates on mobile networks, allowing authentication even in the absence of WiFi. This module supports both voice and data communication and is widely used in IoT applications. When integrated with the Raspberry Pi Pico, it facilitates seamless OTP-based verification, ensuring secure access control.

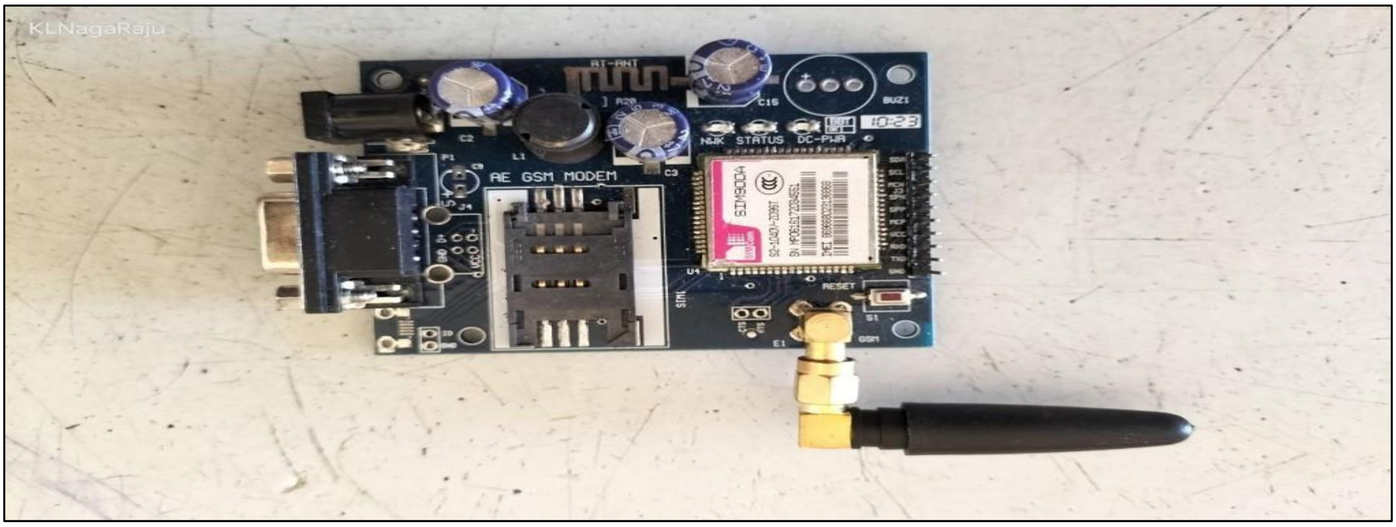

Fig 3 GSM SIM 900A

- *PIR Motor Sensor*

A PIR Motion Sensor is employed to detect human movement using infrared radiation. It triggers the authentication process when someone approaches the door, helping to optimize power consumption by keeping the system in standby mode when not in use. This sensor enhances security by preventing unauthorized access and can be effectively used in both indoor and outdoor environments.

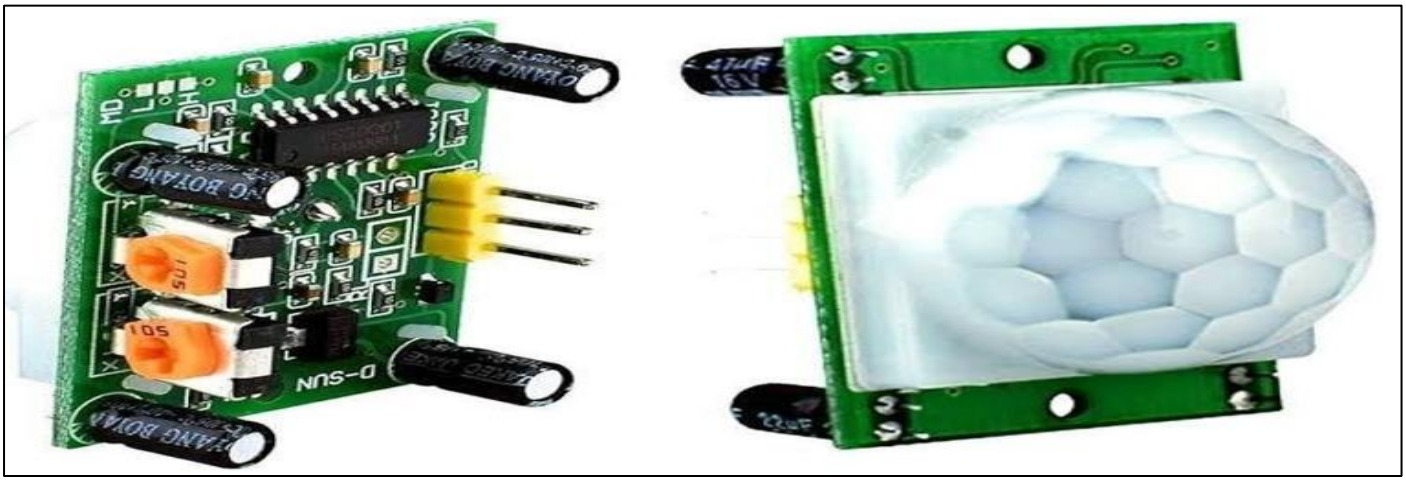

Fig 4 PIR Motion Sensor

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr160

➢ *LCD 16x2 Display*

The LCD 16x2 Display provides real-time feedback to users by displaying authentication status, OTP messages, and system alerts. It consists of 16 columns and 2 rows, allowing text-based interaction with the user. The display is connected to the Raspberry Pi Pico, ensuring easy communication and seamless integration into the security system. Its minimal power consumption makes it a reliable component for embedded applications.[4]

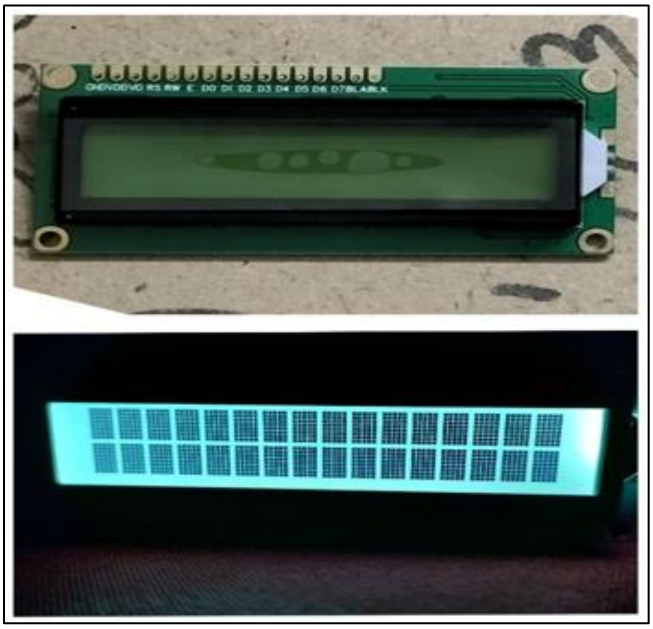

Fig 5 16x2 Liquid Crystal Display

➢ *4x4 Keypad*

A 4x4 Keypad serves as an input device for users to enter OTPs. This matrix keypad consists of 16 buttons arranged in 4 rows and 4 columns. It provides a simple and efficient method for user authentication, working in coordination with the microcontroller to verify OTP entries. Due to their reliability and ease of use, keypads are commonly implemented in access control systems.

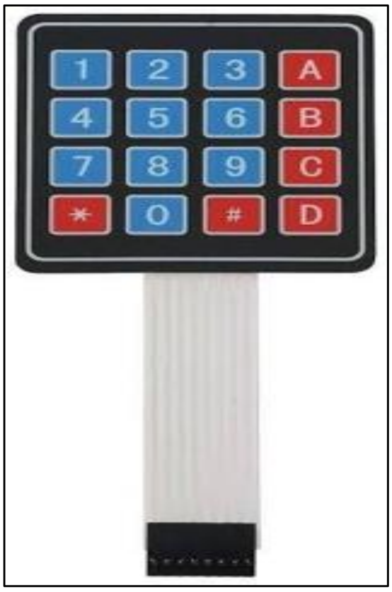

Fig 6 4x4 Keypad

➢ *Relay Module*

The Relay Module acts as an electronic switch, controlling the solenoid lock based on authentication results. It serves as an interface between the low-power microcontroller and the high-power locking mechanism. By using relays, the system ensures the safe switching of electrical components without direct physical contact, automating the locking mechanism upon successful verification.

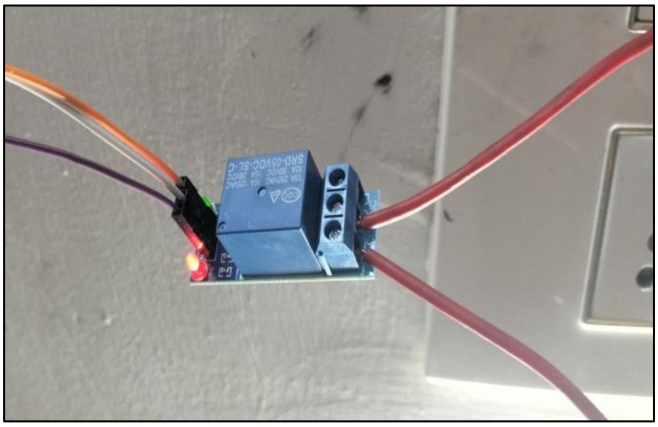

Fig 7 Relay Module

➢ *Solenoid Lock*

The Solenoid Lock is an electronically controlled locking mechanism that ensures secure access control. It engages or disengages based on authentication approval, preventing unauthorized entry. The solenoid lock is controlled using a relay module and powered by an external power supply. It is widely used in smart door locks, safes, and security cabinets due to its robust locking mechanism and reliability in high-security applications.

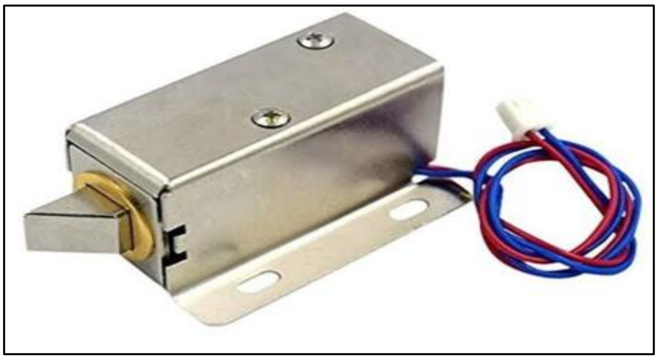

Fig 8 Solenoid Lock

IV. METHODOLOGY

The methodology of this project follows a structured approach to ensure the development of a secure and efficient authentication system. The system integrates biometric authentication and OTP verification to provide a dual-layer security mechanism. The process begins with the PIR sensor detecting motion near the access point, which then activates the ESP32-CAM module to capture the facial image of the user. This image is processed and compared against a pre-stored database of authorised users. If a match is found, the solenoid lock is triggered to grant access.

In cases where facial recognition fails, the system initiates a secondary authentication process by generating a One-Time Password (OTP). The OTP is sent to the registered mobile number through the GSM module via an encrypted communication channel. The user must enter the received OTP using the 4x4 keypad, which is then verified against the generated code. If the OTP matches, the relay module activates, unlocking the door. If incorrect attempts exceed the predefined limit, the system enters a lock-down mode, preventing further access attempts for a specific period.[6] [7]

To enhance user interaction and accessibility, the LCD 16x2 display provides real-time feedback on authentication status, indicating whether access is granted or denied. The system is powered using a Li- ion battery (3S BMS) with a 5V power adapter, ensuring stable operation. The entire authentication process is managed using the Raspberry Pi Pico, which handles input processing, OTP generation, and communication between components using Embedded C and C++ programming.

The system architecture is designed to be scalable, efficient, and secure, ensuring that unauthorized access is prevented while allowing seamless and reliable authentication for legitimate users. This methodology ensures that the proposed system is suitable for smart homes, offices, and high-security areas, offering a robust and technologically advanced access control mechanism.[8]

V. CONCLUSION

This project integrates biometric authentication with OTP based verification to enhance security for smart homes, offices, and high-security areas. The dual-layer approach significantly reduces the risk of unauthorized access while ensuring user convenience. The system's scalability and adaptability make it a viable solution for various security applications.

FUTURE SCOPE

Future advancements in this system will focus on enhanced biometric authentication, 5G-enabled GSM, and LoRa modules for faster and more secure data transmission. Power efficiency can be improved with solar-powered backups and intelligent battery management for uninterrupted operation. Further studies and research should be encouraged for the practical application of automation technology in authentication.

- *Conflict of Interest*

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript, and there is no financial interest to report. We certify that the submission is original work and is not under review at any other publication.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to **Mr. JEEVAN KUMAR VAJJA** for their invaluable guidance and support throughout this research.

REFERENCES

[1]. Thorat, Sohan, et al. “A Survey on Smart Authentication Door Locking System.” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 3, no. 4, 2023, pp. 2581–9429..Available: ijarsct.co.in, DOI: 10.48175/IJARSCT-9873.

[2]. Ignacio, José, et al. “Access System Using Facial Recognition and NFC.” International Research Journal of Advanced Engineering and Science, vol. 8, no. 1, 2023, pp. 193–198. Available: irjaes.com

[3]. Patil, Adarsh V, et al. “Android Based Smart Door Locking System.” International Journal of Engineering Research & Technology (IJERT), vol. 6, no. 13, 24 Apr. 2018. Available: ijert.org, DOI: 10.17577/IJERTCONV6IS13199.

[4]. Arpita Mishra, Siddharth Sharma, SachinDubey, S.K.Dubey, “Password Based Security Lock System”, International Journal of Advanced Technology in Engineering and Science, 2011.

[5]. BhalekarPandurang, JamgaonkarDhanesh, Prof. Mrs. ShailajaPede, GhangaleAkshay, Garge Rahul, “Smart Lock: A Locking System Using Bluetooth Technology & Camera Verification”, International Journal of Technical Research, 2013.

[6]. LiaKamelia, AlfinNoorhassan S.R, MadaSanjaya and W.S., Edi Mulyana , “Door-Automation System Using Bluetooth-Based Android For Mobile Phone”, ARPN Journal of Engineering and Applied Sciences(ISSN 1819-6608), Vol. 9, No. 10, October 2014.

[7]. NeelamMajgaonkar, RuhinaHodekar, PriyankaBandagale, “Automatic Door Locking System”, International Journal of Engineering Development and Research, Volume 4, Issue 1,2013 ISSN: 2321-9939.

[8]. R.A. Ramlee, D. H. Z. Tang, M.M.Ismail, “Smart Home System for Disabled People Via Wireless Bluetooth”, in Proc. of IEEE International Conference on System Engineering and Technology, pp. 1-4, 2012.

[9]. Harnani Hassan, Raudah Abu Bakar, Ahmad Thaqib and FawwazMokhtar, “Face Recognition Based on AutoSwitching Magnetic Door Lock System using Microcontroller” in International Conference on System Engineering and Technology, Indonesia, 2012.

[10]. JunainaMohd Shah, “Door Locking System using RFID Technology,” Faculty of Electrical and Electronic Engineering, UniversitiTun Hussein Onn Malaysia: Final Year Project Report, 2009.