https://doi.org/10.65091/icicset.v2i1.12

Design and Implementation of a Customized Door Lock System for Local Needs

Sarbagya Buddhacharya
Khwopa Engineering College
Purbanchal University
Bhaktapur, Nepal
sarbagya.buddhacharya@gmail.com

Shristi Tuladhar
Khwopa Engineering College
Purbanchal University
Bhaktapur, Nepal
shristituladhar16@gmail.com

Apekshya Chaudhary
Khwopa Engineering College
Purbanchal University
Bhaktapur, Nepal
chaudharyapekshya070@gmail.com

Ojesh Manandhar
Khwopa Engineering College
Purbanchal University
Bhaktapur, Nepal
ojeshmdr664@gmail.com

Ojashpi Khadka
Khwopa Engineering College
Purbanchal University
Bhaktapur, Nepal
ojashpi.khadka@gmail.com

Ramesh Marikhu
Almonds A.I. Company Pvt. Ltd.
Bhaktapur, Nepal
marikhu@gmail.com

***Abstract*— This paper presents a design and implementation of a customized door lock system utilizing Internet of Things (IoT) technology. The proposed system focuses on accessing the door at the ground floor from the top floor of a three- to five-story building, which is not supported by most of the prevailing door lock systems. The idea emerged from a local survey conducted among the 72 houses in the vicinity of Bhaktapur, Nepal, which highlighted the local problem among the elderly population facing difficulty in opening the door at the ground floor while they are residing at the top floor. This research aims to provide a low-cost, affordable door lock system to solve the local issue of remotely accessing the door. The paper employs an ESP32-CAM microcontroller including a camera module and a Wi-Fi module, integrated with an RFID reader, keypad, and a relay-controlled solenoid lock providing the mechanical actuation for door locking and unlocking operations.**

Index Terms*— Internet of Things (IoT), Digital Door Lock System, ESP32

I. Introduction

The concept of the smart home system has gained major attention with the advancement of the Internet of Things (IoT). The major studies and developments in the smart home system in recent years can be broadly classified into three groups: smart home control systems, home security systems, and remote door access. The smart home control system mainly focuses in providing a centralized system for controlling various appliances such as Television (TV), fan, air conditioning (AC), automatic curtain control, and lighting control using different sensors including environmental sensor for purposes such as rain detection and gas sensors for alarming the gas leakage [3],[9],[14]. The main focus of this system is to provide a sophisticated home automation system to provide convenient access and control over the various electrical appliances in a home. The home automation system proposed in [3],[9],[14] uses microcontrollers of different series from the STM32 family, which are connected to different home appliances, and the user interface is provided through infrared (IR), wireless fidelity (Wi-Fi), and Modbus modes of communication.

Several studies have proposed various home security system approaches to achieve security in accessing the home, detecting unauthorized access, and alarming the user about unauthorized access [1], [2], [6]-[8], [11], [12]. In [1], a MATLAB-based software is developed for coding the user's voice to create a database, and the system allows access only to the verified voice of the authorized user which matches with the database, while rejecting the imposter's voices. A novel approach of warning the user about unauthorized access by sending a message to users through GSM communication is proposed in [2]. Likewise, [6] has proposed a secret knocking pattern which is only known to the user, and unauthorized access is detected if the input knocking pattern does not match, and an alert message is sent to the owner via GSM communication. A location-based smart door system is proposed in [7], in which the user's GPS location needs to be within an acceptable proximity from the GPS location of the door while sending a command to the central host through Bluetooth communication. However, if the user's GPS location is not within the acceptable range, access to the door will be considered unauthorized, and a warning message will be sent to the user's application. Similarly, in [12], one-time password (OTP) based authorization for door access is proposed, allowing the user to send the access request via a designated key in the keypad. Following this, the Arduino UNO commands the GSM SIM800L module to generate OTP, which is then sent to a mobile which is already registered. After receiving the OTP, the user can input the OTP using the keypad, which is verified by the Arduino and trigger the solenoid lock to open the door only when the OTP is correct; if not, a buzzer is activated, alarming the attempt of unauthorized access. Moreover, research based on the face recognition system to access the doors under three different lighting conditions, i.e., dim, moderate, and bright light, is performed in [11]. The research contributed an enhanced face recognition system under varying light conditions, specifically in the range of 300 to 800 lumens, which is then connected to the main server via Wi-Fi communication and after verification, an authorized door access is granted. A multi-authentication-based door lock system, incorporating face recognition, fingerprint verification, RFID card access, password entry, and IoT monitoring, is mentioned in [8]. Each attempt to access the door is sent to the cloud-based system, which will then send updated information in the mobile application indicating whether the attempt was successful, or failed match, or unauthorized attempt.

Apart from the study about the door access security and alarming the unauthorized access, some innovative ideas

about remote door access are studied in [4], [5], in which a mobile app is developed to actually control the door locking system. In [4], a Bluetooth-based access door look system is proposed, but it is limited to only short distances, while a Wi-Fi-based smart access to door locking system is proposed in [5], which eliminates the user from the worry of carrying keys and whether the door is locked or not.

All the proposed door lock system focuses on accessing the door from outside of the house, enhancing authorized access and alarming unauthorized access. Most of the research has focused on accessing the door from a limited distance and has not incorporated the issue of accessing the door from a wider range, which could solve the locally inherent problem of accessing the door at the ground floor from the top floor of a multi-story building. This issue has been pointed out in this paper through a local survey performed among the 72 houses in the vicinity of Bhaktapur, Nepal. Most of the available door lock systems are either a part of a smart system, a home security system or a sophisticated door locking system, which makes the equipment costly for the general people and makes them reluctant to use it. This study has attested to this problem and provided a customized low-cost door lock system allowing the user to access the door at the ground floor from the top floor, which is the main contribution of this paper.

II. Survey

This study conducted a local survey in the vicinity of Bhaktapur, Nepal, to know the technical requirements of the user. The information obtained from the survey was used to customize the proposed door lock system as per the user's requirements and needs. A Google form was created with four major questions: (i) to know if participants have prior experience with door lock systems, (ii) if they have prior experience, then the types of door lock systems they have used, (iii) if they require a door lock system, and (iv) the number of stories in their building. The survey was performed in 72 houses, and the participants were from the age group of 20-55 years. The survey results are shown in Fig. 1-4.

The survey result showed that 81.9 % of the users have not used the door lock system as shown in Fig. 1. Similarly, different types of door lock system used by the users are: magnetic, keypad, RFID, fingerprint, face detection, manual switch-based system while other systems include system with key, with voice control, and mechanical control as shown in Fig. 2. Likewise, 74 % of participants showed the desire to use the door lock system while only 1.4 % of user are not willing to use the system as shown in Fig. 3. This shows the inherent need to door lock system in the locality. Lastly, among the participants, 47.9% live in three-story buildings, 26 % live in four-story buildings, and 6.8% live in five-story buildings, as shown in Fig. 4. Altogether, 80.8% of the participants reside in the three- to five-story buildings, which is the major target group of this study.

The majority of the participants have shown a strong desire to use the door lock system. However, they are reluctant to use it mainly because of the high price, unnecessary features that they do not actually need, not compatible with their multi-story buildings, and not satisfying their actual need to open the door at the ground floor from the top floor. This research has tried to specifically address these problems by proposing a door lock system which is compatible with their actual requirement. This work therefore proposes a basic model with only a few basic features, with a manual switch to open the

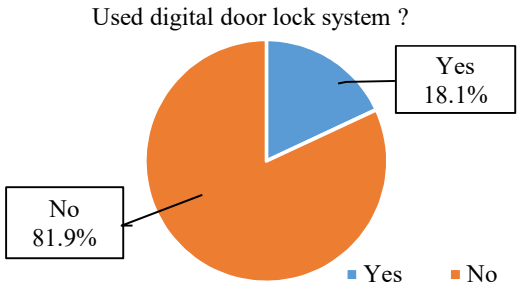


Fig.1: Participants used/unused the door lock system

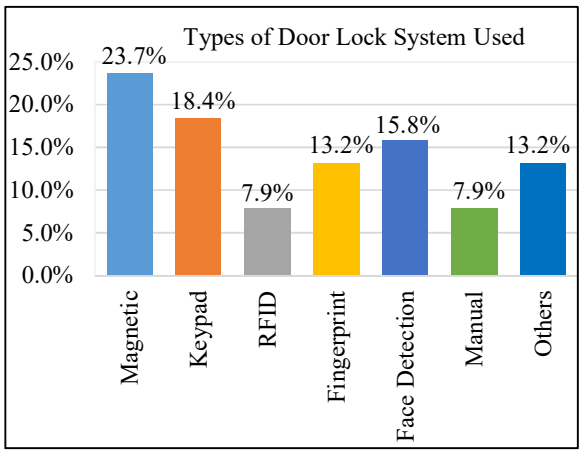


Fig. 2: Types of door lock system used

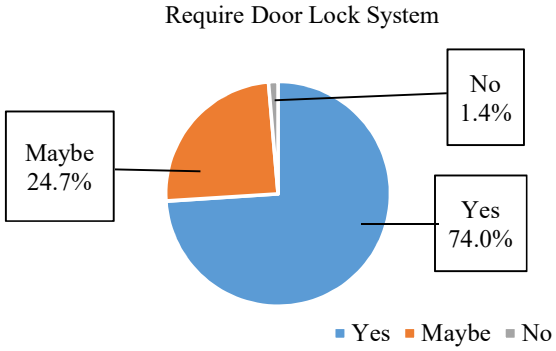


Fig. 3: Requirement of door lock system

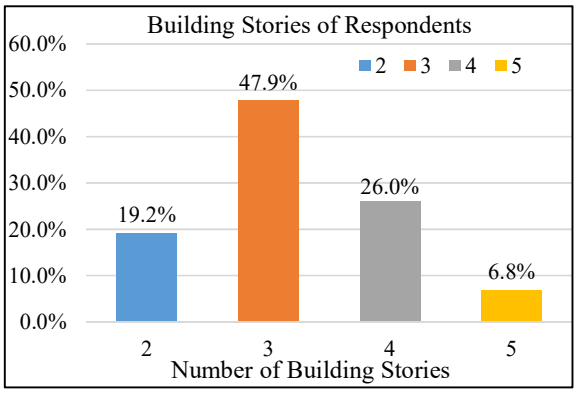


Fig. 4: Number of stories of participants' building

door, which can be installed at different levels of a multi-story building and a remote access to the door via Wi-Fi, particularly focusing on opening the door at the ground floor from the top floor. The study also provides additional features such as RFID access, and Face recognition, but these features will be added only upon the users' demand, thereby limiting the cost of the basic model to be very low within the range of users' expectations.

III. System Model

The study proposes two models, a basic model and an advanced model. These models intend to customize the door lock system as per the users' inherent requirements at an affordable cost.

A. Basic Model

The basic model comprises an ESP32 microcontroller, a one-channel relay, and a solenoid lock as its major components. It offers both switch-based and application-based control to lock and unlock the door. ESP32 controls the lock via a relay, and a transistor is also added for efficient switching. Normally, a solenoid lock is applied 12V power supply through an adaptor, and an additional LiPo battery is also connected to provide a backup power supply in case of power failures. For the switch-based mode, a manual switch is incorporated, which provides direct lock and unlock functionality to the users. The manual switch can be installed on multiple floors as per the users' requirements. On the other hand, for the application-based control, the built-in Wi-Fi module of ESP-32 is configured to create a local server with a unique SSID and password. The IP address to access can be obtained from the serial monitor once the code is uploaded to the microcontroller. The attained IP address can be input in the web browser on a mobile device to access the interface to lock and unlock the door. Both modes can be used simultaneously, and the user can select any of these options to lock and unlock the door. The Blynk app can also be used for application-based control. However, it is not preferred in this study as it was difficult to customize. The detailed block diagram and flowchart are shown in Fig. 5 and 6 respec.

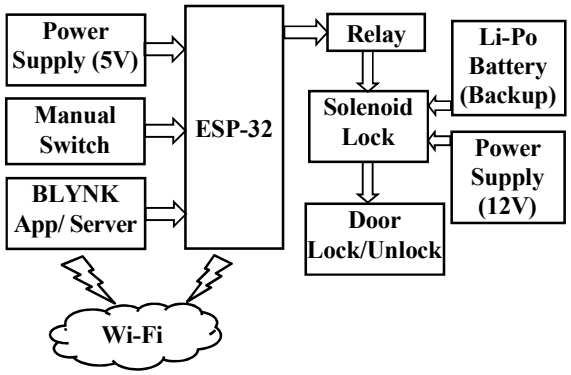


Fig. 5: Block diagram of door lock system (Basic model)

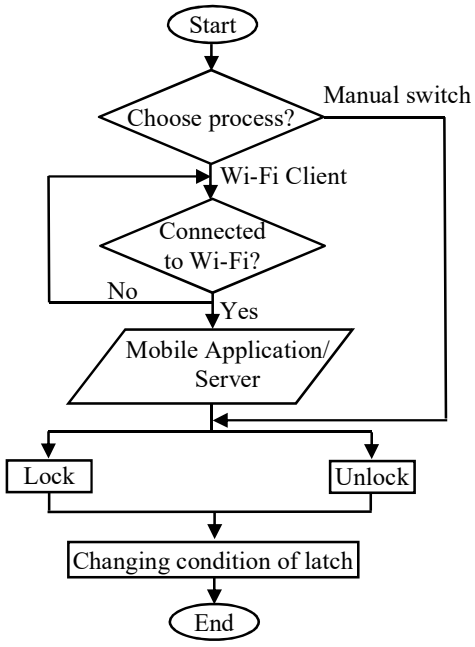


Fig. 6: Flow chart door lock system (Basic model)

B. Advanced Model

The main components are the ESP32 CAM with Wi-Fi and camera module, Battery Management System (BMS), RFID module, manual switch, and solenoid lock. This system provides a switch-based, application-based and authentication-based user access to lock and unlock the door. The switch-based and application-based access is similar to the basic model mainly used to lock and unlock the door from the top floor. The authentication-based access includes face recognition and RFID card access, facilitating the unlocking of the door from the outside. For the RFID card access, each RFID card embedded with a unique identification number (UID) is provided to the user. When the card is brought within the sensing range of the RFID module, it generates the electromagnetic field that powers the card momentarily, and then the module reads the UID of that card through inductive coupling. The UID is then sent to the ESP32-CAM, which is verified with the pre-stored authorized users' identifier in the memory. If there is a match, the microcontroller generates a control signal to the relay driver and the door is unlocked. However, if the UID is not matched, the door remains closed. Similarly, in face recognition, the camera of the ESP32-CAM captures the real-time images of the user, which is input to the face recognition algorithm and compared with the stored

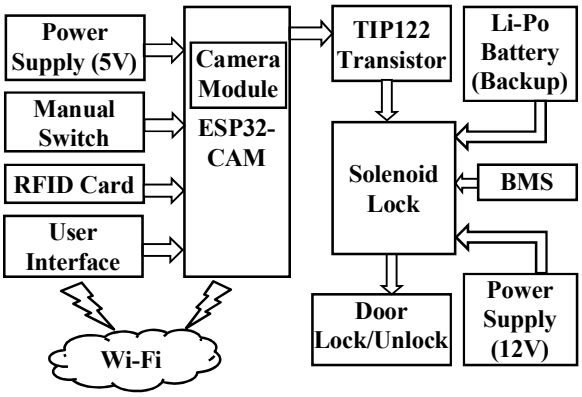


Fig. 7: Block diagram of door lock system (Advanced model)

facial template for verification. For the successful match, the door is unlocked, while it remains locked for the unsuccessful attempts. The detail of face recognition is explained in later sections. A BMS is included to monitor and protect lithium-based portable batteries from overcharging/discharging and overheating, increasing the battery efficiency and lifespan. The block diagram and flow chart for the door lock system (advanced model) are shown in Fig. 7 and 8 respectively.

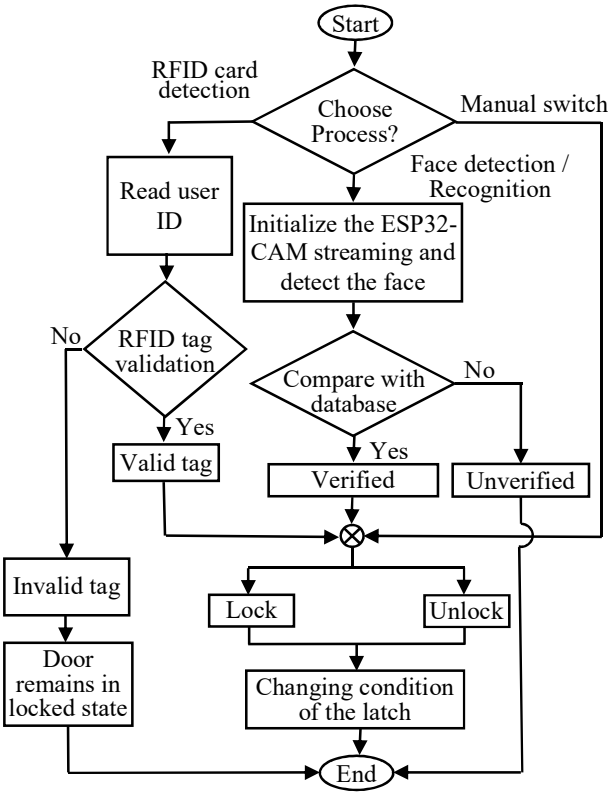


Fig. 8: Flow chart door lock system (Advanced model)

C. Face Recognition

The face detection/recognition is achieved by exploiting the ESP32-CAM's ability to stream live video over Wi-Fi while running its own server. Firstly, the ESP32-CAM board is set up in the Arduino IDE to upload the appropriate firmware and camera configuration. Once the program is successfully uploaded, the assigned ESP32-CAM's IP address can be attained from the serial monitor. Using this IP address in a web browser, the live video stream of the ESP32-CAM can be broadcast. Secondly, the module is modified and enabled to store the captured images on the onboard micro-SD card and also the camera settings were adjusted to support he face detection and recognition. Lastly, a new face is enrolled in the system to create a face database by capturing multiple images to create a facial template and register it. Once enrolled, the ESP32-CAM can recognize the same face later and automatically label it as "Subject 0".

The face recognition system, as depicted in Fig. 9, involves capturing an image containing an individual's face, detecting the presence of a human face by extracting the facial landmarks such as eye spacing, noise alignment, and jawline structure. Once the face is detected, the image is cropped to isolate the region of interest, which is then passed through the image preprocessing, such as resizing and normalization, which is finally converted into a numerical format that represents the face uniquely. The extracted feature vector is compared with the pre-stored face database for verification, and the person is authorized only upon a successful match. Upon successful identification, the system activates an actuator to unlock the door. The communication with the web interface of ESP32-CAM is performed using a standard HTTP address.

The programming structure within the integrated development environment needed for operating ESP32 CAM

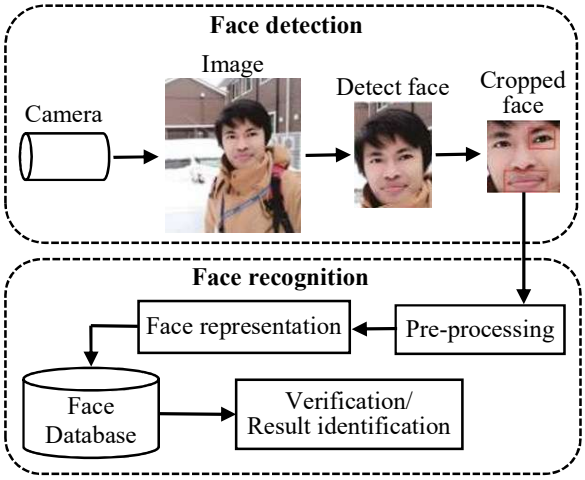


Fig. 9: Face recognition system in ESP32-CAM

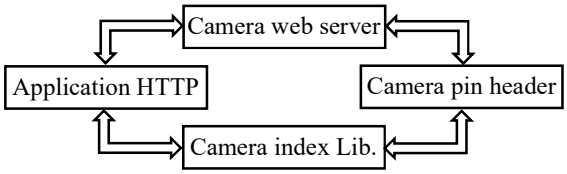


Fig. 10: Programming Packet in Arduino IDE

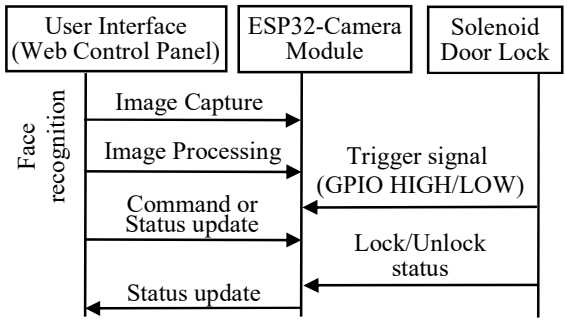


Fig. 11: Data flow diagram of ESP32-CAM

involves combining four entities: the camera web server, the application HTTP (or application server), the camera library, and the camera pin header. These modules must operate concurrently as a unified system, as shown in Fig. 10.

In the data-flow diagram, as demonstrated in Fig. 11, the user interface interacts with the ESP32-CAM to capture the image, process it, perform facial recognition, and send a control signal to the door lock mechanism. At first, the user interface issues a command to the ESP32-CAM to capture an image of the user's face. Secondly, the captured image is processed by the onboard facial recognition algorithm, which extracts the facial features, analyzes them, and compares them with the stored template for verification. The recognition result of the identification process is sent back to the user interface. Finally, based on the recognition outcome, the solenoid lock is controlled. For the case of successful identification of an authorized face, the ESP32-CAM sends a digital HIGH signal to activate the solenoid lock, unlocking the door for a predetermined duration, after which the system automatically resets the signal to LOW, locking the door again.

IV. Prototype Development and Results

The circuit diagrams for the basic and advanced models have been developed. At first, a basic model was developed, and then an advanced model was developed. However, both models can be integrated into the same ESP32-CAM module.

A. Basic Model

The schematic design and the simulation are carried out in the Cirkit Designer as shown in Fig. 12. To incorporate a manual switch with the ESP-32 microcontroller, "VIN" of the microcontroller is connected to one of the terminals of the switch, while the opposite terminal of the switch is connected to "GND" through a resistor of 200 Ω. Likewise, the "D5" pin of the microcontroller is connected to the base terminal of the transistor, while the emitter terminal of the transistor is connected to "VIN" of the relay. The "+VE" and "-VE" terminal of the solenoid lock is connected to the "NO" pin of the relay and the additional "GND" pin of the microcontroller, respectively. The "VCC" and "COM" pins of the relay are connected to the "+VE" terminal of the 12V power supply. After the hardware setup is completed and the code is uploaded to the microcontroller via Arduino IDE, the solenoid lock can be triggered instantly by pressing the switch without any delay in response time. Likewise, for the Wi-Fi access, ESP-32 is programmed to act as a local server, which could be accessed through the IP address attained from the serial port. When this IP address is input in the web browser, the option for "Lock" and "Unlock" is displayed, through which the door can be locked/unlocked with a response time of one second, as shown in Fig. 13.

B. Advanced Model

ESP32-CAM serves as the central controller, which is connected to multiple equipment, including an RFID module (RC522) for card-based authentication, a TIP122 Transistor for switching the solenoid lock, and a push button for manual override or system reset, as shown in Fig. 14. The RFID Module (RC522) communicates with the ESP32-CAM using the SPI interface. The RFID is split into two sub-components, namely, the RFID Reader and the RFID Tag. TIP122 Transistor is used to drive the solenoid lock. The base of the transistor is connected to the "GPIO" pin of ESP32-CAM

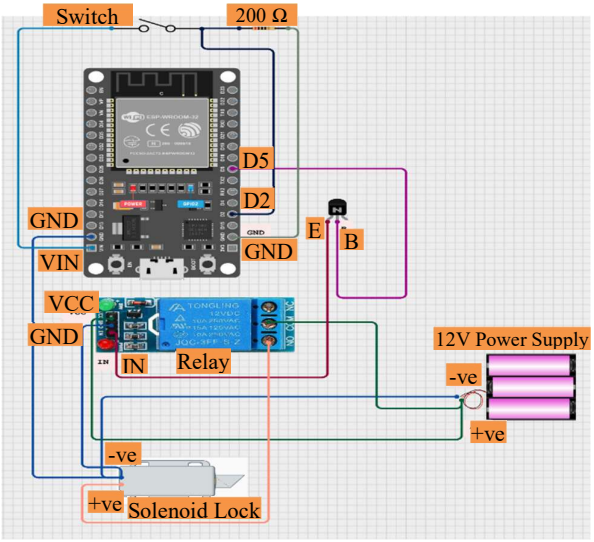


Fig. 12: Circuit diagram for basic model

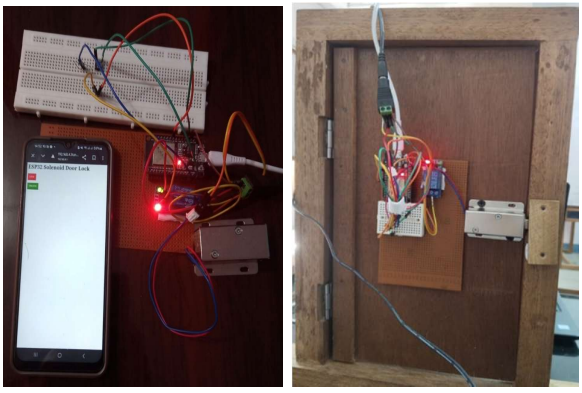
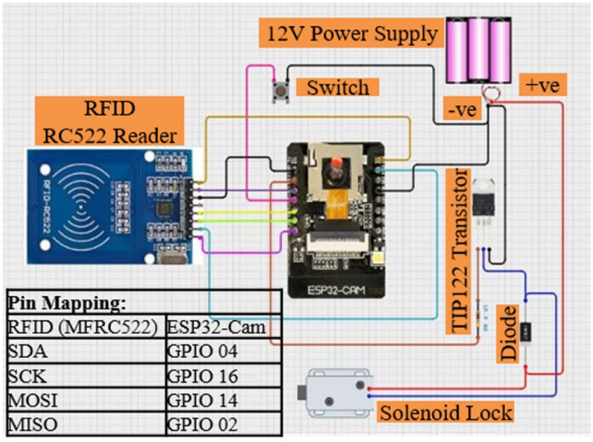


Fig. 13: Developed prototype for basic model

through a resistor, collector to the negative side of the solenoid and emitter to the "GND" pin. A diode is also connected across the solenoid terminals to prevent voltage spikes when switching off. The system is powered by Li-ion batteries. A 3S 10A 12V 18650 Lithium Battery Charger Board Protection Module (BMS) is also included to protect the battery system from overcharging/discharging. The 12V Solenoid Lock has only two states: the locked state, which is the default state and the unlocked state, which is achieved only through the RFID Tag provided only to the authorized users. The developed prototype is shown in Fig. 15, which was tested with the RFID tag. It allowed the successful authorized access while forbidding the unauthorized access.



Pin Mapping:	
RFID (MFRC522)	ESP32-Cam
SDA	GPIO 04
SCK	GPIO 16
MOSI	GPIO 14
MISO	GPIO 02

Fig. 14: Circuit diagram for advanced model

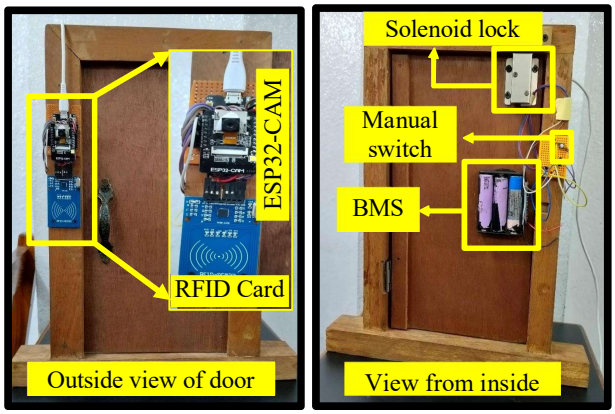


Fig. 15: Developed prototype for advanced model

C. Peformance of face recognition with distance

The ESP32-CAM has a replaceable OV2640 camera with a resolution of 320×240 and a frame size of QVGA. A test was conducted to evaluate the performance of the ESP32-CAM at varying distances. The test results, as listed in Table 1, highlight the fact that the camera module on the ESP32-CAM is capable of detecting faces within the range of 30cm to 90cm. However, at distances of 60cm to 90cm, sometimes multiple attempts are needed before the face is successfully detected. This can be attributed to various factors, such as a reduction in the captured size of facial features as the distance increases and inadequate or uneven lighting conditions. However, faces beyond a distance of 100 cm could not be detected at all. Nevertheless, the camera module is able to detect the face within the practical applicable range and successfully detects and authorizes the faces that are pre-registered in the face database while forbidding the unregistered faces, alerting to an intruder attempt.

TABLE I. FACE RECOGNITION PEFORMANCE WITH DISTANCE

S. No.	Distance (cm)	Detection Results
1	30	Good
2	40	Very good
3	50	Enough
4	60	Enough
5	70	Enough
6	80	Enough
7	90	Enough
8	100	Not-detected
9	110	Not-detected
10	120	Not-detected

V. CONCLUSION

The study has highlighted the inherent local need through a survey conducted among 72 houses in the vicinity of Bhaktapur, Nepal. Considering the expectation of the user, two models, the basic model and the advanced model, have been proposed, permitting the user to select the features based on their requirement, cost and interest. The basic model provides a manual switch and a Wi-Fi-based access to lock/unlock the door, which is mainly focused on accessing the door at the ground floor from the top floor or the higher floors. Likewise, in the advanced model, additional features such as RFID and face recognition are added, which mainly focus on access from outside. A prototype model is proposed using the ESP32-CAM microcontroller with inbuilt Wi-Fi and camera module, RFID module and solenoid lock. For the manual switch, the response time is without delay and for the Wi-Fi-based access, the response time is one second. Face recognition is feasible within an acceptable distance of 30 cm to 90 cm. A mobile-based interface is provided to the user for easy access to the door. Overall, the study is able to point out the local needs for a customized door lock system and present a prototype model to realize it. Furthermore, other features could be easily added based on Bluetooth access, key access, etc., subject to users' needs and cost constraints. In the future, the study aims to develop a product ready to be used by the general public based on the findings made in this research.

REFERENCES

[1] H. N. M. Shah, M. Z. A. Rashid, M. F. Abdollah, M. N. Kamarudin, K. L. Chow, and Z. Kamis, "Biometric voice recognition in security system," *Indian Journal of Science and Technology*, vol. 7, no. 2, pp. 104–112, Feb. 2014.

[2] R. Hasan, M. M. Khan, A. Ashek, and I. J. Rumpa, "Microcontroller based home security system with GSM technology," *Open Journal of Safety Science and Technology*, vol. 5, pp. 55–62, Jun. 2015.

[3] W. Hongyan, M. Xiangyin, and Z. Yang, "Design and implementation of Smart Home integrated control system," in *Proc. International Conference on Computer and Information Technology Application (ICCITA)*, Chengdu, China, 2016.

[4] A. D. O. Agbo, M. Chinaza, and J. O. Odinya, "Design and Implementation of a Door Locking System Using Android App," *International Journal of Scientific & Technology Research*, vol. 6, no. 8, pp. 198–203, Aug. 2017.

[5] A. N. M. Erwan, M. N. H. M. Alfian, and M. S. M. Adenan, "Smart Door Lock," *International Journal of Recent Technology and Applied Science*, vol. 3, no. 1, pp. 1–15, Mar. 2021.

[6] R. S. C. Reddy, P. V. Krishna, M. K. Chaitanya, M. Neeharika, and K. P. Rao, "Security system based on knock-pattern using Arduino and GSM communication," *International Journal of Engineering and Techniques*, vol. 4, no. 1, pp. 154–157, Jan.–Feb. 2018.

[7] T. Adiono, S. Fuada, S. F. Anindya, I. G. Purwanda, and M. Y. Fathany, "IoT-enabled door lock system," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 5, pp. 445–451, 2019.

[8] N. R. S. Nakandhrakumar, S. Aravinth, R. Venkatasamy, K. Balachandar, J. A. Dhanraj, and N. Dhamodharan, "Design and development of IoT based smart door lock system," in *Proc. 2022 Third International Conference on Intelligent Computing, Instrumentation, and Control Technologies (ICICICT)*, 2022, pp. 1525–1532.

[9] A. Abdullah, S. Wang, and Y. Cai, "The design of STM32 micro-controller intelligent home system based on cloud platform," *International Core Journal of Engineering*, vol. 8, no. 1, pp. 536–541, 2022.

[10] S. S. S. Sreeja Mole and A. S. Rao, "Design and implementation of password based door lock security system using 8051, Arduino and keypad," *International Journal of Management, Technology, and Engineering*, vol. 13, no. 4, pp. 119–125, Apr. 2023.

[11] D. R. Saputra and A. Winarno, "Home door security system with face recognition using ESP32-CAM," *Journal of Applied Electrical & Science Technology, University of PGRI Adi Buana Surabaya*, vol. 6, no. 2, pp. 9–14, 2024.

[12] V. T. Gaikwad, P. A. Gawande, G. S. Chirade, M. S. Pandhe, S. N. Panat, B. A. Dehankar, and S. V. Kantale, "Design and implementation of an OTP-based smart locking system using GSM," *Journal of Embedded Intelligence and Vision Systems*, vol. 2, no. 4, Apr. 2025.

[13] M. Ma and Z. Wang, "Design of home smart access control system based on STM32," in *Proc. of SPIE, Fourth International Conference on Electronic Information Engineering and Data Processing (EIEDP 2025)*, vol. 13574, 1357445, pp. 1–9, 2025.

[14] L. Gao and G. Li, "Design and implementation of smart home control system based on STM32," in *Proc. of the 2023 International Conference on Wireless Communications, Networking and Applications (WCNA 2023)*, P. Siarry et al., Eds., *Lecture Notes in Electrical Engineering*, vol. 1361, Singapore: Springer, 2025, pp. 112–125.