Smart door: Motion,face-recognition and voice recognition IOT security

[1] Mr.B.Ajantha Reddy,[2] Mr.K.Ch.Malla Reddy,[3] Immadi Venkata Naga Sai Pujitha,[4] Byragani Manasa,[5] Bathula Varshini,[6] Shaik Fathima,

[1]Assistant Professor, Department of ECE, Krishna Chaitanya Institute of Technology & Sciences, Markapur.

[2] Associate Professor, Department of ECE, Krishna Chaitanya Institute of Technology & Sciences, Markapur.

[3,4,5,6] Student, Department of ECE, Krishna Chaitanya Institute of Technology & Sciences, Markapur.

Abstract: -

The purpose of this project is to make home or office or any area secure. When someone presses the doorbell, then the doorbell makes a video call to the registered number. If someone roams in front of the door it notifies you by sending message. Then he can see the person who is roaming in front of our door. So, if the person is known we can open the door otherwise we can be alert. And also, we can talk to the person through mobile only and the person can reply there itself, because it contains the audio speaker so that we can hear the outside people talks trough the mobile once we pick up the video call. If someone tries to steal it then the steal alarm will be activated.

Keywords:

Smart Doorbell, IOT Doorbell, Security IOT, Smart doorbell, Smart lock, Wireless doorbell, Smart video surveillance.

INTRODUCTION: -

Over the past few years, IOT (Internet of Things) became very important in today's technology. And now days, IOT enabled tools are also became an important part in industries. Because, IOT refers to interrelated, internet connected objects that are able to collect and transfer data over wireless network without human intervention. This is why, now all industries are shifting their interest towards IOT based devices. As it is using sensors, it was low in cost and it consumes low power.

BACKGROUND: DOORBELL SYSTEM: -

Keypads and sophisticated facial recognition technology are only two of the locking mechanisms built into these doors that can tell the difference between the rightful owner and an intruder. Having said that, there have been several shortcomings and restrictions in earlier Internet of Things (IoT) inventive studies that have used RFID-based smart doors. Radio frequency identification is a wireless technology [10]. The results of this research form the basis of a new security system that uses passive Radio Frequency Identification (RFID) technology to lock doors. For safe, user-recorded access to space, we turned to radio frequency identification (RFID) technology. By making use of passive RFID technology, the suggested solution hopes to improve the specified venues' security and access control [11]. The left-hand object in Fig.1 is the interface that holds the lock; it scans the whole RFID chip in the tag whenever it comes into contact with the card. This is the basic idea of an RFID system. There are a number of typical issues that might arise when using RFID as an interface to open IoT smart doors. An difficulty arises when RFID technology is integrated into a laboratory setting. This allows for the automation of several operations, such as data gathering and inventory management, as well as real-time asset monitoring.

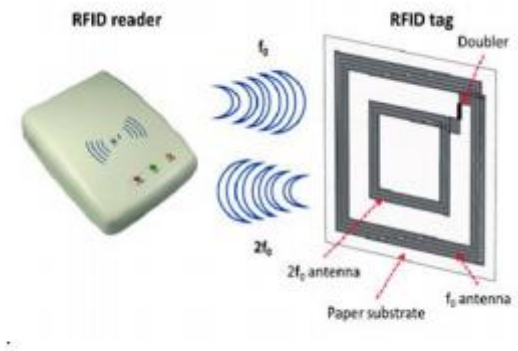


Fig. 1 Concept of RFID system.

The use of facial recognition and detection technologies in smart home security applications is another emerging trend in door safety technology. A MyRIO 1900 and LabVIEW were used to program the system. A wireless network connects myRIO to the PC. A camera linked to MyRIO via a USB connection captures the picture of a person. Although WiFi is convenient, it might influence the real-time performance of the face detection and identification system due to possible delay or instability in data transfer [12]. The devices' shortcomings include a face detection and identification technology that is performance-and accuracy-dependent on the camera and USB connection quality. Forensic science, banking, safety monitoring, and allowing authorized individuals to have preferred access (such in restricted areas) are just a few of the many domains that might greatly benefit from an efficient face recognition system [13]. The principles of the system's operation are shown in Fig. 2. The four faces used in this project will be scanned whenever someone attempts to open the door, and information will be derived from that scan. The next step was to check whether the face was a good fit with the current data. The system will provide access to user C if their data is same or very similar to the existing data, for example, if their name is C. The performance of the face detector is tested under several conditions, including different distances, light intensities, light positions, the color of the person's clothing, and accessories. Figure 3 demonstrates that certain face recognition systems use the Local Binary Pattern (LB), a simple and effective texture operator that assigns binary values to picture pixels by thresholding their immediate surroundings [14].

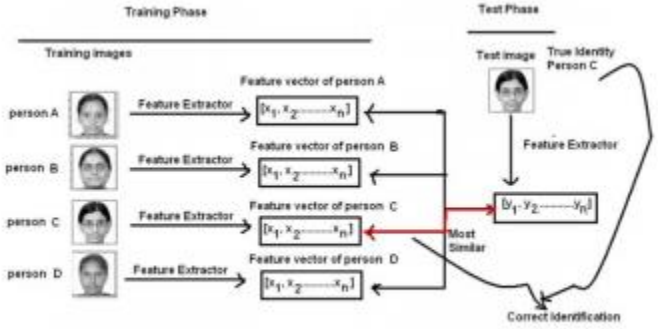


Fig. 2 Concept of PCA-Based Face Recognition [15]

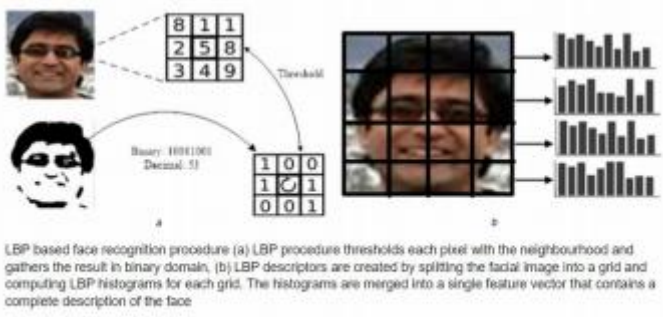


Fig. 3 Concept of LBP -Based Face Recognition [15].

On the other hand, PCA-based and LBP-based face recognition methods may be vulnerable to variations in face texture, noise, and changes in picture resolution [16]. When there are large obstructions, such facial hair or accessories, it could be difficult for them to identify faces. When dealing with numerous people in large-scale face recognition settings, LBP could potentially have limits. There are a number of situations in which the face

identification module could struggle to provide reliable results, including being too far away from the camera, extremely changing lighting conditions or angles, or when people are wearing items that obscure a large part of their features. Another possible issue is that the face identification module has trouble differentiating between faces and backdrops or shirts that are the same color as skin tones [17]. Another one suggested a two-tiered hierarchical network (HN) design for facial recognition, with FaceNet serving as the top layer and a discriminative learning technique as its bottom. In addition, we developed a model that takes into account the embedded system's multi-mode recognition and the homeowner's consent as sent by email. The identification procedure might be slowed down or made vulnerable if it relies on the homeowner's email permission [18].

III. METHODOLOGY

Better security and access control may be achieved by enhancing the smart door system's capability, as shown in Figure 4, which analyzes human actions and precisely identifies them. Finding people and understanding what they're trying to accomplish is the main goal of the suggested smart door system. At first, the system takes a picture from a camera or a foam spot and uses facial recognition software to figure out whether the thing it saw is a person. It starts by verifying that the code entered via the Arduino Uno-connected keypad is legitimate. The door will open and the authorized person will be let in if the code is right. The system also checks whether the Blynk app is being utilized in case the keypad is not being used [19, 20].

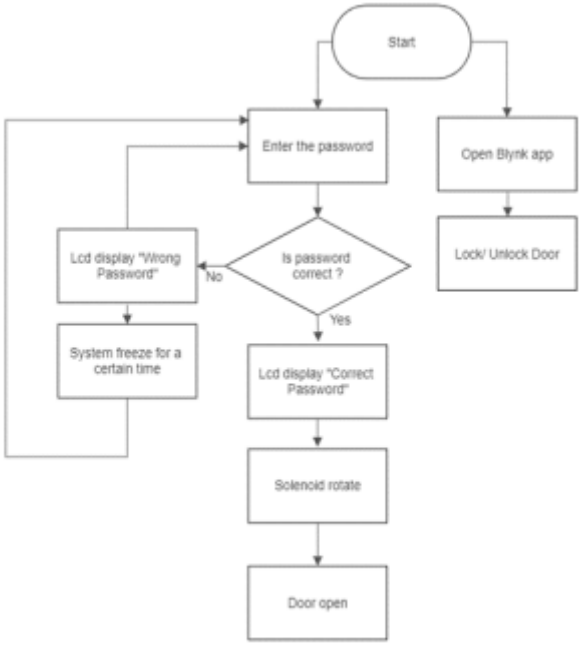


Fig. 4 IoT Smart Door using Keypad and Blynk Process.

For a safe and easy way to manage who can enter and out, check out Figure 5. It's an Internet of Things (IoT) smart door system that uses the ESP32 Camera module and Arduino Uno to detect motion and recognize faces. The smart door can only be opened by authorized users thanks to the system's use of several techniques. One other way to open the Internet of Things smart door is using a motion sensor. The ESP32 Camera module takes a picture and transmits it to the Blynk app. The owner is notified along with the picture and may decide whether to let the person in front of the smart door access. This system is more secure since it lets the owner see the person's identification before letting them in. Plus, if the Blynk app and keypad aren't being used, the system will use a PIR motion sensor that is linked to the ESP32 Camera module. The camera snaps a picture of anyone is standing in front of the door as soon as it senses motion. Quickly, the Blynk app receives this photo and alerts the owner that someone is trying to get in. The owner may see the picture and decide for themselves whether or not to provide access. The smart door opens whenever it is authorized, making entrance a breeze. The integration of keypad functionality, face recognition, and motion sensing creates a strong access control system that can adapt to different situations and user preferences. With the Internet of Things (IoT) smart door system, homeowners and building managers can rest easy knowing that their property is better protected thanks to improved access management made possible by cutting-edge technology.

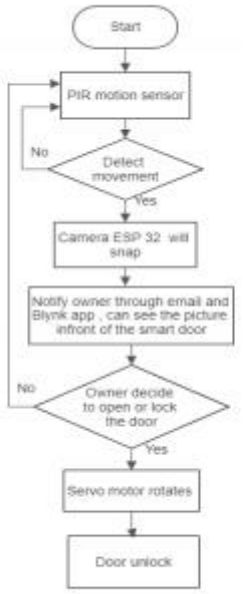
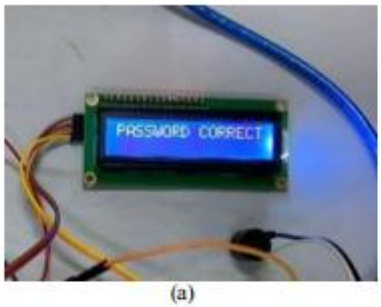


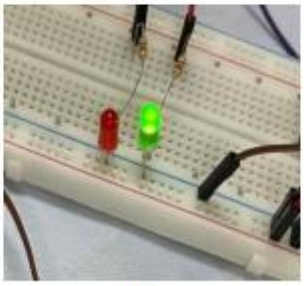
Fig. 5 IoT Motion Sensing with Face Recognition Process.

A. Test with the Correct Password

When the door lock is in the lock state, as shown in Figure 6, the LCD will show the message "Password Correct." "Door Unlocked" appeared on the LCD after we entered the proper password to test the system. As seen in Figure 6 (b), the green LED would likewise light up to indicate that the password is correct. In the event that someone is about to ring the doorbell, the buzzer would go off for three seconds. In addition, the door may be opened by simply rotating the servomotor. The servomotor would go back to its default position after 10 seconds, and the door would lock as it always does.



(a)



(b)

Fig. 6 LCD (a) Lock Condition (b) Entering the Correct Password.

B. Test with Incorrect Password

An incorrect password will cause the red LED to light up and a buzzer to play for three seconds, as shown in Figure 7 (a). The user inputs an incorrect password, which is shown on the LCD (Figure 7(b)), indicating that the password was entered incorrectly. No rotation will occur; the servomotor will stay still. See Fig. 7 (c) for an example of what happens when the user tries to open the door three times but gets stuck: an LCD screen says "Please Wait," meaning the user has to wait one minute before they can use the keypad to input the password again. No password may be entered by the user during this one minute. In conclusion, we can say that the

keypad locking technique is an effective way to keep the smart door secure. To avoid theft or abuse, it is vital to restrict the number of tries to enter a password and to make sure that users do not forget the right password. It is easier to provide people accurate feedback when they can see and hear indications, such LED lights and a buzzer. Finally, our smart door-locking system now has the ability to respond appropriately to both valid and incorrect password inputs. By restricting the amount of password tries and applying a time penalty for users who fail to open the door, the keypad locking system adds an extra layer of protection.

(a) (b) (c)

Fig. 7 (a) Red LED lights up when the wrong password LCD is displayed when (b) entering the wrong password (c) "Please Wait" after three wrong attempts.

With this rollout, we also included support for opening the Internet of Things smart door via the Blynk app. The user may open the IoT smart door by touching a button on their smartphone screen, as shown in Figure 8, using Blynk and its application. The servo motor will spin around its own axis and stay that way for ten seconds after the button is pushed. Throughout this time, users will be able to access the Internet of Things smart door. The smart door will be latched and the servo motor will return to its original position after 10 seconds. For the Internet of Things smart door, the Blynk app is the way to go because of how easy and convenient it is to use. The user only has to touch a button on their smartphone screen to unlock the door, eliminating the need for a keypad or password. This may make it easier for users to access and provide them a better experience when they engage. But it's critical to make sure the Blynk app is secure and that only approved users may unlock the door. Our tests showed that the Blynk app's buttons did, in fact, respond to user input. Users are able to open the door with the anticipated motion of the servo motor when the button is pushed. The door is securely fastened after 10 seconds because the servo motor goes back to its initial position.

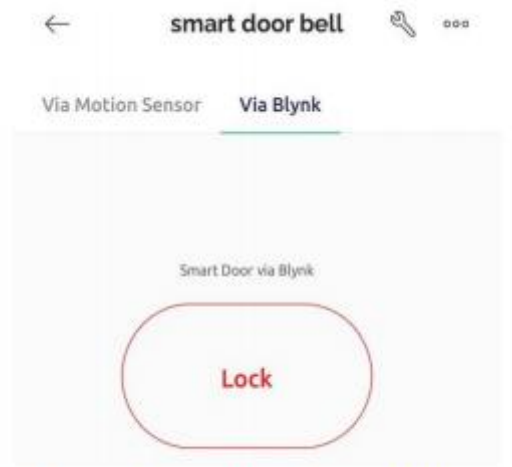
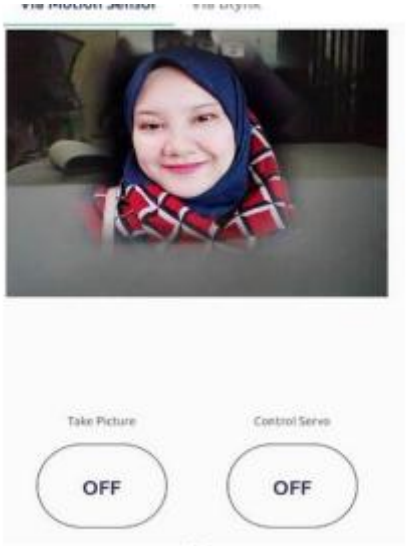


Fig. 8 Displays the Control Door Lock via the Blynk app.

Lastly, we integrated a PIR motion sensor to detect movements in its vicinity and open the IoT smart door accordingly. The smart door's PIR motion sensor takes a picture of the area in front of the door the second it senses movement, such as when someone tries to open it. After that, they will view a picture of the smart door's front panel, which will have an interface similar to Fig. 9 (a). Pressing the "open" button on the screen will cause the servomotor to spin and open the door for the user if they identify them. The servomotor will go back to its default position after a short while, and the smart door will lock automatically. As shown in Figure 9 (b), a subsequent email alert is issued by Blynk to indicate that an unauthorized individual is attempting to access the residence. The owner of the Internet of Things smart door has the option to disregard the alert or see the recorded footage using the Blynk app. The user gets alerted that there is an object blocking the smart door the moment they launch the Blynk app.



(a)

Fig. 9 (a) Display control door via motion sensor

(b)

Fig. 10 (b) notification appears from email and Blynk app.

This project's data analysis is centered on the PIR (Passive Infrared) motion sensor. It entails deciphering the data acquired by the sensor in order to discover patterns of human movement or presence. In Fig. 10, we can see how far and wide the PIR motion sensor can detect movement in the designated region. The prototype door's PIR motion sensor, as seen in the green region in the middle, was mounted at a height of 76 cm and faced forward. The blue region depicts the range where the PIR motion sensor can detect any movement within three seconds without any failures, according to the tests. Conversely, the yellow region denotes the range of motions that the PIR motion sensor is limited to detecting, which is 5–18 seconds. For this reason, it is reasonable to assume that the PIR motion sensor has a range of 240 cm at its most sensitive. On the other hand, the PIR motion sensor was shown to be ineffective in detecting non-human motions, such as things falling from a height, in all three trials. Because it is able to identify just human motion and not any other kind of movement, this security feature is deemed safe to employ.

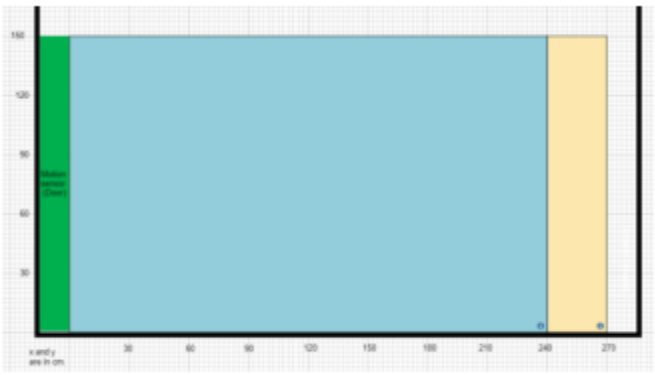


Fig. 11 Displays of the motion sensor to detect movement range.

The functionality of the prototype door's PIR motion sensor to detect movement within a specific range was shown. Within a three-second time frame, the blue region signifies the effective range of the PIR motion sensor that detects movement. Be aware, however, that the yellow circle represents the sensor's restricted detection range for motions lasting 5–18 seconds. Within a range of up to, the PIR motion sensor can reliably identify people moving about. length 240 cm. On all three occasions, however, it was unable to identify motions that were not caused by humans, such as things falling from above. That yet, the PIR motion sensor's ability to reliably and safely identify human movements—the key to unlocking the smart door—makes up for this drawback.

Conclusion

Finally, the motion-sensing and face-recognition technologies integrated into the suggested Internet of Things smart door framework have been effectively implemented to improve security and access management. By taking pictures and evaluating human presence and behavior, the technology provides strong verification and permits easy and safe entrance. The smart door is more secure as a whole thanks to facial recognition technology, which allows the system to correctly identify authorized users. This feature offers a dependable method of access control by limiting access to authorized persons and prohibiting unauthorized entrance. The Internet of Things smart door provides further safety, ease, and comfort with its motion detector and facial recognition features. The homeowner may see who is trying to get into their home, see what the cameras have caught, and decide whether to let them in or not based on all that information. With this degree of management, homeowners can make sure their property is safe and secure. Improving the speed and accuracy of face recognition systems might be the focus of future research and development in this field. The system's capabilities may be much more enhanced if we looked at adding other security measures like biometric authentication or speech recognition.

REFERENCES

[1] S. A. L. Sujita B. Dabekar, Manasi S. Lunge, Prof. Deepali Yewale, "IOT Based Smart Door Locked System Using Node MCU," *Ijraset Journal For Research in Applied Science and Engineering Technology*, vol. 10, no. 7, pp. 4384-4388, July 2022 2022, doi: https://doi.org/10.22214/ijraset.2022.45909.

[2] M. K. R. Effendi, M. Kassim, N. A. Sulaiman, and S. Shahbudin, "IoT Smart Agriculture for Aquaponics and Maintaining Goat Stall System," *International Journal of Integrated Engineering*, Article vol. 12, no. 8, pp. 240-250, 2020, doi: 10.30880/IJIE.2020.12.08.023.

[3] N. Z. Zamzari, M. Kassim, and M. Yusoff, "Analysis and Development of IoT-based Aqua Fish Monitoring System," *International Journal of Emerging Technology and Advanced Engineering*, Article vol. 12, no. 10, pp. 191-197, 2022, doi: 10.46338/ijetae1022_20.

[4] K. Gupta, N. Jiwani, M. H. U. Sharif, M. A. Mohammed, and N. Afreen, "Smart Door Locking System Using IoT," in *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 10-11 Nov. 2022 2022, pp. 1-4, doi: 10.1109/ICACCM56405.2022.10009534.

[5] M. Kassim, A. S. Salleh, S. Shahbudin, M. Yusoff, and N. A. Kamaluddin, "IoT Bus Tracking System Localization via GPSRFID," in *2022 IEEE International Conference in Power Engineering Application, ICPEA 2022 - Proceedings*, 2022, doi: 10.1109/ICPEA53519.2022.9744710

[6] M. N. A. M. M. H. S. O. F. Mohammed Shoaibuddin Ahmed, "Smart and Secure Door Lock with Dual-Factor Authentication for Critical Zones," *Mathematical Statistician and Engineering Applications*, vol. 72, no. 1, pp. 1491-1501, 01/12 2023, doi: 10.17762/msea.v72i1.2373.

[7] M. Khalid and S. Majeed, "A Smart Visitors' Notification System with Automatic Secure Door Lock using Mobile Communication Technology," *International Journal of Computer Science and Information Security*, vol. 16, 12/19 2018.

[8] U. A. Norarzemi *et al.*, "Development Of Prototype Smart Door System With IoT Application," *Progress in Engineering Application and Technology*, vol. 1, no. 1, pp. 245-256, 12/14 2020.

[9] D. Aswini, R. Rohindh, K. S. M. Ragavendhara, and C. S. Mridula, "Smart Door Locking System," in *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, 8-9 Oct. 2021 2021, pp. 1-5, doi: 10.1109/ICAECA52838.2021.9675590.

[10] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," in *2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, 26-28 Oct. 2022 2022, pp. 453-457, doi: 10.1109/GECOST55694.2022.10010367.

[11] A. Waqar, I. Othman, N. Shafiq, and A. Mateen Khan, "Integration of passive RFID for small-scale construction project management," *Data and Information Management*, vol. 7, no. 4, p. 100055, 2023/12/01/ 2023, doi: https://doi.org/10.1016/j.dim.2023.100055.

[12] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," in *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 1-2 Nov. 2017 2017, pp. 342-347, doi: 10.1109/ICITISEE.2017.8285524.
[13] Z. Zhu and Y. Cheng, "Application of attitude tracking algorithm for face recognition based on OpenCV in the intelligent door lock," *Computer Communications*, vol. 154, pp. 390-397, 2020/03/15/ 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.003.
[14] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, "Smart Home Security Using IoT and Face Recognition," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 16-18 Aug. 2018 2018, pp. 1-6, doi: 10.1109/ICCUBEA.2018.8697695.
[15] M. P. Gawande and D. G. Agrawal, "Face recognition using PCA and different distance classifiers," *IOSR Journal of Electronics and Communication Engineering*, vol. 9, pp. 01-05, 2014.