Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 7, Issue 07, July -2020

Door Lock System Using Raspberry Pi

IOT BASED DOOR LOCK SYSTEM

[1]Saurabh Sharma, [2]Dr.D.D. Chaudhary

[1]*Department of E&TC, Sinhgad Institute of Technology, Lonavala*
[2]*Department of E&TC, Sinhgad Institute of Technology, Lonavala*

Abstract: *We are facing security issues in every area of this period. So to solve this question we are proposing a door locking / unlocking process regulated in real time application that harnesses the power of IOT and machine learning for smooth functionalities. The door unlocking device suggested here uses a Raspberry Pi 3 model B for processing along with a Pi Webcam to face up as a user view. Often, fingerprint sensor is used to allow door unlocking fail proof. Using this sensor, situations such as poor lighting and camera malfunction can be managed using ease. From time to time, the face detection and recognition program used for door opening will be able to learn the faces of users and refresh their dataset. So any small user-facing adjustments like inserting spectacles or cutting beard can be managed with ease.*

Keywords:- *Raspberry Pi 3, Pi View, Cascade Classifiers, Machine Learning, IOT, Fingerprint Sensor*

I. INTRODUCTION

Automation and health became a critical aspect of life. The Internet of Things has proven to be the technology harbinger combined with protection for the naïve people. Live video recording was used for quite some time. These days, video monitoring has become very smart and reliable. With the power of extracting and processing the image, live video feature recognition became common. Video data is broadcast and processed using module Pi Camera. A face-recognition algorithm is made to run on the image after gathering compressed image from live video stream. Faces that are present in the processing image are detected using the Haar Cascade classifier for face recognition. Then-face fits with the model previously learned, and the percentage of trust is determined. If the percentage of trust reaches 80 percent then a control message is transmitted via Raspberry Pi to the servo motor. This control message would start the servo motor thus spinning the door knob or handle.

The primary application of this door locking / unlocking device is the facial recognition. We use the new camera module to take the image and check it with the storage database, then if the image fit then send a request to the administrator and if the administrator returns a authentication code in the form of OTP then the system will open the door and if OTP does not fit the stored data then the system will never allow the user to open.

II. SYSTEM OVERVIEW

The complete proposed system will consists of Raspberry Pi model B, Pi camera module, a fingerprint sensor, a MG995 Tower Pro Servo motor along with the required circuitry for connection.
Functional modules for operation of the system are as follows:

Step1. Storing user data

Step2. Model for training of user face

Step3.Face detection from image input

Step4. Face recognition

Step5. Giving unlocking permission Step6.Remotely controlling door unlocking

For above said steps the system regularly updating data set of known faces.

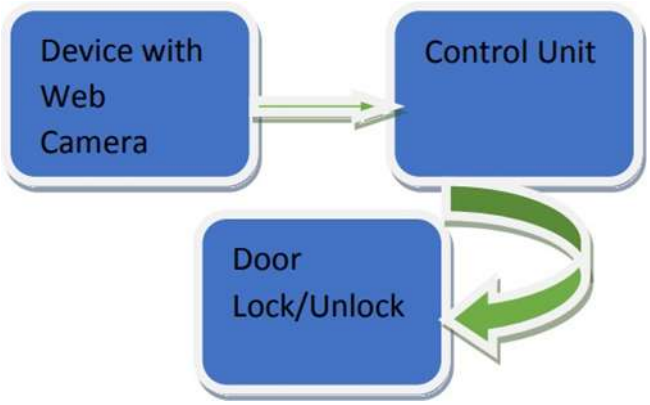

Fig. 1 System Architecture for proposed model

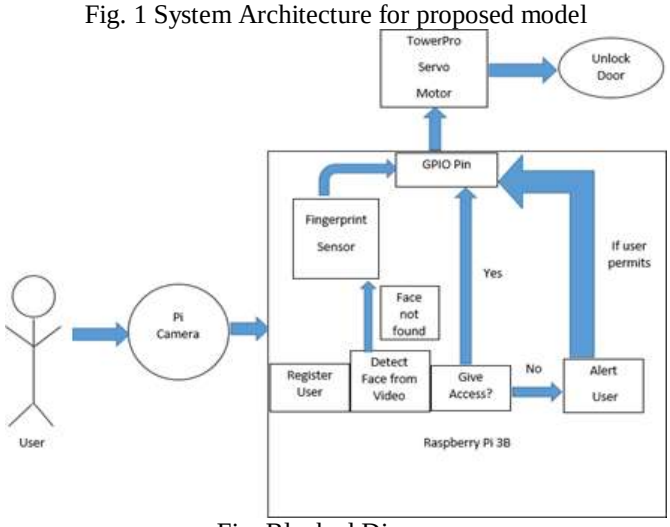

Fig. Blocked Diagram

III. PROPOSED METHODOLOGY

If a person enters at the door and appears to the camera then the individual's faces are deleted from the feed and placed in the device. Then, the removed mask is preprocessed. Therefore the profile fits current user(s) identity database. Connection consent is accorded to the individual in the event that he / she is a verified customer. If not, the controller may be issued an error message and may grant or refuse permission to open the door remotely. Right now let's dive into various methodologies.

Storing user data:
We obtained facial data from more than a thousand photographs from the users. Such images were often cut to a suitable size and only specific features such as the nose, chin and eyes were considered as a sample. For the sampling process all the history data which are not a genuine face have been removed.

Model for training of user face:
LBPH Face Recognizer is used to make raspberry pi3 recognize user's profile. Local Binary Patterns Histogram is a common face recognition algorithm that labels an image's pixels by generating a threshold value for neighboring pixels and a binary number is the result created. We are taking 3X3 matrix from top left corner for each user image (we received a thousand of them). Considering the threshold of the middle pixel of the matrix we define every pixel value. Converting this new binary value into decimal gives the 3X3 matrix 's current pixel value for the middle pixel. This matrix generation method is extended to full image formation. Following this a histogram is generated for every image from the pixel values generated above. Each histogram represents the characteristics of a given image..

Face detection from video input:
We also used a Pi Camera module to grab user's camera frame from a live stream. Used to get area of interest from the video stream after receiving a live video feedback from Pi Camera, haar cascade frontal face classifier. This facet classifier helps to differentiate faces from non-facial artifacts.

Face Recognition:
After the training of LBPH algorithm using genuine images, a new unknown image is now given to the learned recognition model as input. This new face is created from the above stage of video stream facet selection. Using the same

LBPH algorithm a histogram for this new image is created. Then for facial matching, we equate the pattern of qualified faces histograms with the histogram for new unknown faces. For contrast we use Euclidean distance calculation here. Such distance from Euclidean gives one a confidence factor. Higher the importance of trust means the probability of genuine usage is higher. It is because the values of confidence here indicate how closely related the two histograms are.

Give unlocking permission:
We set the confidence value for this program to 80 per cent. If the confidence value is higher than that, then the servo motor will receive a signal message from the general purpose input output (GPIO) pin of raspberry pi. This message to activate begins the servo motor. The motor must eventually produce required amount of torque to rotate the door handle.

Remotely controlling door unlocking:
If any unfamiliar face is identified then the system owner is sent a prompt response. User will then grant permission to unlock remotely from the prompt dialog box. This feature would require the doors to be remotely unlocked for visitors or relatives going into the building.

Regularly Updating data set of known faces:
To manage future improvements that arise in the user's face, such as growing beard or wearing eyeglasses, we must continuously refresh the generated data collection for the user. Here, using time as a guideline, we'll grab with time some new user faces to manage transitions.

Handle poor camera vision:
For situations where consumer is not spotted by camera due to poor light, using the fingerprint sensor, we have implemented a fail-safe feature. When the door is not unlocked, the user may use the fingerprint sensor to open the door.

IV. IMPLEMENTATION AND RESULT

So we need some experimental setup to get a better understanding of proposed model.
Who is approved by the admin first stands in front of the camera, taking the person's face and stored in the photographs of the admin archive. If the images stored with the captured image are recognized the door will be locked / unlocked. If the image of the user is not remembered, the program must send the image capture to the admin and wait by admin for the OTP. If admin allows the device to be locked / unlocked with OTP, the system allows the user to save the captured picture in the admin folder.
The software may be mounted without human intervention where restricted access is necessary.
The complete hardware setup above is shown to detect people 's face in real time and to send images matching the database. This system was tested with different IoT configurations.

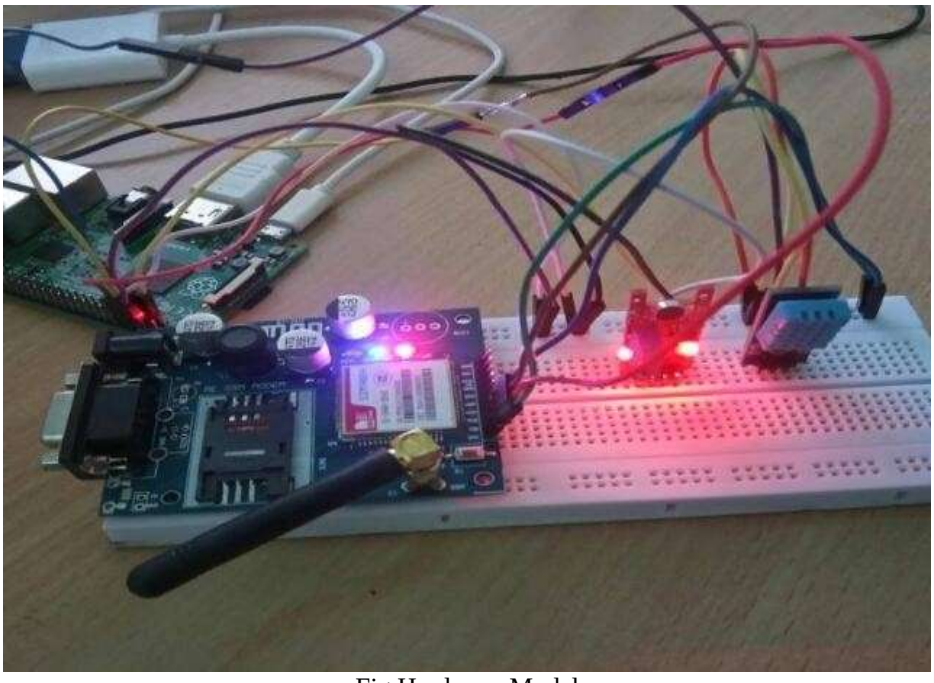

Fig.Hardware Model

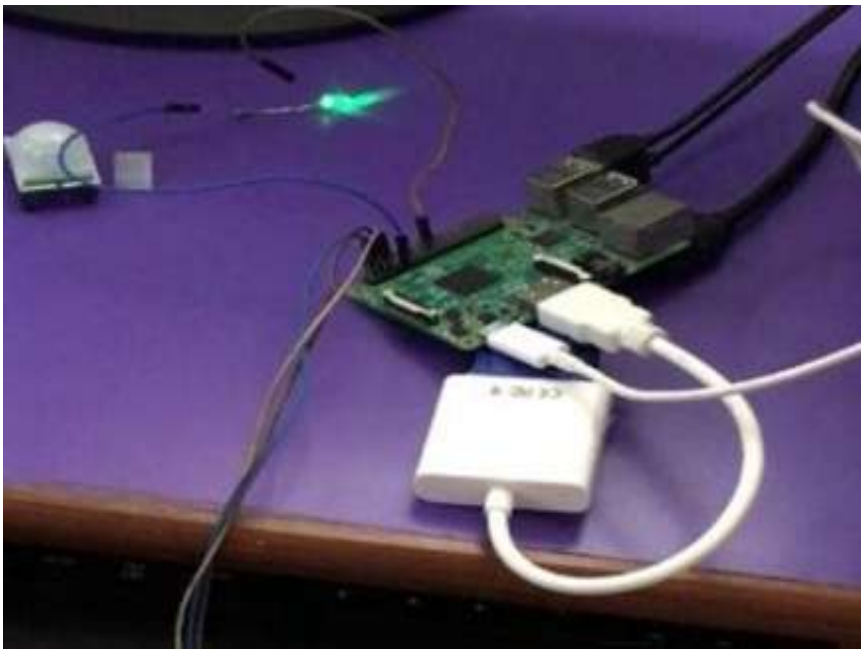

Fig. 3 Working Model

This is a time graph of accuracy for performance and time taken for detection of faces as a real data should receive. We get better result as system trained the data which are stored in the database and face detection should be very easy. That simply shows if the image is found in the database system get more accurate and produce result is simple as possible. So that, this proposed model getting more accurate when system trained day by day with real time images.

V. CONCLUSION

Smart door locking/unlocking system will help in developing keyless door locking/unlocking and also remote door unlocking. This IOT based device will remove the need of manually locking/unlocking the door for the registered user. Also for an unknown user, this device will provide an extra layer of security for the residents of the house. An alert message will be immediately send to the registered user when unknown face is detected. This will help in user to decide whether or not to allow a particular person.

VI. REFERENCES

[1] Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization systems for wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 6, pp. 6–12, 2007.

[2] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: indoor location sensing using active RFID," in Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom '03), pp. 407–415, IEEE, Fort Worth, Tex, USA, March 2003.

[3] C.-N. Huang and C.-T. Chan, "ZigBee-based indoor location system by k-nearest neighbor algorithm with weighted RSSI," Procedia Computer Science, vol. 5, pp. 58–65, 2011.
A. Oka and L. Lampe, "Distributed target tracking using signal strength measurements by a wireless sensor network," IEEE Journal on Selected Areas in Communications, vol. 28, no. 7, pp. 1006–1015, 2010.

[4] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF based user location and tracking system," in Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00), vol. 2, pp. 775–784, IEEE, Tel Aviv, Israel, March 2000.

[5] Z. Dian and L. M. Ni, "Dynamic clustering for tracking multiple transceiver-free objects," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom '09), pp. 1–8, Galveston, Tex, USA, March 2009.

[6] Xu, B. Firner, R. S. Moore et al., "SCPL: indoor device free multi- subject counting and localization using radio signal strength," in Proceedings of the 12th International Conference on Information Processing in Sensor Networks (IPSN '13), pp. 79–90, Philadelphia, Pa, USA, April 2013.

