International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 02 | Feb 2022 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION OF IDS (INTRUDER DETECTION SYSTEM)

Kanchan[1], Vedika Agarwal[2], Shivansh Agarwal[3] , Sukriti Singh[4], Satakshi[4]

[1] *Assistant Professor of Computer Science Engineering Department, MIT College, Uttar Pradesh, India*
[2] *Student. of Computer Science Engineering Department , MIT College, Uttar Pradesh, India*

Abstract - *The primary goal of an intruder detection system is to provide home security and monitoring The project's The goal is to create a more advanced home monitoring system that uses machine intelligence and the industrial iot. In order to not only detect but also block intruder entry, allowing the user to rest certain that he is safe. We used a Raspberry Pi as our core hardware for our system, which is connected with a motion detection system and a buzzer system to detect and avert intrusion. . After the detection is complete, the user will get a multimedia message which will allow him either sound the buzzer system or save the intruder's data (in case ,the intruder is not a theft to the user) and the next time the detection is done the previously recorded data will be taken into consideration*

Key Words **Raspberry Pi ,Buzzer Circuit, Face Recognition**

1. INTRODUCTION

Numerous alternatives in conventional and biometric innovation to meet home security demands.and offices during throughout the previous several years Some of the more common security measures, including If you have keys, passcodes, or ID cards, these might be an issue. if the access items are stolen or lostWhen access is taken by those who don't have authority to acquire access, such security solutions have flaws. and when regular activities, such as work or school, cause someone to leave the house empty. Even when the house is locked or properly locked, this renders it vulnerable to break-ins and theft. People from all areas of life benefit from the growth of information technology and communication today. Because biometric systems may fulfil two functions: identification and verification, they are fast growing, particularly in the realm of home security technology. Biometrics contain features that cannot be forgotten, faked, or lost, and their inherent existence in people is distinct from that of other individuals, assuring their uniqueness.Face recognition

as authentication is very good, according to the journal, because the face is a physiological trait that is simplest to identify between persons, As a result, it's one of the forensics technologies that's always being researched and developed..

The Internet of Things (IoT) is a system of interconnected physical devices that can interact and share data without the need for human involvement. Because IoT allows us to gather information from all kinds of mediums, such as humans, animals, automobiles, and household appliances, it has been explicitly characterized as a "Infrastructure of the Information Society." By integrating electronic hardware within any physical device that may be given an IP address, including detectors, application, and networking gear The project's objective is to develop a better home monitoring system that incorporates artificial intelligence and the internet of things. to facilitate data transfer over a networkAny real-world device may be integrated into an IoT system.

Other research papers focused on constructing a door security system that combines Raspberry as a microcontroller and open source OpenCV as a face reader, where this study scans faces that have been entered into the database and then matches the photos obtained by the webcam.In this project,we create a face recognition system. It aids in the selection of a suitable approach from a large number of options based on our application needs, as well as the resolution of existing difficulties in real-time applications to some extent. In real-time scenarios with multiple variables and seamless settings, we obtain 96.8% accuracy. This technology may be described as an automated electronic lock. This technique is intended to be able to combat theft in homes that are frequently abandoned by their owners.

This work is expected to make a substantial contribution to a new field of research on the use of accurate face recognition technology in residential door locking systems. As a result, the purpose of this study is to develop a facial recognition systemfor use on home doors.

2. METHODS

We suggest a facial recognition method for home surveillance using a buzzer circuit in this study, namely stepsof data collection from homeowners, data training, the Raspberry Pi for facial recognition as well as a buzzer system linked to the alert box program.We use the facial recognition technology using CNN's approach in this journal. Specifically, the Raspberry Pi will be used as a microcontroller and the buzzer circuit will be used for alerting the nearby people and help them to know somethingis suspicious.

2.1. Data Collection from Homeowners–

The steps of data collection are done manually, most notably by using a programme designed to take face data from each homeowner, which comprises of 5 people, for a total of 1,100 data points, which will then be split by 1030 for training data. The technique of facial enlargement begins with moving 10-15 different phrases for 15 different degrees.

2.2. Data training-

The training procedure is carried out on a separate computer with Intel Core i5 8000 Processor specifications and 8gb ram DDR4 Memory, where this training process will also build a model that will be utilised to recognise the face, due to the Raspberry Pi's limited processing. In the training stages, the CNN Alex net technique with two convolution processes and two pooling processes is employed, as well as SoftMax with multiple iterations of 20 times with the parameters

2.3. The Raspberry Pi for facial recognition-

The Raspberry Pi was designed in 2012 with the goal of making digital creation accessible to everyone. Pi's of various types are utilized in classrooms, libraries, research fac ilities, and, of course, hackerspaces across the world. Raspbian is a Debian-based Linux system. To expand the Raspberry Pi's capabilities, accessories may be added. The camera board features a flexible flat cable (FFC) that connects to the Raspberry Pi board's camera interface slot[1]. The camera interface is found between the HDMI and Ethernet connections.

Fig -1: Raspberry Pi

2.4. Buzzer system linked to the alert box programme-

The buzzer systemis a systemthat alerts others around based on the answer obtained by the user via the alert box application. The alert box application is a cloud storage-based program that delivers the image of the intruder to the user after facial recognition by the Raspberry Pi. The user has the choice of responding yes or no, which determines whether the buzzer systemis switched on or off.

The suggested system will make use of the following technologies:

2.4.1. Motion detection technology-

Motion detectors are frequently used in security applications to monitor a specific location for unauthorized access. A motion detector, like a burglar alarm, plays an important security function. When an accelerometer, for example, is actuated, a security camera is activated to record video or take a snapshot of the intruded area and alert the users.. The proposed system makes use of a Passive Infrared (PIR) motion detector, which detects changes in infrared energy level caused by moving objects such as humans and animals.

2.4.2. Python (Programming Language)

In addition, as compared to languages such as C++ and Java, this programming language requires users to implement less code lines to perform coding principles. Having a main function in python is useful. It makes it easier to see the difference between where our functions/classes are defined and where your entry point is. More importantly, it allows you to only run code from that python script in the case thatit is the main script being run. [1][2]Python is therefore ideal for developing the suggested Raspberry Pi Surveillance System.

2.4.3. IOT (Internet of Things) AND AI (Artificial Intelligence and Internet of things)

The system necessitates an invasive and costly wired installation as well as the usage of high-end personal computers. The system formerly relied on a phone connection and employed a phone-based remote controlled.. The remote control and monitoring of a house over the internet necessitates the use of a laptop or computer, which is huge and cumbersome to carry about all day. As an alternative, mobile phones with operating systems can be used for remote control and monitoring of a home. The systemcommunicates between devices using wireless technology. They build a network with inbuilt Wi-Fi technology, allowing appliances to connect with one another.

2.4.4. Developing Face recognition in Raspberry Pi-

The first step is to take care you've got Python and also the OpenCV module put in. we'll be mistreatment the OpenCV python module to handle all of the serious image process concerned..

```
sudo apt-get install python
python-opencv
```

Fig -2: installation

To properly identify a face using a picture, the code must examine each sub-region of the image for facial traits. We may need to check as many as 600 features, or possibly more. To achieve this, OpenCV does some simple, rapid, broad tests on each sub-region to determine whether it includes anything that may be a face. If these preliminary tests are positive, additional extensive testing will be conducted to confirm the initial finding. This also involves ensuring that OpenCV can rapidly determine that some sub-regions lack a face, allowing you to save time by skipping the more extensive checks. We'll need to provide a Template matching file to really conduct these cascades. This file is an XML file that provides information from a training session in which a large number of photos were processed to determine how well it performed in cascading tests. While you may create these files yourself through a training process, there are a number of ready-made files that will identify a variety of typical targets.

We can now look at how to recognize faces inside photographs now that we have everything set. To keep things simple, we'll assume we have a static image in the file 'faces.jpg' that we're going to attempt to process. Create a new cascade classifier based on one of the Haar cascade files as the initial step.

One thing to be aware of is that 'cv2 Cacade Classifier67()%' will not complain if the filename handed doesn't exist. Since OpenCV does most of the processing in

```
face_img = cv2.imread('faces.
jpg')
 gray_img = cv2.cvtColor(face_img,
cv2.COLOR_BGR2GRAY)
```

Fig -3: Image capturing code

greyscale, we will need to convert the image if it is in color.We can now get OpenCV to start looking for faces. A good starting point could be the function below.

```
faces = face_cascade.
detectMultiScale(gray_
img, scaleFactor=1.1,
minNeighbors=5, minSize=(30,30),
flags=cv2.cv.CV_HAAR_SCALE_IMAGE)
```

Fig -4 Face Detection

This will give a list of objects defining where OpenCV has found what looks like a face. Something to keep in mind is that using machine learning, so they are not 100 per cent correct.

Depending on the quality of the images being processed, you will need to change the parameters of the 'detectMultiScale()' function to match your situation.

The scaleFactor() tries to account for the fact that the subject in the image may be closer or Farther away than those in training the classifier.

3. SYSTEM DESIGN-

For the system design, the design can be represented using the Use-Case Diagram and Flow Chart Diagram

3.1. Use case diagram –

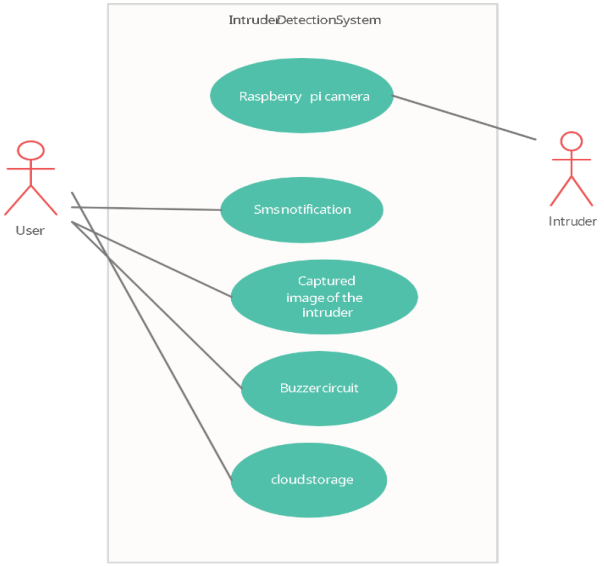

Fig -5: IDS Case Diagram

According to the use-case illustration above, the intruder activates the PIR motion sensor, which is then followed by the USB Camera, which takes a picture of the intruder. Meanwhile, if the system identifies an intruder, the user will be notified by SMS and email. Aside from that, the user may view the live video feed on their mobile devices and access the Dropbox cloud storage, which keeps all of the acquired images[3]. Furthermore, the user will have access to the alarm box, which when activated will allow the user to sound the buzzer to inform anyone around.

3.2. Flow chart-

The intruder detection system is initially initiated and configured, as shown in the flow chart diagram above.

Following that, the sensor detects motion. When motion is detected, the facial recognition system iS activated, and a picture of the intruder is acquired. The system assesses not if the internet is available after capturing image. available, and if it is, it transmits the image of the intruder to the user along with an alert message, and the buzzer is turned on or off based on the user's response.

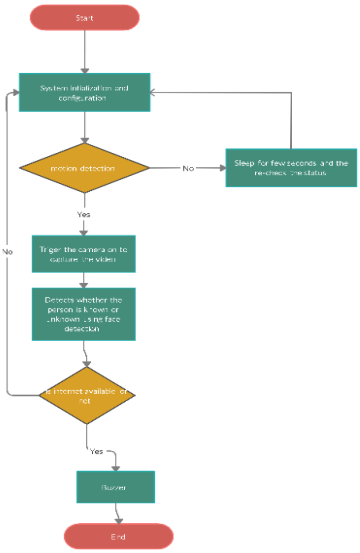

Fig -6: Efficient Working Flowchart

4. SYSTEM ARCHITECTURE

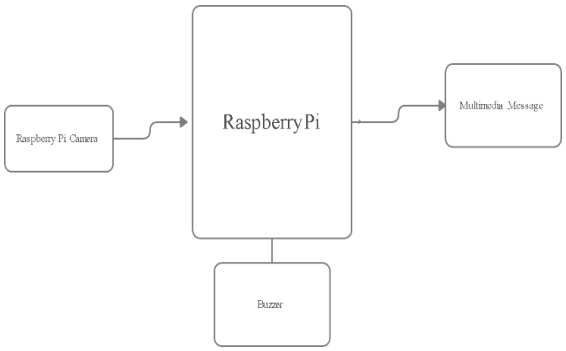

Fig -7: Architecture

5. TESTING AND COMPARISION

Five homeowners and five non-homeowners were evaluated in morning conditions..

5.1. Latency Testing

When the system is switched off, the calculating operation begins and continues until the magnet triggers and the door swings and closes. During latency testing, the time it takes the system to execute a facial reading is assessed.. The test was repeated 20 times, with a reading time of 5.90 seconds on average for homeowners and non-homeowners.

5.1.1. Face recognition stage-

a. Detection of known face –

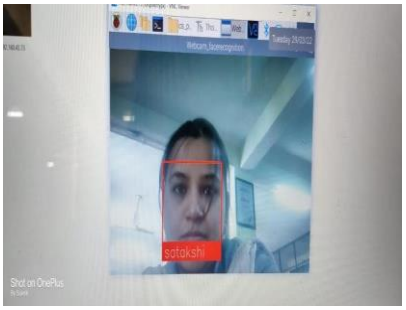

Fig -8: Screenshots

b. Detection of unknown face –

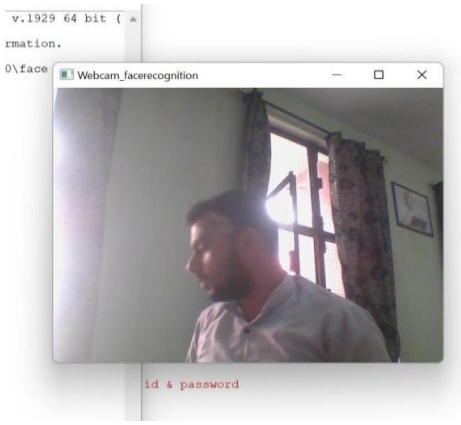

Fig -9:Screenshots

5.2. Sending the mail of unknown face-

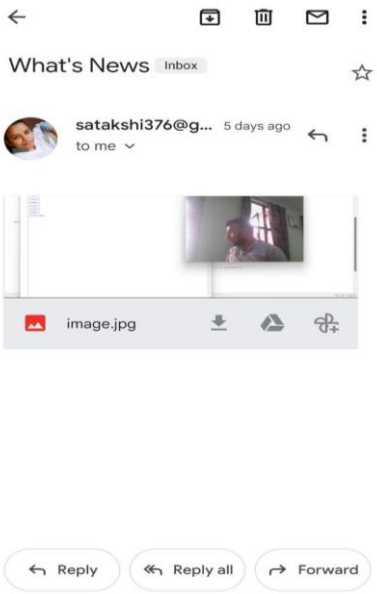

Fig -10:Screenshots

6. UI design

It comprises of the three major components-

6.1. Home page

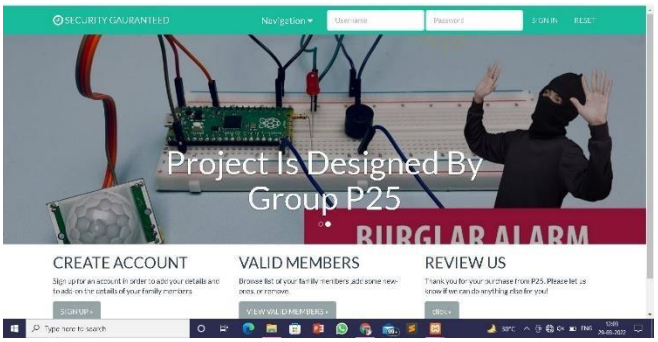

Fig -11

6.2. Login page –

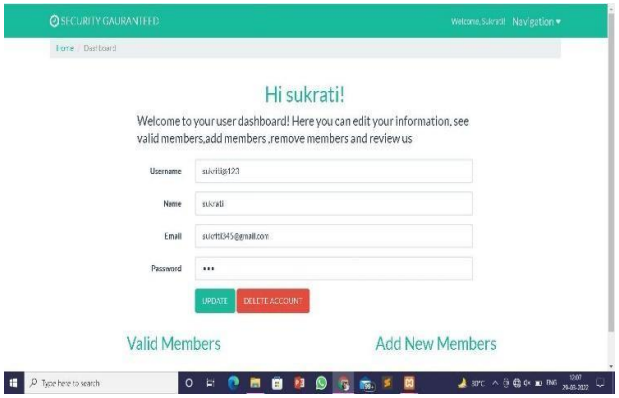

Fig -12

6.3 Uploading images

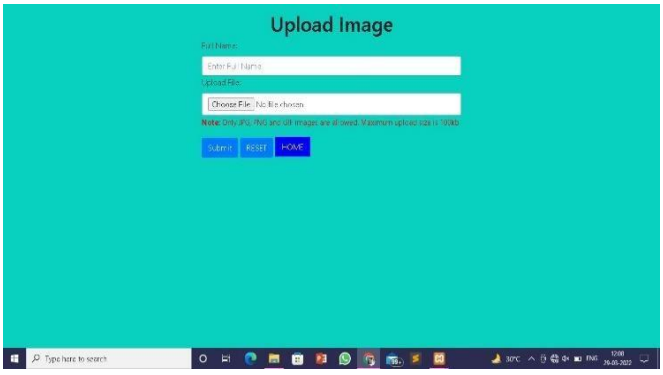

Fig -13

6.4. Database-

In this project we have created a database on phpMyAdmin for storing the image data of the valid members –

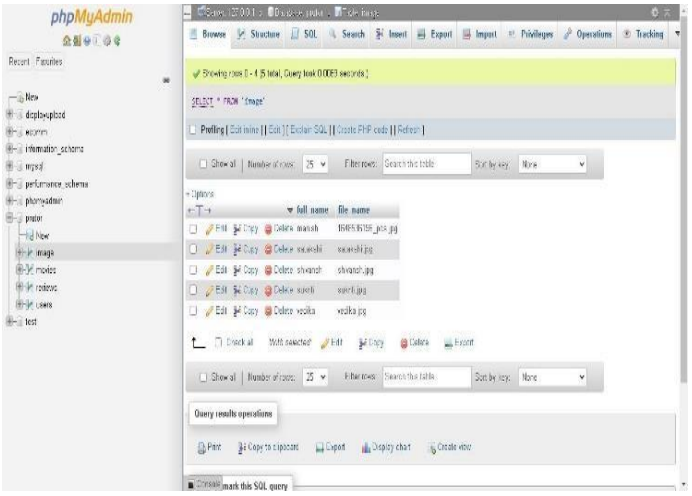

Fig -14:Database of IDS

7. Future scope-

To refresh your memory, intrusion detection systems (IDS) identify when someone or anything tries to breach a system or resource. A buzzer and multimedia message, as well as behavior analysis, are used to detect abnormal people. However, with future development, an alert box can be combined with an intrusion detection system, allowing the user to trigger the buzzer independently after receiving multimedia messages via registered mail.

8. CONCLUSION

After putting firewall technology at the network perimeter, IDS are becoming a key component for many enterprises.External and internal users can both be protected by IDS.Where traffic does not get via the firewall at all, this is an attack vector for attackers.The following considerations, on the other hand, must be kept in mind at all times.An IDS implementation will fail if all of these points are missing.A highly secure network requires more than a firewall.

1. 4. Human action is required: The assault must be investigated by a security administrator or network management at least once. It is identified and reported, with the goal of determining how it occurred, correcting the problem, and taking the required steps to avoid such assaults from occurring in the future.

8. REFERENCES

[1] Research paper by Engineering Research Councilof Canada and Dalhousie University Electronic Commerce Executive Committee.

[2] Chun-Liang Hsu, Sheng-Yuan Yang, Wei-Bin Wu,'Constructing Intelligent Home Security System Design with Combining Phone-Net and Bluetooth Mechanism', IEEEInternational Conference on Machine Learning and Cybernetics, Boading,pp.3316-3323,2009.

[3] S. Kanagamalliga, S. Vasuki, A. Vishnu Priya, V. Viji,'A Zigbee and Embedded based Security Monitoring and Control System', InternationalJournal of Information Science and Techniques(IJIST),Vol.4, No.3,pp.173-178, 2014.