IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Challenges And Opportunities Of Artificial Intelligence In Security Areas

Vinod Kumar Gupta
Research Scholar, Computer Science, Ambikapur, Chhattisgarh, India

ABSTRACT: -Intelligent Home Security System using Artificial Intelligence is the project undertaken to replace traditional means of security with modern IOT and A.I. based systems. Some commercial products based on image recognition are readily available, but such single security level systems can be easily breached. To overcome these drawbacks, we have implemented an A.I. based 2 level security system that can be easily scaled and can be packed with more features without loss in performance.
.

KEYWORDS: Artificial Intelligence, Machine Learning, Tensorflow, Image Recognition, Voice Recognition, Spectrogram, IOT, MQTT.

1. INTRODUCTION

There are currently 7.6 billion people on Earth, 3.7 billion are connected to the internet; almost 50% of that connected population lives in Asia, 24% of whom reside in India for which the number comes up to 440 million. Investment in digitisation and urbanisation and friendly regulatory policies hold key to ensuring that India continues to advance on its path of socioeconomic progress. The market potential of all things IOT in India alone is predicted to be $9 billion by 2020. India is one of the key countries poised for largescale implementation of IOT projects - not only to be able to set new standards but also as a key geography to anticipate the emergence of a new humanism embracing people and devices.[A.I. has become a thing of magic now a days and almost every company wants to integrate a part of it in their project. A.I. gives an edge to the devices that traditional hard-coded logic can't compete with. With each passing day, overlap between IOT devices and A.I. is increasing. The combination of both, one serving as a tool for data acquisition and deployment while the later acting as a tool for computation. Applications of A.I. in IOT are endless and one of them is it use in home security. As majority of Indian homes still use traditional mechanical locks and tower bolts, home breaks are inevitable. Apprehending the culprit is sometimes impossible and important meetings are missed if no one's at home. To counter this, we developed our project by implementing a two-tier security system, which is server based, provides good enough accuracy and provide a lot of features for commercial use.. Artificial intelligence (AI) has gained a massive footprint in modern society's day-to-day existence. Many don't realize it, but AI is now a primary driving force for many things we currently enjoy and do. It is part of nearly everything we do, from the moment your alarm, placed across the room on top of a dresser, woke you in the morning and you reached for your phone to turn it off to the end of the day when you used your car's GPS to find the least-congested route from your office to your home.

It's a sobering realization that AI's integration into our lives is just starting. It's becoming more prominent in another area of our home life: home security.

Many homeowners are now choosing AI-powered home security systems that take conventional electronics like e-locks and CCTV networks to the next level.

What Makes an AI Home Security System Appealing?

AI and home security are a match made in heaven. Security is paramount for every household, and AI enhances its functionalities to be more agile, flexible and effective. An AI home security system also offers a high degree of personalization. One of the best things about investing in an AI smart home security is that you can customize and pick options that best suit your lifestyle and needs. Of course, the "intelligence" of the technology is another significant benefit because it makes home security SOPs easier to implement, for example, locking your front doors when leaving the house. It's also more convenient to use, for example, activating a door's smart feature to open when you have both hands full carrying groceries, carrying your sleeping child, etc.

Considering the present and predicted capabilities of AI and home security technology, what can we expect from innovators and manufacturers of modern home security systems moving forward?

2. RESEARCH OBJECTIVES

Home protection and family safety are the primary purposes of a home security system. While this includes detecting burglary, a security system also detects a number of other threats, including smoke, fire, carbon monoxide poisoning, and water damage. Whether you self-monitor or pay for professional monitoring, you can know if there's danger in your home, wherever you are. A professionally monitored security system will call emergency services for you if a smoke or flood sensor is activated, whether you are home, away, or asleep. It's worth noting that you have to buy the security company's equipment in order to get professional monitoring of smoke and water sensors, which is not included in standard packages and comes at an additional cost.

AI and home security are a match made in heaven. Security is paramount for every household, and AI enhances its functionalities to be more agile, flexible and effective.

An AI home security system also offers a high degree of personalization. One of the best things about investing in an AI smart home security is that you can customize and pick options that best suit your lifestyle and needs. Of course, the "intelligence" of the technology is another significant benefit because it makes home security SOPs easier to implement, for example, locking your front doors when leaving the house. It's also more convenient to use, for example, activating a door's smart feature to open when you have both hands full carrying groceries, carrying your sleeping child, etc.

THE PROS OF AI HOME SECURITY

With how quickly artificial intelligence can learn and interpret data, it's easy to see where security professionals see the upsides. AI does have the potential to make living spaces more secure for the people who occupy them.

1. Facial Recognition

This could be practical for both homeowners and apartment renters. Homeowners may have fewer people going in and out of where they live. This will make it easy for AI to tell if someone could be an intruder. By learning the occupants' faces, it can detect when someone trying to enter isn't them. From there, the AI can alert security providers and tell the attempted burglar to leave. In apartments, it may be even more helpful. While more people are living in a rented-out building, AI still has the ability to learn each face. It can be easier for an intruder to enter a building unnoticed by neighbors or standard cameras without machine learning. Artificial intelligence can eliminate this problem by recognizing everyone who lives there, making it safer for renters.

2. Routine Memorization

As the AI security system learns faces, it can also start to remember routines set by those who live there. If someone often comes home at a particular time, the system will learn that and note any discrepancies. By

linking a routine to a face, it can tell who usually arrives and at what time. When someone is trying to get in with the wrong face at the wrong time, the AI can recognize this and send out alerts accordingly.

3. Geofencing

Geofencing creates a virtual boundary. It allows artificial intelligence to recognize the area it should be protecting. Once someone crosses that boundary, the security system can analyze whether the occupant, an animal, or an intruder triggered it. It can then learn whether this is someone it should recognize or someone looking to break in. This can also set up awareness for any devices a person might own. The geofence can detect when something using Wi-Fi, GPS, or cellular data enters or exits the perimeter. If a thief enters the area with a cellphone or removes connected devices from the home, authorities can know the thief's identity and what they stole.

3. PROPOSED SYSTEM (METHODOLOGY)

As home security is the issue of this paper, we went with a two-tier security approach with image identification being one and voice identification being second. The system that we designed is a server-client model, where a Raspberry-Pi and a NodeMCU are clients and an Acer laptop being a server. The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote teaching of basic computer science in schools and in developing countries. The Raspberry Pi 3 used is this project is a Raspberry Pi 3 Model B+ which hosts a Broadcom BCM2837B0 SOC which has 4x Cortex-A53 cores and runs on 1.4GHz. It also has a 10/100 Mbit/s Ethernet, 802.11 b/g/n/ac dual band 2.4/5 GHz wireless, Bluetooth 4.2BLE.[7] Raspberry Pi is responsible for acquiring data from the subject and transmit the data through TCP sockets to the server. NodeMCU is an open source IoT platform which includes firmware which runs on ESP8266 Wi-Fi SoC from Espressif Systems and the hardware is based on the ESP-12 module.Due to cost restraint and low speed internet the decision of running a "server" on the laptop was made. The server is a laptop which is connected to the same home Wi-Fi router to which the Raspberry Pi and the NodeMCU is connected. To make the system completely wireless, the data communication between the server and the Raspberry Pi is done through TCP Sockets and the communication between the server and the NodeMCU is done through an IoT protocol called MQTT. MQTT stands for Message Queuing Telemetry Transport and is an ISO standard publish-subscribe-based messaging protocol. It works on top of the TCP/IP protocol. It was designed for connections with remote location where a "small code footprint" is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker. In our system, the publisher is the server, the client is a NodeMCU and the server is an open MQTT server provided my iot.eclipse.org. Whenever the subject is in proximity of the Raspberry-Pi, which is connected with a USB camera, the RPi take a bunch of photos and a voice sample of the subject saying the command "Open the door". Theses files are then sent to the server through TCP socket.

The IP address of the server connected to the home router is known to the RPi. After the files are transmitted, the socket communication is closed and the RPi is out of the loop. After the files are received, they are stored folder. The image file is read, resized and moved in the test folder. The wav file is read, and a spectrogram is created. A spectrogram is a graph of spectrum frequencies of a signal as it varies with time. The jpeg file of spectrogram is saved in the test folder. After saving both the files, the image recognition model tests those images and gives a confidence level which is compared against a threshold. Once the threshold is crossed, that means the both the images are of the authorized personality or administrator. After authentication, the server sends a MQTT message to the NodeMCU on a specific topic. After receiving the message, the NodeMCU operates the server to be moved downwards thus opening the tower lock. If the threshold is not crossed even by one confidence level, the condition holds false and the server sends an email alert with an image file attached and an SMS to the administrator. Both the RPi and the server are in infinite loop and the RPi is runs the python script at boot.

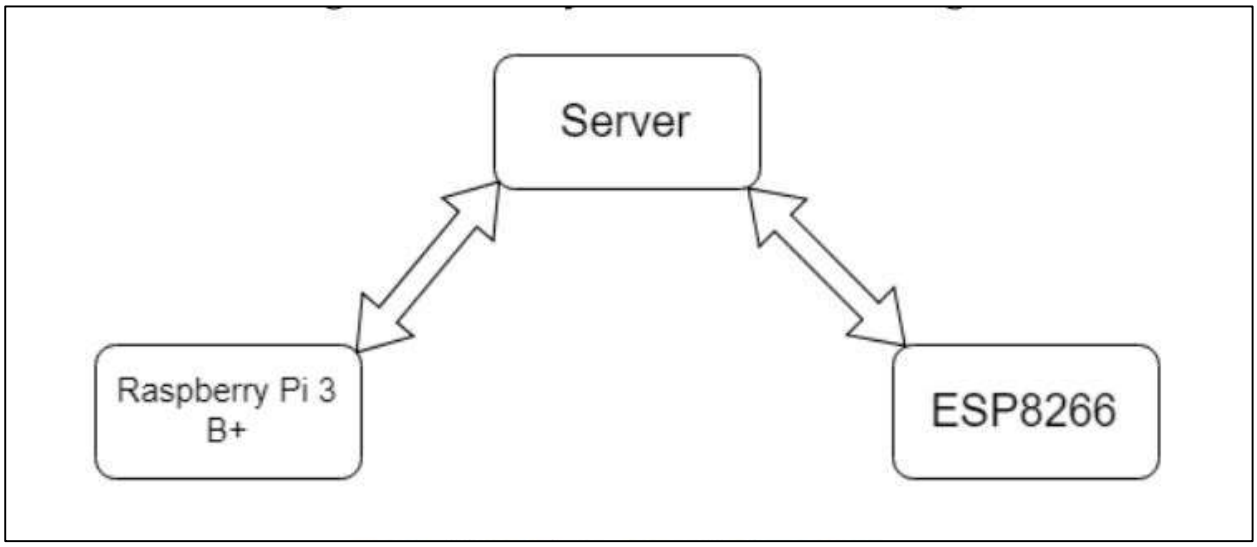

FIG 01 : SYSTEM BLOCK DIAGRAM

The RPi has Raspbian OS running on it with all the useful python modules installed. The images are captured using a USB camera instead of a PiCam so that both the voice and wav files can be captured while keeping the cost of materials low. The images are processed with the help of on python library called OpenCV. OpenCV (Open source computer vision) is a library of programming functions mainly aimed at real-time computer vision. The voice sample is of duration of 4 seconds and it is recorded using Pyaudio module. The image file is in .jpg format and the voice sample is in .wav format. Both these files are sent to the server through TCP sockets from where all the recognition and control operations take place. After recognition the server sends the appropriate commands to the NodeMCU.

FACE AND SPECTROGRAM RECOGNITION

Image Recognition, in the context of machine vision, is the ability of software to identify objects, places, people, writing and actions in images. In this project

we have used image recognition to

identify the face of the authorized personnel and the spectrogram of the voice of the same. To achieve this we used Google's Inception v3, which is a widely-used image recognition model that has been shown to attain greater than 78% accuracy on ImageNet dataset. It is based on the original paper: "Rethinking the Inception Architecture for Computer Vision" The model itself is made up of symmetric and asymmetric building blocks, including convolutions, average pooling, max pooling, concats, dropouts, and fully connected layers. Batchnorm is used extensively throughout the model and applied to activation inputs. Loss is computed via Softmax.

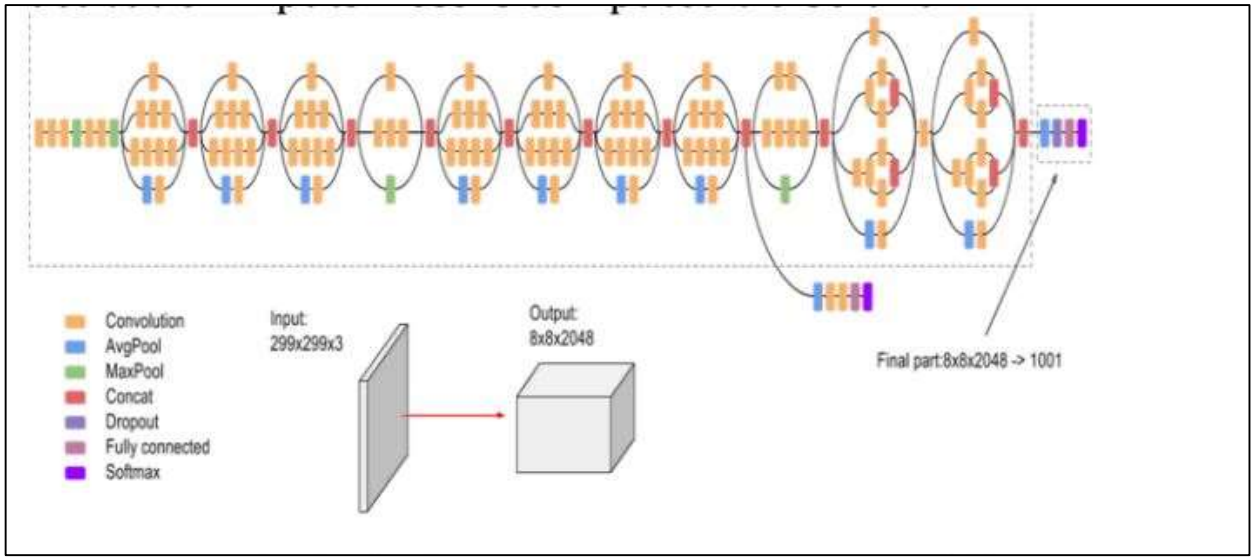

Fig. 02 : ARCHITECTURE OF INCEPTION MODEL

The model is trained on 20,000 images of the administrator and around 10,000 images of the second co-author of this paper. Just like images of faces, images of spectrogram of both, the administrator and the co-author were taken and labelled appropriately. OpenCV was used for acquisition and augmentation of the images. To spectrogram, a certain amount of noise was added while keeping the fidelity of audio intact. With this approach, the need for second model is eliminated and the code size is significantly reduced. But this results in longer augmentation and training sessions. Inception model is based on TensorFlow library from Google. The editors used for this project is eclipse with Pydev plugin, Idle and Arduino. The training of model took almost 6 hours to complete and augmentation took almost 1 hour.

4. RESULTS AND EVALUATION

1] Data Acquisition:

Fig-03: Acquired Admin Faces

2] Training of images:

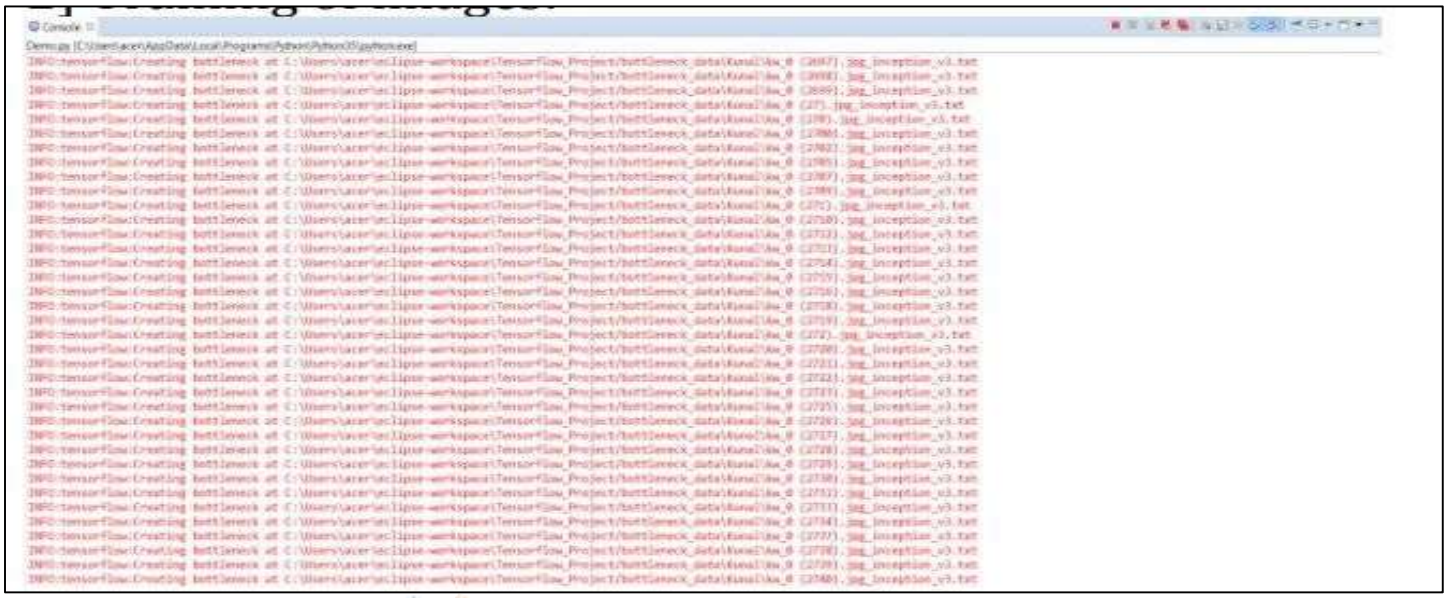

Fig-04: Training

3] Completion of training

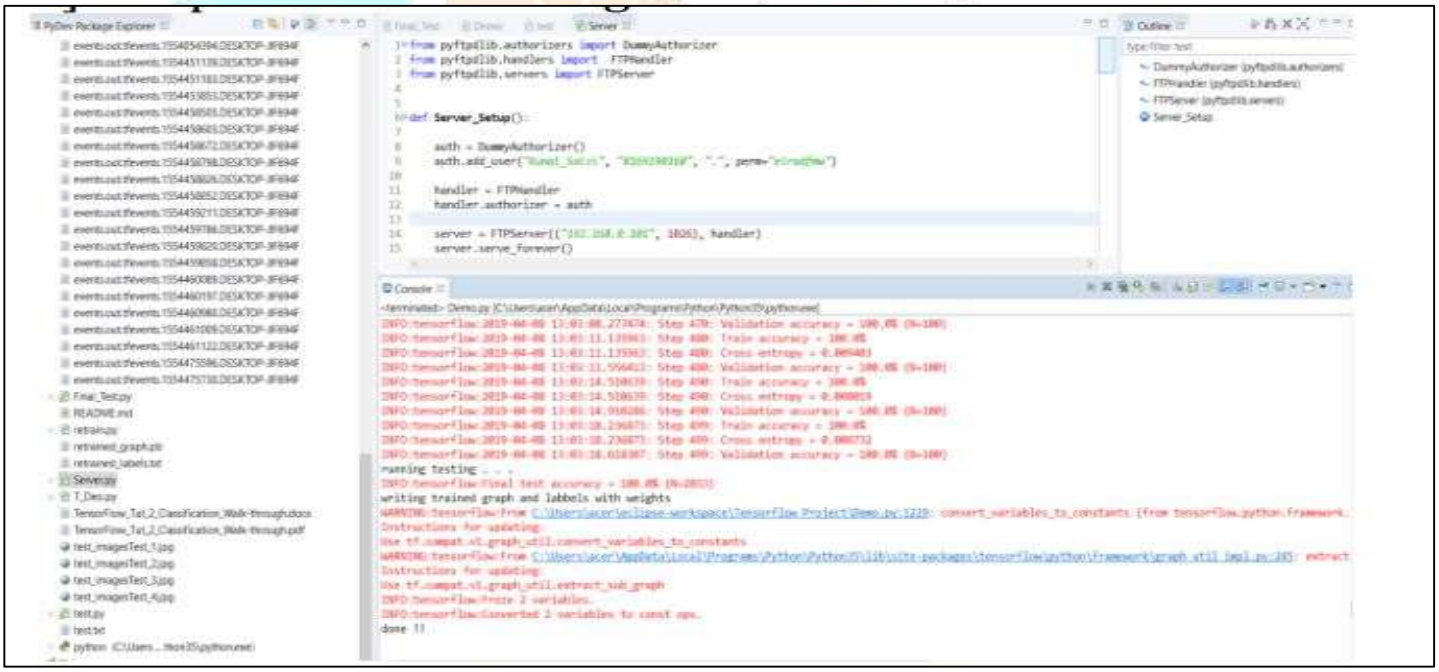

Fig-05: After training is done

4] Image Recognition Output

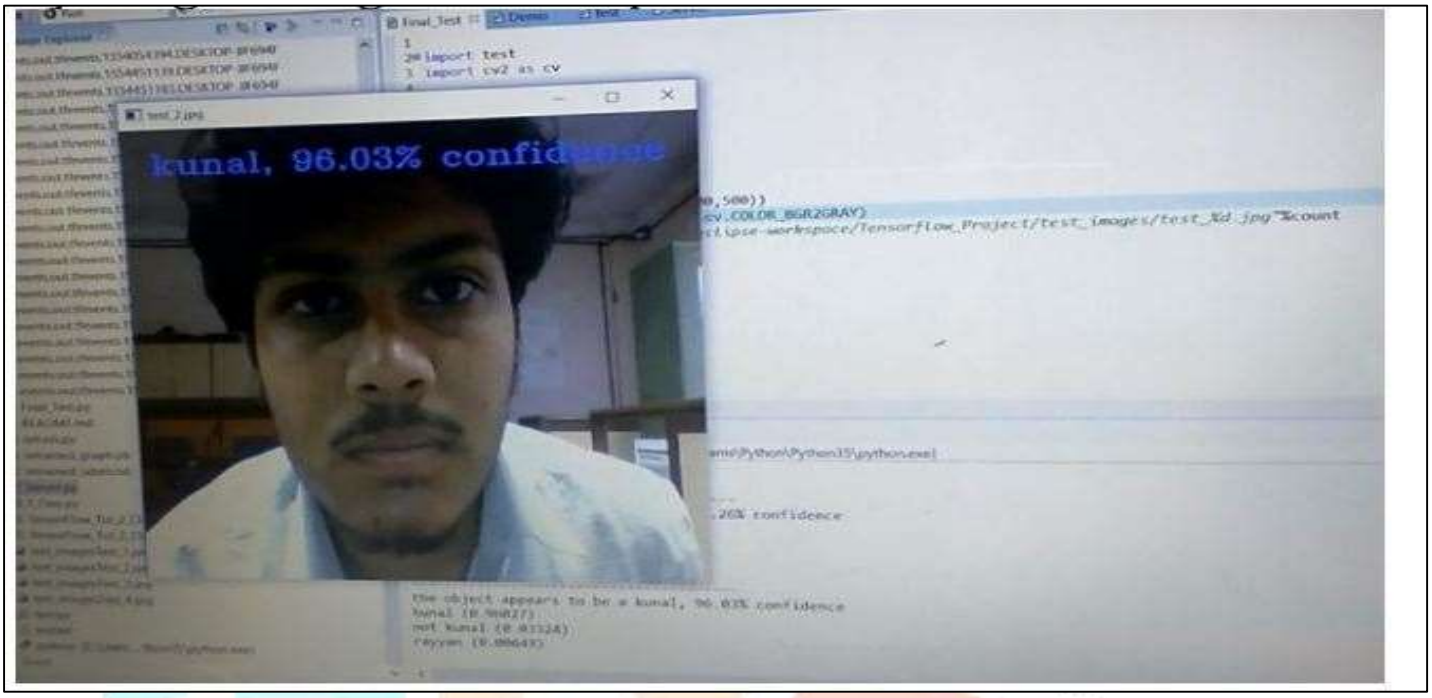

Fig 06 : Output

6] Email Received when the threshold is not crossed

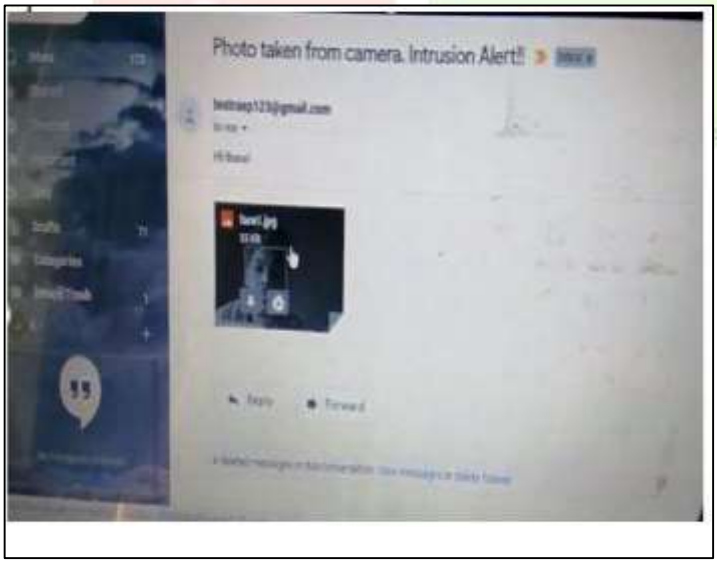

Fig-07: Email alert from server

7] SMS Received

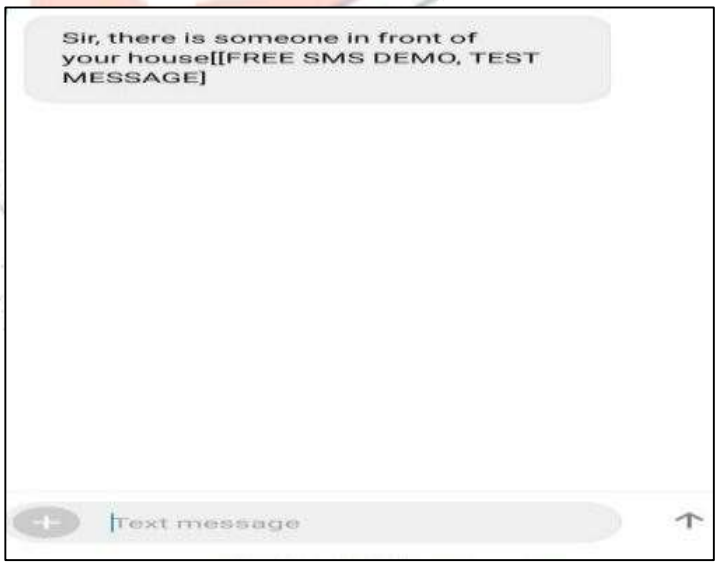

Fig-08: SMS from server

6. CONCLUSION AND FUTURE WORK

The scope of the project was to implement principles of A.I. and IoT in the security sector. We were able to implement our face and voice recognition system efficiently and with low bill of materials. The code can be more refined, and more features can be added in order to make it into

a full-fledged product for commercial use. Instead of an ESP8266 SoC, a Bluetooth enabled ESP32 can be used in order to add Bluetooth support so that the admin can still enter the house even when there is a power outage.

Home security system is a solution to problems like theft, instruction, fire, energy conservation etc. The Raspberry Pi is a great platform for building highly capable, embedded systems. This makes it possible for users to rest assured that their belongings are secure. Now a day's people are not aware about the importance of energy conservation. So in our project we are implementing a system for energy conservation by the use of PIR sensor. So this will save the electricity. The end product will have a simplistic design making it easy for users to interact with. The project is aimed at developing the security of Home against Intruders, and THEFT.

In this system we found some mechanism, techniques, methods like face recognition, voice recognition, door lock, spectrum methods etc.

7. ACKNOWLEDGMENT

The IoT, (IInternet Of Things) with its Inter-connectivity capability, has many advantages to technology as a whole but also security. In the near future, your home security system could have either locally or in the cloud a database with friends, family or potential offenders and persona non grata, and by using facial recognition technologies, can, depending on the gravity of the situation, either silently notify you in a low priority breach, alert you in a medium security breach, or go full metal jacket alerting everyone from you to police and security companies with who you have contracts.

Today, home security is fairly straightforward. If you live in a home that has an "alarm" you've got a bevy of motion sensors dotted around your house, a central keypad by your front door with a standard keypad to disarm it and a box on the front of your house that says "look at me, I'm protecting something valuable inside".

With the steady march of connected devices invading the home, and a number of companies looking to improve how we secure it, the future of home security is going to change drastically in the next couple of years, whether that is remotely controlling our lighting, seeing inside our house, or merely having sensors on our doors and windows detecting movement.

"Nothing concerns us more than the fear of someone breaking into our own home, yet very few homeowners heed the warnings until it's too late," explains Kris Hogg, chairman of CEDIA, the Custom Electronic Design and Installation Association. "A lot of the time monitored alarm systems can be integrated with the very latest hi-tech lighting and automation facilities in order to provide even greater levels of security."

Those systems include integrating the alarm system with an intelligent lighting system, such as the Lutron Homeworks system, so all the lights in your property will automatically switch on or flash incessantly when an intruder is detected, or setting your lights to randomly come on and off while you are on holiday to fool would-be burglars.

8. REFERENCES

[1]Jiahong Su Et.and Al.[2023] 'Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence in education', Computers and Education: Artificial Intelligence 4 (2023) 100118

[2]Dimitrios I. Tselentis [2023] 'Artificial Intelligence (AI) Literacy in Early Childhood Education: The Challenges and Opportunities', Computers and Education: Artificial Intelligence 4 (2023) 100124

[3]Thomas K.F. Chiu Et. And Al.[2023] ' The usefulness of artificial intelligence for safety assessment of different transport modes', Accident Analysis and Prevention 186 (2023) 107034

[4]Sajid Nazir Et. And Al.[2023] 'Survey of explainable artificial intelligence techniques for biomedical imaging with deep neural networks', Computers in Biology and Medicine 156 (2023) 106668

[5]M. Chen, C. Claramunt, A. Çöltekin, Et. Al.[2022]. 'Artificial intelligence and visual analytics in geographical space and cyberspace: Research opportunities and challenges', S0012-8252(23)00127-7

[6]Philipp M. Sieberg Et.and Al[2023] 'Challenges and potentials in the classification of wear mechanisms by artificial intelligence', Wear 522 (2023) 204725

[7]Justin Y.Y. Lee, Yanhao Miao, Ricky L.T. Chau , Mark Hernandez, Patrick K.H. Lee[2022] 'Artificial intelligence-based prediction of indoor bioaerosol concentrations from indoor air quality sensor data', Environment International 174 (2023) 107900

[8]Victor Partel , Lucas Costa Et. And Al. [2021] 'Smart tree crop sprayer utilizing sensor fusion and artificial intelligence', Computers and Electronics in Agriculture 191 (2021) 106556

[9]J AM ACAD DERMATOL Et. And Al. [2022] 'Artificial intelligence and imaging: Opportunities in cardio-oncology', American Heart Journal Plus: Cardiology Research and Practice 15 (2022) 100126

[10]Nidhi Madan Et. And Al.[2022] ' Application of big data and artificial intelligence in epidemic surveillance and containment', Intelligent Medicine 3 (2023) 36–43

[11]Zengtao Jiao Et. And Al. [2023] 'TRASTUZUMAB CARDIOTOXICITY SURVEILLANCE BY ARTIFICIAL INTELLIGENCE-AUGMENTED ELECTROCARDIOGRAPHY IN A MULTI SITE STUDY', Presentation Number: 1308-097

[12]Zachi Itzhak Attia, Suraj Kapa, Peter Noseworthy, Meir Tabi, Samuel Asirvatham Et. And Al.[2020] 'HOME CARDIAC SURVEILLANCE WITH ARTIFICIAL INTELLIGENCE DIGITAL PATIENT MONITORING DURING TREATMENT WITH PERTUZUMAB, TRASTUZUMAB AND HYALURONIDASE-ZZXF FOR HER2- POSITIVE BREAST CANCER (HARRIET): STUDY DESIGN AND RATIONALE', NCT04395508,