

IOT Based Face Recognition and Motion Sensing Security System

Submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering
degree in Electronics and Communication Engineering

By

Aaron John K (37130002)
Jerin Samuel Alanraj J (37130169)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC | 12B Status by UGC | Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL – 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC | 12B Status by UGC | Approved by AICTE

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **Mr. Aaron John K (37130002), Jerin Samuel Alanraj J (37130169)** who carried out the project entitled **IOT Based Face Recognition and Motion Sensing Security System** under my supervision from November 2020 to March 2021.

Internal Guide

Dr. T. VINO, B.E., M.E., Ph.D.

Head of the Department

Dr. T. Ravi M.E., Ph.D.

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

We **J. JERIN SAMUEL ALANRAJ (37130169)** and **K. AARON JOHN (37130002)** hereby declare that the Project Report entitled IOT BASED FACE RECOGNITION AND MOTION SENSING SECURITY SYSTEM done by us under the guidance of Dr. T. Vino M.E., Ph.D., at Sathyabama Institute of Science and Technology is submitted in partial fulfilment of the requirements for the award Bachelor of Engineering degree in ELECTRONICS AND COMMUNICATION ENGINEERING.

DATE:

PLACE:

JERIN SAMUEL ALANRAJ J (37130169)

AARON JOHN K (37130002)

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to Dr. N.M. Nanditha M.E., Ph.D., **Dean, School of Electrical and Electronics** and Dr. T. Ravi M.E., Ph.D., **Head of the Department of Electronics and Communication Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide Dr. **T. VINO, B.E., M.E., Ph.D.** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The Internet of Things (IoT) combines the idea of technology providing value to our daily lives. One major category in which technology benefits us is the concept of security and privacy. Smartphones can act as a security alert system as the Smartphone is the most widely-used smart device. Recently, the use of Artificial Intelligence (AI) - integrated smart IoT devices has significantly increased as well. In this paper, we developed a smart IoT security system for the smart-home, in which, a Raspberry Pi acts as a security system which to record videos and capture images. Also, a Passive Infrared (PIR) Motion Sensor is used to detect motion. We propose to use motion sensor data and the images gathered to predict a security threat using a face recognition classification technique along with our developed algorithm. The system has the capability to notify the user in case of any emergency by sound a loud alarm and capturing the image of the intruder and sending an email. In this project, we utilize two codes, GUI.py and Security.py. The GUI.py code is run in the Desktop/laptop since the Raspberry Pi doesn't have enough processing power to train the model. OpenCV and Python compiler are installed in the desktop. OpenCV is the huge open-source library for the computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's systems.

The system depends on the PIR Motion Sensor to detect motion, and run code based upon high signal. The high signal from the PIR Motion Sensor will run Security.py code from the Raspberry Pi 3 B+ board's operating system. The Security.py code will allow the USB Webcam to record video and capture images.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No.
	ABSTRACT	v
1	INTRODUCTION	1
	1.1 Basics of IOT	1
	1.1.1 History of IOT	2
	1.1.2 Applications of IOT	3
	1.1.2.1 Consumer Application	3
	1.1.2.2 Organizational Applications	5
	1.1.2.3 Industrial Applications	8
	1.1.3 Enabling Technologies for IOT	11
	1.1.3.1 Addressability	11
	1.1.3.2 Application Layer	12
	1.1.3.3 Short-range Wireless	12
	1.1.3.4 Medium-range Wireless	13
	1.1.3.5 Long-range Wireless	13
	1.1.3.6 Wired	13
	1.1.4 IOT Adoption Barriers	13
	1.2 What is Face/Facial Recognition System?	16

	1.2.1 History of Face/Facial Recognition	17
	1.2.2 Techniques for Face Recognition	20
	1.2.3 Applications	23
2	LITERATURE SURVEY	26
3	AIM AND SCOPE OF THE WORK	27
	3.1 Aim	27
	3.2 Scope of the Work	27
4	SYSTEM ARCHITECTURE	28
	4.1 Hardware	28
	4.2 Software	30
	4.3 Algorithm Used	34
	4.3.1 GUI.py Algorithm	34
	4.3.2 Security.py Algorithm	34
	4.4 Performance Analysis	35
	4.4.1 PIR Motion Sensor	35
	4.4.2 USB Webcam	35
5	RESULT	38
6	CONCLUSION AND REFERENCES	39
	6.1 Conclusion	39

LIST OF FIGURES

FIGURE No.	TITLE	PAGE No.
1.1	IOT	2
1.2	Smart Home	4
1.3	IOT used for Medical and Healthcare	7
1.4	IOT used for Manufacturing	9
1.5	IOT in Agriculture	10
1.6	IOT in the Maritime Industry	11
4.1	Raspberry Pi 3B+	29
4.2	HP Class 10 16GB SDHC	29
4.3	PIR Motion Sensor	29
4.4	USB Webcam	30
4.5	5V Buzzer	30
4.6	Breadboard and Jumper Wires	30
4.7	Output immediately after running GUI.py	31
4.8	Capturing Images Using GUI	31
4.9	Capture Images Converted into Grey Scale	31
4.10	GUI displaying the “Images Saved” message	31
4.11	GUI displaying the “Images Trained” message after pressing the Train images button	31
4.12	Screenshot of the Video Feed	32

FIGURE No.	TITLE	PAGE No.
4.13	Email notification from Raspberry Pi	32
4.14	The picture of the intruder.	32
4.15	The picture of the intruder attached in the email	33
5.1	Image of a known person	38
5.2	Image of the Intruder	38

CHAPTER 1

INTRODUCTION

A smart-home consists of a computer, Smartphone, and other smart sensors or actuators that are equipped with an IoT connection. Internet of Things (IoT) involves interrelated computing devices transferring data over a network without requiring interaction between the computer and the user. This creates a platform for a security system by allowing the user to feel safe at home and feel safe leaving the home knowing that the user will be alerted when someone comes near the home. One key category in which technology benefits us is the concept of security and safety. With the fact that most of our population today carries technology around on their person as compared to the earlier years of smartphones makes it more appealing that smartphones can act as a security alert system. Time and evidence are two factors necessary for proactive crime prevention. The recent increase in availability and use of smart IoT devices and the ubiquity of smartphones allows the ability of individuals to monitor house/office/store security conditions on a continuous basis. This project's major impact for society is to establish a viable and easily available approach to the community by gathering data and identifying risky behaviors in the smart-home environment. In this research, we developed a system (smart IoT system) that allows the user to detect unauthenticated access in the smart-home.

1.1 Basics of IOT

The **Internet of things (IoT)** describes the network of physical objects - “things” or objects—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet

Things have evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems.^[1] Traditional fields of embedded systems, wireless sensor networks, control

systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT can also be used in healthcare systems.

There are a number of serious concerns about dangers in the growth of IoT, especially in the areas of privacy and security, and consequently industry and governmental moves to address these concerns have begun including the development of international standards.

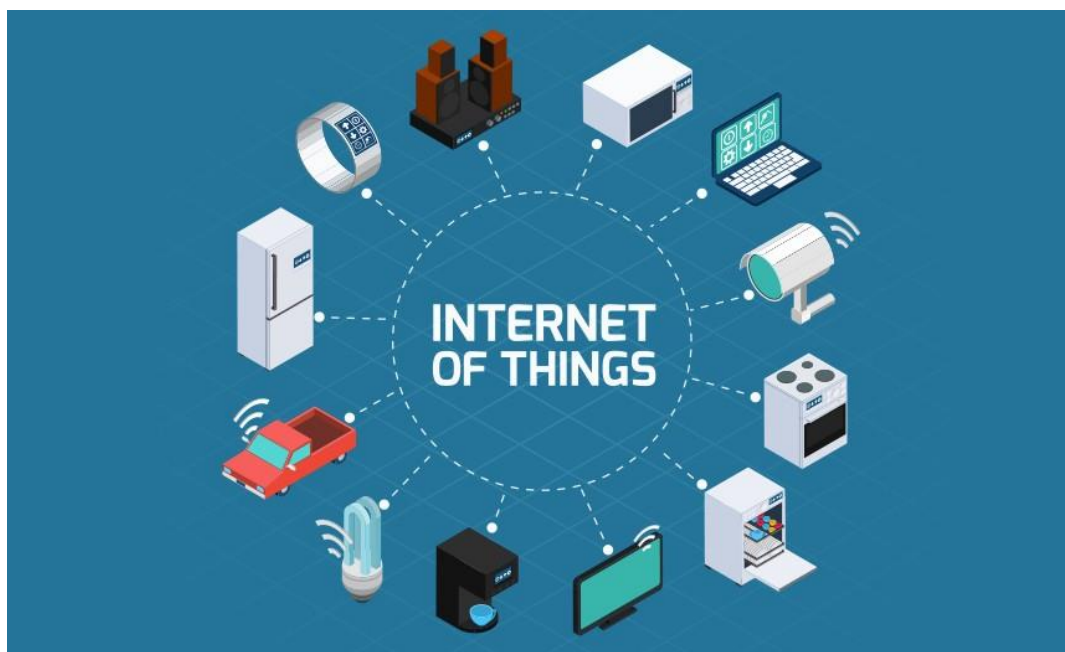


Fig 1.1: IOT

1.1.1 History of IOT

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly

loaded drinks were cold or not. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IOT. In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.

The term "Internet of things" was coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet *for* things". At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.

1.1.2 Applications of IOT

The extensive set of applications for IoT devices is often divided into consumer, commercial, industrial, and infrastructure spaces.

1.1.2.1 Consumer applications

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

Smart home

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems and camera systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off or by making the residents in the home aware of usage. A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's Home Kit, manufacturers can have their home products and accessories controlled by an application in iOS devices such as the iPhone and the Apple Watch. This could be a dedicated app or iOS native applications such as Siri. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub. In addition to the commercial systems, there are many non-proprietary, open-source ecosystems; including Home Assistant, OpenHAB and Domoticz.



Fig 1.2: Smart Home

Elder care

One key application of a smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.

1.1.2.2 Organizational applications

Medical and healthcare

The **Internet of Medical Things (IoMT)** is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. The IoMT has been referenced as "Smart Healthcare", as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than \$300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." Moreover, the use of

mobile devices to support medical follow-up led to the creation of 'm-health', used analyzed health statistics."

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and-throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wireless powered disposable sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.

As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar, to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information. Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behavior. This can lead to more accurate underwriting and new pricing models.

The application of the IoT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible

through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.



Fig 1.3: IOT used for Medical and Healthcare

Transportation

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e., the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance.

V2X communications

In vehicular communication systems, vehicle-to-everything communication (V2X) consists of three main components: vehicle to vehicle communication (V2V), vehicle to infrastructure communication (V2I) and vehicle to pedestrian communications (V2P). V2X is the first step to autonomous driving and connected road infrastructure.

Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature:

- The integration of the Internet with building energy management systems in order to create energy efficient and IOT-driven "smart buildings".
- The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors.
- The integration of smart devices in the built environment and how they might be used in future applications.

1.1.2.3 Industrial applications

Also known as IIoT, industrial IoT devices acquire and analyze data from connected equipment, operational technology (OT), locations and people. Combined with operational technology (OT) monitoring devices, IIoT helps regulate and monitor industrial systems. Also, the same implementation can be carried out for automated record updates of asset placement in industrial storage units as the size of the assets can vary from a small screw till the whole motor spare part and misplacement of such assets can cause a percentile loss of manpower time and money.

Manufacturing

The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control allow IoT to be used for industrial applications and smart manufacturing. IoT intelligent systems enable rapid manufacturing and optimization of new products, and rapid response to product demands.

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IIoT. IoT can also be applied to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Industrial management systems can be integrated with smart grids, enabling energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by networked sensors.



Fig 1.4: IIoT used for Manufacturing

Agriculture

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs.

In August 2018, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related

to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide. The specific computer programs used in the process fall under the Azure Machine Learning and the Azure IoT Hub platforms.

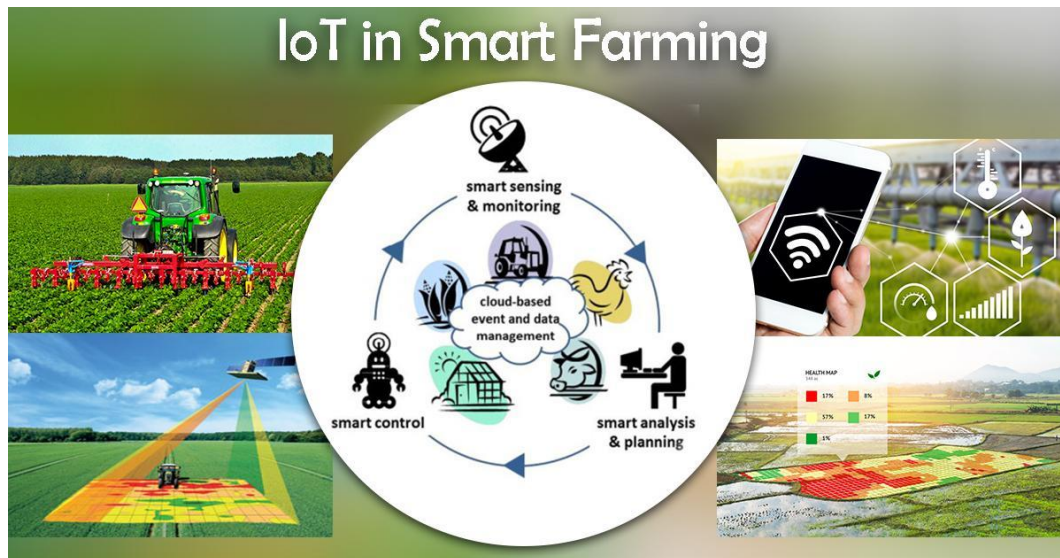


Fig 1.5: IOT in Agriculture

Maritime

IoT devices are in use monitoring the environments and systems of boats and yachts. Many pleasure boats are left unattended for days in summer, and months in winter so such devices provide valuable early alert of boat flooding, fire, and deep discharge of batteries. The use of global internet data networks such as Sigfox, combined with long life batteries, and microelectronics allows the engine rooms, bilge, and batteries to be constantly monitored and reported to a connected Android & Apple application for example.

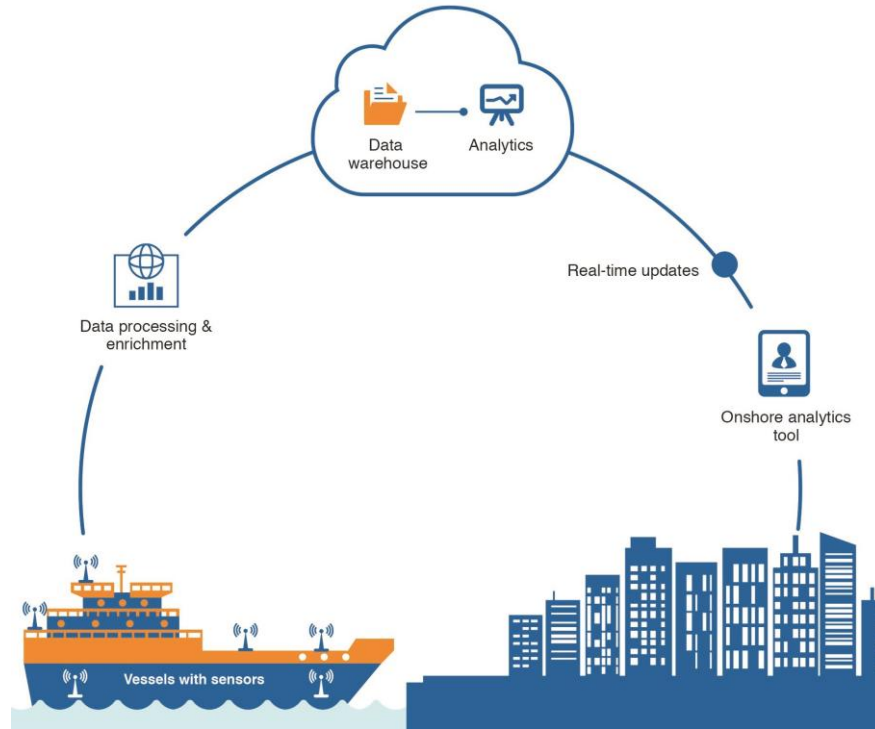


Fig 1.6: IOT in the Maritime Industry

1.1.3 Enabling Technologies for IOT

There are many technologies that enable the IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill:

1.1.3.1 Addressability

The original idea of the Auto-ID Center is based on RFID-tags and distinct identification through the Electronic Product Code. This has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners. Integration with the Internet implies that devices will use an IP address as a distinct identifier. Due to

the limited address space of IPv4 (which allows for 4.3 billion different addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.

1.1.3.2 Application Layer

- ADRC defines an application layer protocol and supporting framework for implementing IoT applications.

1.1.3.3 Short-range wireless

- Bluetooth mesh networking – Specification providing a mesh networking variant to Bluetooth low energy (BLE) with increased number of nodes and standardized application layer (Models).
- Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth.
- Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range.
- Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
- Wi-Fi – Technology for local area networking based on the IEEE 802.11 standards, where devices may communicate through a shared access point or directly between individual devices.
- ZigBee – Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.
- Z-Wave – Wireless communications protocol used primarily for home automation and security applications

1.1.3.4 Medium-range wireless

- LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.
- 5G - 5G wireless networks can be used to achieve the high communication requirements of the IoT and connect a large number of IoT devices, even when they are on the move.

1.1.3.5 Long-range wireless

- Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless, RPMA.
- Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

1.1.3.6 Wired

- Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.
- Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as HomePlug or G.hn utilize PLC for networking IoT devices.

1.1.4 IOT Adoption Barriers

Lack of interoperability and unclear value propositions

Despite a shared belief in the potential of the IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Mike Farley argued

in Forbes that while IoT solutions appeal to early adopters, they either lack interoperability or a clear use case for end-users. A study by Ericsson regarding the adoption of IoT among Danish companies suggests that many struggles "to pinpoint exactly where the value of IoT lies for them".

Privacy and security concerns

As for IoT, information about a user's daily routine is collected so that the "things" around the user can cooperate to provide better services that fulfill personal preference. When the collected information which describes a user in detail travels through multiple hops in a network, due to a diverse integration of services, devices and network, the information stored on a device is vulnerable to privacy violation by compromising nodes existing in an IoT network.

For example, on 21 October 2016, a multiple distributed denial of service (DDoS) attacks systems operated by domain name system provider Dyn, which caused the inaccessibility of several websites, such as GitHub, Twitter, and others. This attack is executed through a botnet consisting of a large number of IoT devices including IP cameras, gateways, and even baby monitors.

Fundamentally there are 4 security objectives that the IOT system requires: (1) data confidentiality: unauthorized parties cannot have access to the transmitted and stored data. (2) data integrity: intentional and unintentional corruption of transmitted and stored data must be detected. (3) non-repudiation: the sender cannot deny having sent a given message. (4) data availability: the transmitted and stored data should be available to authorized parties even with the denial-of-service (DOS) attacks.

Information privacy regulations also require organizations to practice "reasonable security". **California's SB-327 Information privacy: connected devices.** "would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information

contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified." As each organization's environment is unique, it can prove challenging to demonstrate what "reasonable security" is and what potential risks could be involved for the business. **Oregon's HB 2395** also "Requires *person that manufactures, sells or offers to sell connected device*] **manufacturer** to equip connected device with reasonable security features that protect **connected device and** information that connected device *collects, contains, stores or transmits*] **stores** from access, destruction, modification, use or disclosure that consumer does not authorize."

Traditional Governance Structure

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies' traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence." Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity." This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements." Some of these companies risk being 'kodaked' – "Kodak was a market leader until digital disruption eclipsed film photography with digital photos" – failing to "see the disruptive forces affecting their industry" and "to truly embrace the new business models the disruptive change opens up." Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online" but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business."

Business planning and project management

According to 2018 study, 70–75% of IoT deployments were stuck in the pilot or prototype stage, unable to reach scale due in part to a lack of business planning.

Studies on IoT literature and projects show a disproportionate prominence of technology in the IoT projects, which are often driven by technological interventions rather than business model innovation.

Even though scientists, engineers, and managers across the world are continuously working to create and exploit the benefits of IoT products, there are some flaws in the governance, management and implementation of such projects. Despite tremendous forward momentum in the field of information and other underlying technologies, IoT still remains a complex area and the problem of how IoT projects are managed still needs to be addressed. IoT projects must be run differently than simple and traditional IT, manufacturing or construction projects. Because IoT projects have longer project timelines, a lack of skilled resources and several security/legal issues, there is a need for new and specifically designed project processes. The following management techniques should improve the success rate of IoT projects:

- A separate research and development phase
- A Proof-of-Concept/Prototype before the actual project begins
- Project managers with interdisciplinary technical knowledge
- Universally defined business and technical jargon

1.2 Basics of Face/Facial Recognition System

A **facial recognition system** is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

While initially a form of computer application, facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such

as robotics. Because computerized facial recognition involves the measurement of a human's physiological characteristics facial recognition systems are categorized as biometrics. Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless process. Facial recognition systems have been deployed in advanced human-computer interaction, video surveillance and automatic indexing of images. They are also used widely by law enforcement agencies.

1.2.1 History of Face/Facial Recognition

Automated facial recognition was pioneered in the 1960s. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson worked on using the computer to recognize human faces. Their early facial recognition project was dubbed "man-machine" because the coordinates of the facial features in a photograph had to be established by a human before they could be used by the computer for recognition. On a graphics tablet a human had to pinpoint the coordinates of facial features such as the pupil centers, the inside and outside corner of eyes, and the widows' peak in the hairline. The coordinates were used to calculate 20 distances, including the width of the mouth and of the eyes. A human could process about 40 pictures an hour in this manner and so build a database of the computed distances. A computer would then automatically compare the distances for each photograph, calculate the difference between the distances and return the closed records as a possible match.

In 1970, Takeo Kanade publicly demonstrated a face matching system that located anatomical features such as the chin and calculated the distance ratio between facial features without human intervention. Later tests revealed that the system could not always reliably identify facial features. Nonetheless, interest in the subject grew and in 1977 Kanade published the first detailed book on facial recognition technology.

In 1993, the Defense Advanced Research Project Agency (DARPA) and the Army Research Laboratory (ARL) established the face recognition technology

program FERET to develop "automatic face recognition capabilities" that could be employed in a productive real life environment "to assist security, intelligence, and law enforcement personnel in the performance of their duties." Face recognition systems that had been trialed in research labs were evaluated and the FERET tests found that while the performance of existing automated facial recognition systems varied, a handful of existing methods could viably be used to recognize faces in still images taken in a controlled environment. The FERET tests spawned three US companies that sold automated facial recognition systems. Vision Corporation and Miros Inc were both founded in 1994, by researchers who used the results of the FERET tests as a selling point. Visage Technology was established by an identification card defense contractor in 1996 to commercially exploit the rights to the facial recognition algorithm developed by Alex Pentland at MIT.

Following the 1993 FERET face recognition vendor test the Department of Motor Vehicles (DMV) offices in West Virginia and New Mexico were the first DMV offices to use automated facial recognition systems as a way to prevent and detect people obtaining multiple driving licenses under different names. Driver's licenses in the United States were at that point a commonly accepted form of photo identification. DMV offices across the United States were undergoing a technological upgrade and were in the process of establishing databases of digital ID photographs. This enabled DMV offices to deploy the facial recognition systems on the market to search photographs for new driving licenses against the existing DMV database. DMV offices became one of the first major markets for automated facial recognition technology and introduced US citizens to facial recognition as a standard method of identification. The increase of the US prison population in the 1990s prompted U.S. states to establish connected and automated identification systems that incorporated digital biometric databases, in some instances this included facial recognition. In 1999 Minnesota incorporated the facial recognition system FaceIT by Visionics into a mug shot booking system that allowed police, judges and court officers to track criminals across the state.

Until the 1990s facial recognition systems were developed primarily by using photographic portraits of human faces. Research on face recognition to reliably locate a face in an image that contains other objects gained traction in the early 1990s with the principle component analysis (PCA). The PCA method of face detection is also known as Eigenface and was developed by Matthew Turk and Alex Pentland. Turk and Pentland combined the conceptual approach of the Karhunen–Loève theorem and factor analysis, to develop a linear model. Eigenfaces are determined based on global and orthogonal features in human faces. A human face is calculated as a weighted combination of a number of Eigenfaces. Because few Eigenfaces were used to encode human faces of a given population, Turk and Pentland's PCA face detection method greatly reduced the amount of data that had to be processed to detect a face. Pentland in 1994 defined Eigenface features, including Eigen eyes, Eigen mouths and Eigen noses, to advance the use of PCA in facial recognition. In 1997 the PCA Eigenface method of face recognition was improved upon using linear discriminant analysis (LDA) to produce Fisherfaces. LDA Fisherfaces became dominantly used in PCA feature based face recognition. Eigen faces were also used for face reconstruction. In these approaches no global structure of the face is calculated which links the facial features or parts.

Purely feature based approaches to facial recognition were overtaken in the late 1990s by the Bochum system, which used Gabor filter to record the face features and computed a grid of the face structure to link the features.^[14] Christoph von der Malsburg and his research team at the University of Bochum developed Elastic Bunch Graph Matching in the mid 1990s to extract a face out of an image using skin segmentation. By 1997 the face detection method developed by Malsburg outperformed most other facial detection systems on the market. The so-called "Bochum system" of face detection was sold commercially on the market as ZN-Face to operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hairstyles and glasses—even sunglasses".

Real-time face detection in video footage became possible in 2001 with the Viola–Jones object detection framework for faces. Paul Viola and Michael Jones combined their face detection method with the Haar-like feature approach to object recognition in digital images to launch AdaBoost, the first real-time frontal-view face detector. By 2015 the Viola-Jones algorithm had been implemented using small low power detectors on handheld devices and embedded systems. Therefore, the Viola-Jones algorithm has not only broadened the practical application of face recognition systems but has also been used to support new features in user interfaces and teleconferencing.

1.2.2 Techniques for Face Recognition

While humans can recognize faces without much effort, facial recognition is a challenging pattern recognition problem in computing. Facial recognition systems attempt to identify a human face, which is three-dimensional and changes in appearance with lighting and facial expression, based on its two-dimensional image. To accomplish this computational task, facial recognition systems perform four steps. First face detection is used to segment the face from the image background. In the second step the segmented face image is aligned to account for face pose, image size and photographic properties, such as illumination and grayscale. The purpose of the alignment process is to enable the accurate localization of facial features in the third step, the facial feature extraction. Features such as eyes, nose and mouth are pinpointed and measured in the image to represent the face. The so established feature vector of the face is then, in the fourth step, matched against a database of faces.

Traditional

Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze

the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features.

Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches: geometric, which looks at distinguishing features, or photo-metric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. Some classify these algorithms into two broad categories: holistic and feature-based models. The former attempts to recognize the face in its entirety while the feature-based subdivide into components such as according to features and analyze each as well as its spatial location with respect to other features.

Popular recognition algorithms include principal component analysis using eigenfaces, linear discriminant analysis, elastic bunch graph matching using the Fisherface algorithm, the hidden Markov model, the multilinear subspace learning using tensor representation, and the neuronal motivated dynamic link matching.

Human identification at a distance (HID)

To enable human identification at a distance (HID) low-resolution images of faces are enhanced using face hallucination. In CCTV imagery faces are often very small. But because facial recognition algorithms that identify and plot facial features require high resolution images, resolution enhancement techniques have been developed to enable facial recognition systems to work with imagery that has been captured in environments with a high signal-to-noise ratio. Face hallucination algorithms that are applied to images prior to those images being submitted to the facial recognition system utilize example-based machine learning with pixel substitution or nearest neighbor distribution indexes that may also incorporate demographic and age related

facial characteristics. Use of face hallucination techniques improves the performance of high-resolution facial recognition algorithms and may be used to overcome the inherent limitations of super-resolution algorithms. Face hallucination techniques are also used to pre-treat imagery where faces are disguised. Here the disguise, such as sunglasses, is removed and the face hallucination algorithm is applied to the image. Such face hallucination algorithms need to be trained on similar face images with and without disguise. To fill in the area uncovered by removing the disguise, face hallucination algorithms need to correctly map the entire state of the face, which may be not possible due to the momentary facial expression captured in the low-resolution image.

3-dimensional recognition

Three-dimensional face recognition technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3D face recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. Three-dimensional data points from a face vastly improve the precision of face recognition. 3D-dimensional face recognition research is enabled by the development of sophisticated sensors that project structured light onto the face. 3D matching technique are sensitive to expressions, therefore researchers at Technion applied tools from metric geometry to treat expressions as isometries. A new method of capturing 3D images of faces uses three tracking cameras that point at different angles; one camera will be pointing at the front of the subject, second one to the side, and third one at an angle. All these cameras will work together so it can track a subject's face in real-time and be able to face detect and recognize.

Thermal Cameras

A different form of taking input data for face recognition is by using thermal cameras, by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or makeup. Unlike conventional

cameras, thermal cameras can capture facial imagery even in low-light and nighttime conditions without using a flash and exposing the position of the camera. However, the databases for face recognition are limited. Efforts to build databases of thermal face images date back to 2004. By 2016 several databases existed, including the IIITD-PSE and the Notre Dame thermal face database. Current thermal face recognition systems are not able to reliably detect a face in a thermal image that has been taken of an outdoor environment.

In 2018, researchers from the U.S. Army Research Laboratory (ARL) developed a technique that would allow them to match facial imagery obtained using a thermal camera with those in databases that were captured using a conventional camera. Known as a cross-spectrum synthesis method due to how it bridges facial recognition from two different imaging modalities, this method synthesizes a single image by analyzing multiple facial regions and details. It consists of a non-linear regression model that maps a specific thermal image into a corresponding visible facial image and an optimization issue that projects the latent projection back into the image space. ARL scientists have noted that the approach works by combining global information (i.e. features across the entire face) with local information (i.e. features regarding the eyes, nose, and mouth). According to performance tests conducted at ARL, the multi-region cross-spectrum synthesis model demonstrated a performance improvement of about 30% over baseline methods and about 5% over state-of-the-art methods.

1.2.3 Applications

Social media

Founded in 2013, Lookserly went on to raise money for its face modification app on Kickstarter. After successful crowdfunding, Lookserly launched in October 2014. The application allows video chat with others through a special filter for faces that modifies the look of users. Image augmenting applications already on the market, such as FaceTune and Perfect365, were limited to static images, whereas Lookserly

allowed augmented reality to live videos. In late 2015 SnapChat purchased Looksery, which would then become its landmark lenses function. Snapchat filter applications use face detection technology and on the basis of the facial features identified in an image a 3D mesh mask is layered over the face.

DeepFace is a deep learning facial recognition system created by a research group at Facebook. It identifies human faces in digital images. It employs a nine-layer neural net with over 120 million connection weights, and was trained on four million images uploaded by Facebook users. The system is said to be 97% accurate, compared to 85% for the FBI's Next Generation Identification system.

Face ID

Apple introduced Face ID on the flagship iPhone X as a biometric authentication successor to the Touch ID, a fingerprint based system. Face ID has a facial recognition sensor that consists of two parts: a "Romeo" module that projects more than 30,000 infrared dots onto the user's face, and a "Juliet" module that reads the pattern. The pattern is sent to a local "Secure Enclave" in the device's central processing unit (CPU) to confirm a match with the phone owner's face.

The facial pattern is not accessible by Apple. The system will not work with eyes closed, in an effort to prevent unauthorized access. The technology learns from changes in a user's appearance, and therefore works with hats, scarves, glasses, and many sunglasses, beard and makeup. It also works in the dark. This is done by using a "Flood Illuminator", which is a dedicated infrared flash that throws out invisible infrared light onto the user's face to properly read the 30,000 facial points.

ID verification

The emerging use of facial recognition is in the use of ID verification services. Many companies and others are working in the market now to provide these services to banks, ICOs, and other e-businesses. Face recognition has been leveraged as a form of biometric authentication for various computing platforms and devices; Android 4.0 "Ice Cream Sandwich" added facial recognition using a smartphone's front camera as

a means of unlocking devices, while Microsoft introduced face recognition login to its Xbox 360 video game console through its Kinect accessory, as well as Windows 10 via its "Windows Hello" platform (which requires an infrared-illuminated camera). In 2017 Apple's iPhone X smartphone introduced facial recognition to the product line with its "Face ID" platform, which uses an infrared illumination system.

CHAPTER 2

LITERATURE SURVEY

AUTHORS	JOURNAL NAME AND YEAR	METHODOLOGY
AKM Jahangir Majumder, Joshua Aaron Izaguirre	A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition (2020)	Local Binary Patterns Histogram
Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo	Face Recognition Security System (2013)	Skin Texture Analysis
Dwi Ana Ratna Wati	Design of Face Detection and Recognition System for Smart Home Security Application (2017)	PCA Algorithm
Jonathan, Adhi Kusnadi, Daud Julio	Security System With 3 Dimensional Face Recognition Using PCA Method and Neural Networks Algorithm	Back propagation Neural Networks Algorithm and Eigen faces

CHAPTER 3

AIM AND SCOPE OF THE PRESENT INVESTIGATION

3.1 Aim

To create an IOT Based Face Recognition and Motion Sensing Security System Using Raspberry Pi 3 Model B+.

3.2 Scope of the Present Investigation

Our primary focus is on threat detection which will help to predict a security threat due to any unauthorized access in the smart-home environment. To address the issue of threat detection, the aim of this research is to determine a security threat using smartphones. Data collected from our GUI .py code helps us train our model and to identify a security vulnerability in the Smart-home.

Our proposed approach combines computation with hardware designed to utilize motion detection using machine learning to authenticate the motion detected by the PIR Motion Sensor to avoid false triggers on authenticated people in the area.

CHAPTER 4

SYSTEM ARCHITECTURE

The strength of our proposed IoT security system is dependent on built-in wireless communication technologies to provide a low-cost solution with maximum freedom of wireless capability. In addition, we have used a USB webcam and a PIR Motion Sensor that are user-friendly and easy to install.

In this project, we utilize two codes, GUI.py and Security.py. The GUI.py code is run in the Desktop/laptop since the Raspberry Pi doesn't have enough processing power to train the model. OpenCV and Python compiler are installed in the desktop. OpenCV is the huge open-source library for the computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's systems. By using it, one can process images and videos to identify objects, faces, or even handwriting of a human.

The GUI.py code is used to capture 25 images of the person we don't want to recognize as an intruder and to train the model for that person. The captured images are converted into grayscale and stored in the TrainingImages folder.

Each aspect of the hardware is adjusted and modified using the Security.py code to ensure an accurate and reliable IoT security system. The system depends on the PIR Motion Sensor to detect motion, send a high signal through the general-purpose input/output (GPIO), and run code based upon that high signal. The high signal from the PIR Motion Sensor will run Security.py code from the Raspberry Pi 3 B+ board's operating system, Raspbian, which is stored on the micro SDHC card. The Security.py code will allow the USB Webcam to record video and capture images. The captured image of the intruder will be sent to the user through an email.

4.1 Hardware

All hardware components used in our developed security system are shown in Figure 1. Raspberry Pi 3B+, USB Webcam, a Passive Infrared (PIR) Motion Sensor that detects motion based upon infrared light radiating from objects in its field of view, a HP 16GB Class 10 Micro SDHC card to store the RasbianOS and images, a 5V

buzzer which is used to notify the user when an intruder is detected and a breadboard with jumper cables for making the connections.

The USB Webcam supports multiple different resolutions and frame rates. The wide-angle focus lens remains in a fixed position and provides a 90-degree wide angle, which is important for a camera module with a fixed angle.

The PIR Motion Sensor can be set to detect motion from 5 meters to 7 meters. These are set to 7 meters. The sensors detect infrared light in a 100-degree cone extending from the sensor to the set range. The delay time, or how long the motion sensor will output high after motion is detected can be set from 0.3 seconds to 300 seconds. When the repeatable trigger is off, the output will automatically change from a high to a low level when the sensor output is high, and the delay time is over. When the repeatable trigger is on, it will keep the output high all the time when the sensor is retriggered repeatedly and will output low when idle and not triggered.

The HP class 10 16GB micro SDHC Card is specifically designed for video monitoring cameras. It can read up to 100MBs per second and write up to 10MBs per second.



Fig: 4.1 Raspberry Pi 3B+

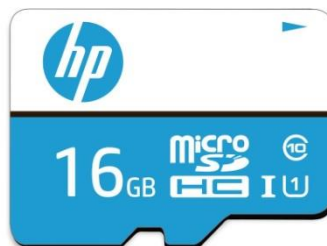


Fig 4.2: HP Class 10 16GB SDHC



Fig: 4.3 PIR Motion Sensor



Fig: 4.4 USB Webcam



Fig: 4.5 5V Buzzer



Fig: 4.6 Bread Board and Jumper Wires

4.2 Software

We have developed the software part of the project using the python language. A secure shell (SSH) program called VNC viewer is used to communicate to the Raspberry Pi 3B+ device without having to connect them to a monitor or keyboard and mouse. To utilize the USB Webcam for video capture and image processing, OpenCV was used. OpenCV is the huge open-source library for the computer vision, machine learning, and image processing. To utilize notifications for notifying the user about an intruder simple mail transfer protocol (SMTP) library module is used. SMTP is a protocol, which handles sending e-mail and routing e-mail between mail servers. Python provides `smtplib` module, which defines an SMTP client session object that can be used to send mail to any Internet machine (here a Raspberry Pi 3B+) with an SMTP or ESMTP listener daemon.

To collect the data of the person we don't want to consider intruders we used the GUI.py code. The GUI.py code has two functions. One to capture 25 images of the person we don't want to recognize as an intruder and the other to train the model for that person. The captured images are converted into grayscale and stored in the TrainingImages folder. We'll be giving every resident a unique ID & name in the GUI. Once this is done, we just updated the ResidentDetails.csv and Trainer.yml file in the raspberry pi. The outputs of the GUI.py code are shown in Figure 2.

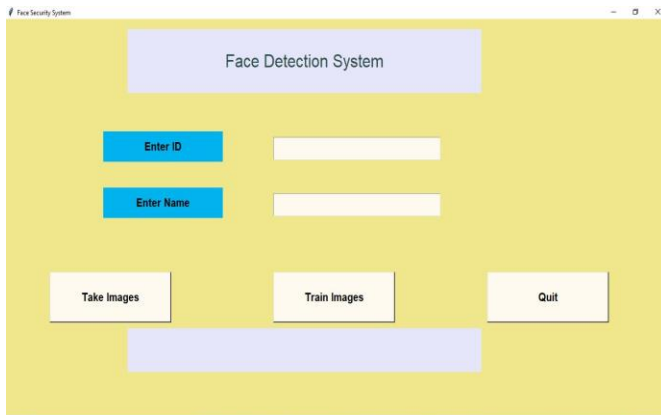


Fig: 4.7 Output immediately after running GUI.py.

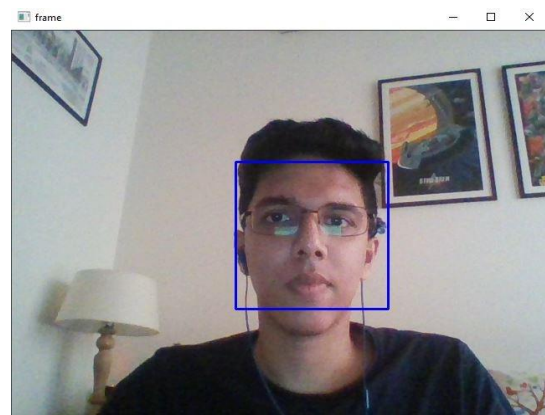


Fig: 4.8 Capturing

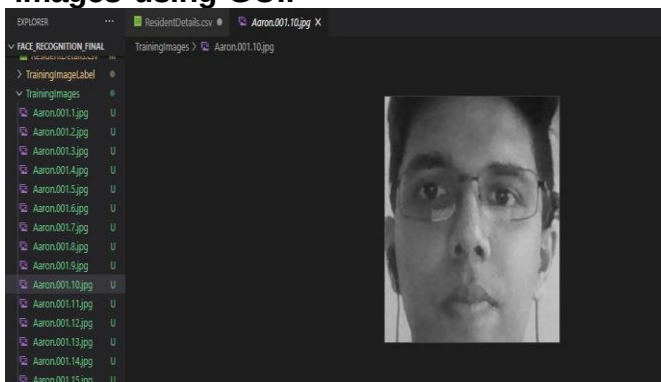


Fig 4.9: Captured image converted into grayscale.

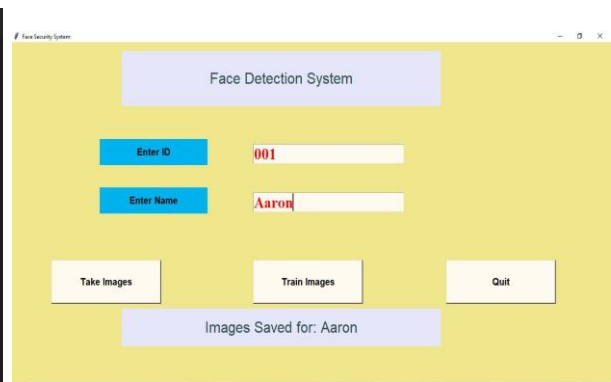


Fig: 4.10 GUI displaying the “Images Saved” message.

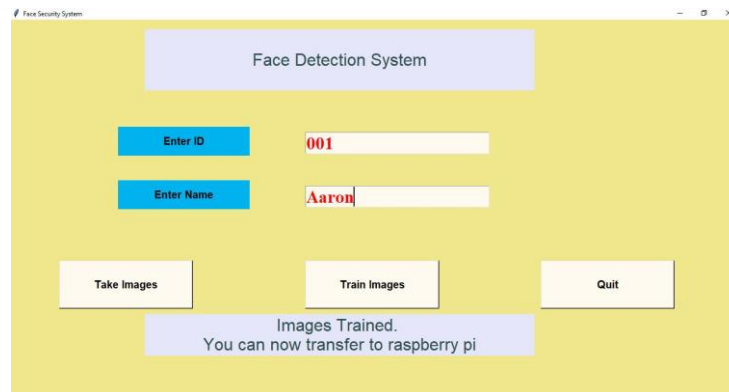


Fig: 4.11 GUI displaying the “Images Trained” message after pressing the Train images button.

On the Raspberry Pi we will run the Security.py code. When a motion is detected a video feed will start. According to our Security.py code, the buzzer will be rung when

an unknown person is detected and the notification email will include a standard motion alert with a picture of the unknown person or intruder. The screenshots of the video feed and notification email are shown in Figure 3 and Figure 4.

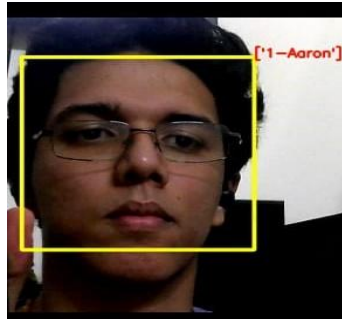


Fig 4.12: Screenshot of the video feed

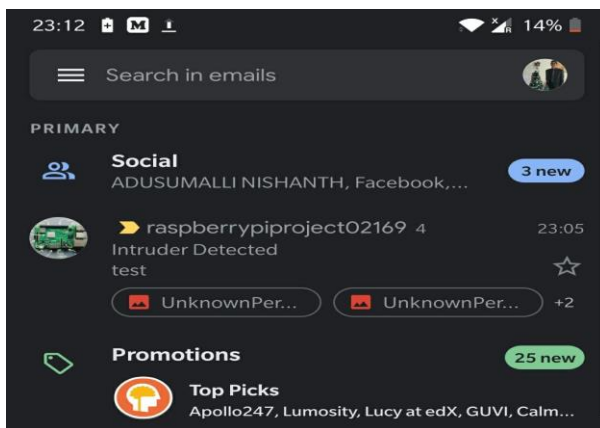


Fig: 4.13 Email notification from Raspberry Pi intruder.

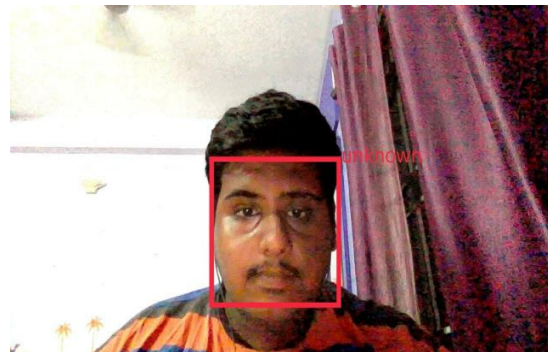


Fig: 4.14 The picture of the intruder.

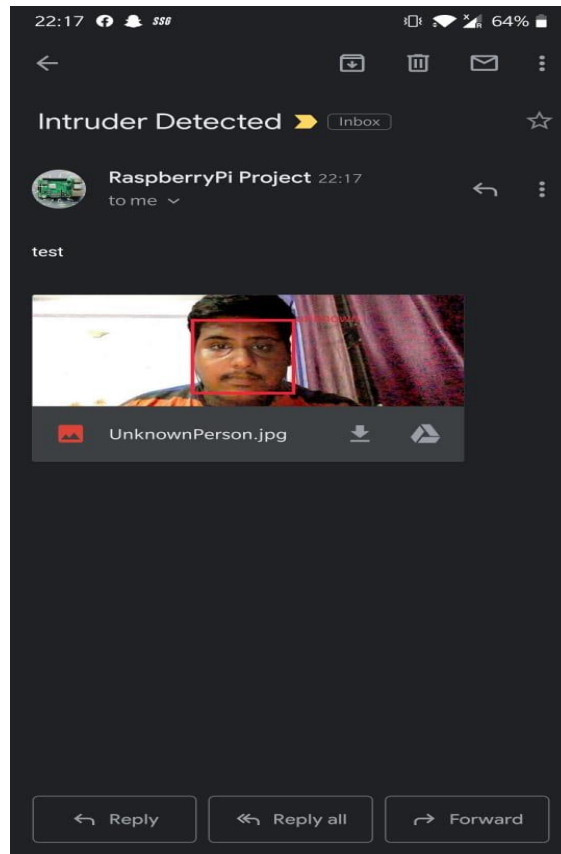


Fig: 4.15 The picture of the intruder attached in the email.

4.3 ALGORITHM USED

4.3.1 GUI.py Algorithm:

- i. Capture 10 images in the dataset folder.
- ii. Create empty Face (name) and ID list.
- iii. Loop through all the image paths and load the IDs and the images.
- iv. Load the image and converting it to gray scale.
- v. Get the ID from the image.
- vi. Extract the face from the training image sample.
- vii. If the face is detected then append that in the list as well as the ID.
- viii. GUI created.

4.3.2 Security.py Algorithm:

- i. Import all libraries needed.
- ii. Initiate the buzzer and motion sensor.
- iii. Calculate seconds of the video.
- iv. Use OpenCV's face recognition module.
- v. Read the CSV file which has the details of the residents.
- vi. Turning on the camera.
- vii. Convert feed to grayscale.
- viii. Predict the similarity.
- ix. Getting the name and ID for that specific resident.
- x. Display name and ID and put a rectangle around the face.
- xi. If person is not known give them "Unknown ID".
- xii. Capture their image.
- xiii. Send the mail about the intruder.
- xiv. Turn on LED and Buzzer and turn them off after 3 seconds.

4.4 PERFORMANCE ANALYSIS

Data collection consists of utilizing both PIR Motion Sensor and USB Webcam in different testing scenarios. Test cases for the PIR Motion Sensor involve checking whether a motion alert occurs when a person walks past the sensor within its range. We can't test output signals with the USB Webcam like we can with the PIR Motion Sensor, but we can use the camera to test our authentication access feature. Using the images from the camera module, we can use machine learning to train our IoT security device using the Local Binary Patterns Histograms (LBPH) algorithm with authorized people. If our device detects motion from unauthorized people, the user will be notified with image via email.

4.4.1 *PIR Motion Sensor*

Motion is detected via the PIR Motion Sensor's signal. When the GPIO input of the signal is low, no motion is detected at that current moment. On the other end, when the GPIO input of the signal is high, motion is currently being detected. We set the sensitivity of each PIR Motion Sensor to the medium range, which is about 5 meters. This was done to deter false positives. We set the time delay of each PIR Motion Sensor to the lowest setting, 0.3 seconds, so the sensor will check if motion is being detected or not as much as possible. We also set the repeatable trigger for each PIR Motion Sensor, which means that the GPIO input will remain high until the motion isn't detected anymore.

4.4.2 USB Webcam

When motion is detected, it is important that clear and accurate recordings and captures are made available to the user. While the USB Webcam doesn't detect motion itself, it will store images for the user based upon the PIR Motion Sensor detecting motion. The images taken (using GUI.py code) from the USB Webcam will also be used for machine learning with the LBPH algorithm. The test cases for the camera involve testing the facial recognition feature. This was done by running the

Security.py script and allowing the program to use the USB Webcam and the OpenCV library to check whether the USB Webcam detected a face or not.

For this project we utilize one of the most popular algorithms for facial recognition, the Local Binary Patterns Histogram (LBPH) algorithm. This algorithm is based off the local binary pattern (LBP) operator, which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. Utilizing the LBP operator, we can use LBPH for a facial recognition feature by following steps:

Radius: Used to build the circular LBP and represents the radius around the central pixel. Neighbors: The quantitative value of sample points to build the circular LBP.

Grid X: The quantitative value of horizontal cells. Grid Y: The quantitative value of vertical cells. To train the algorithm, a dataset must be created with facial images of authenticated people in combination with an ID value. By applying the LBP operator, we create a new image, based up, on the original image, with highlighted facial characteristics. This is done using two of our parameters: radius and neighbors. To create this new image, the following steps of the LBP procedure will be done:

- Split a part of the image into a window of 3x3 pixels, which is equivalent to a 3x3 matrix.
- The central value of the matrix is taken to define the new values from the 8 neighbors.
- A new binary value is set for each neighbor of the central value.
- We set the binary value to 1 if the neighbor value is equal to or higher than the central value. The binary value is set to 0 if the neighbor value is lower than the central value.
- The matrix will contain only binary values. We will add each binary value from each neighboring position from the matrix into a new binary value.
- Once we have that new binary value, we convert it to a decimal value and set it to the central value of the matrix, which equates to a pixel from the original image.
- Now that we have our new image, we extract the histograms using the grid x and grid y parameters by dividing the image into multiple grids.

Each histogram will contain 256 positions representing pixel intensity. Each histogram will be added together to create a new, bigger histogram. This new histogram will represent the characteristics of the original image. The LBPH algorithm is trained at this point. Each final histogram created will represent each image. Using the input image captured from the USB Webcam, we create a final histogram for it and compare it to the final histograms in our database of authenticated people. The formula we use to compare the two final histograms is the Euclidean distance:

$$D = \sqrt{\sum_{i=1}^n (hist1_i - hist2_i)^2}$$

The algorithm output will be the ID from the image with the closest final histogram and the calculated distance. If the calculated distance is lower than the central value, the algorithm has successfully recognized the input image.

CHAPTER 5

RESULT

When there is movement and the system captures the image and then verifies the captured image with our trained algorithm and when the image does not match with our trained data then our developed project sends out a loud alarm and then sends the captured image of the intruder to the owner's email-id. If our algorithm recognizes the person then it shows the data stored in our database.



Fig: 5.1 Image of a known person

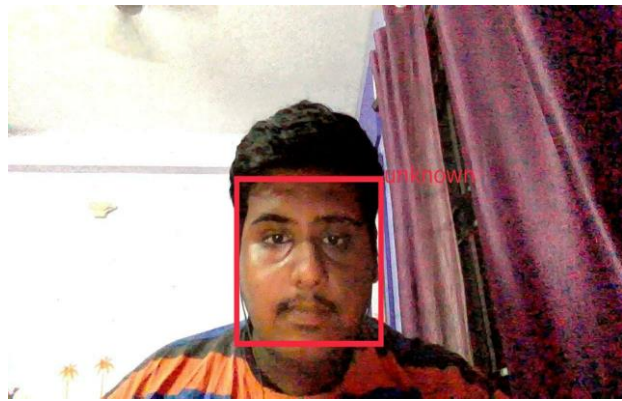


Fig: 5.2 Image of the Intruder

CHAPTER 6

CONCLUSION AND REFERENCES

6.1 Conclusion

In this project, we developed a motion detecting IoT security system that can alert the user and nearby neighbors by sounding the loud alarm in case of any emergency and send an email to the user's email address.

The results from tests are also presented to show that this approach provides a high degree of classification accuracy in detecting unauthenticated access in the smart-home.

6.2 References

- [1] AKM Jahangir Majumder, Joshua Aaron Izaguirre, "A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition," in Computer Vision (ICCV), 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC).
- [2] Amer Dergham, Michel Owayjan, Gerges Haber, Nidal Fakhri, "Face Recognition Security System", in International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2013) At: University of Bridgeport
- [3] Balakrishnan. R and D. Pavithra, "IoT based monitoring and control system for home automation", 2015 Global Conference on Communication Technologies (GCCT).
- [4] Chandra S. K. and U. C. Pati, "IoT based intrusion detection system using PIR sensor", 2017 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), 2017.
- [5] Poojitha .B, R. Rani and S. Lavanya, "IoT Based Home Security System Using Raspberry Pi with Email and Voice Alert", International Journals of Advanced Research in Computer Science and Software Engineering ISSN, 2018.
- [6] R. A. D. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application", 2017 2nd International

- conferences on Information Technology Information Systems and Electrical Engineering (ICITISEE), 2017.
- [7] A. Aftab et al., "LBPH based improved face recognition at low resolution", 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018.
 - [8] Z. XueMei and ChengBing Wei, "A real-time face recognition system based on the improved LBPH algorithm", 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP), 2017.
 - [9] S. L. Suma and S. Raga, "Real Time Face Recognition of Human Faces by using LBPH and Viola Jones Algorithm", International Journal of Scientific Research in Computer Science and Engineering, 2018.
 - [10] A. M. Jagtap et al., "A Study of LBPH Eigenface Fisherface and Haar-like features for Face recognition using OpenCV", 2019 International Conference on Intelligent Sustainable Systems (ICISS), 2019.
 - [11] P. Neha, S. Ambatkar and S. Kakde, "IoT based smart surveillance security system using raspberry Pi", 2017 International Conference on Communication and Signal Processing (ICCSP), 2017.
 - [12] S. Nico and W. Ridwan, "Design of Smart Home Security System using Object Recognition and PIR Sensor", *Procedia Computer Science*, vol. 135, 2018.
 - [13] D. Arun, L. Abirami, M. Gomathi, G. Manju and S. Siva Sakthi, "IoT Based Smart Home Security System", International Conference on Latest Innovations in Applied Science Engineering and Technology (ICLIASET 2017), March 2017.
 - [14] A. Dorothy, S. Beatrice, Britto Ramesh Kumar and J. Jerlin Sharmila, "IoT Based Home Security through Digital Image Processing Algorithms", 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017.
 - [15] M. Sahani, C. Nanda, A. K. Sahu and B. Pattnaik, "Web-based online embedded door access control and home security system based on face recognition", 2015 International Conference on Circuits Power and Computing Technologies [ICCPCT-2015], 2015.