

IOT Based Home Intruder Alerting System

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

By

IMMANUEL B (39130168)
JEBIN GERALD J (39130185)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS

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 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

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 **IMMANUEL B (39130168) and JEBIN GERALD J (39130185)** who carried out the project entitled " **IOT BASED HOME INTRUDER ALERTING SYSTEM** " under our supervision from November 2022 to April 2023.

Internal Guide

Dr. S.POORNAPUSHPAKALA, M.E., Ph.D.,

Head of the Department

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

Submitted for Viva voce Examination held on 27.04.2023

Internal Examiner

External Examiner

DECLARATION

We, **IMMANUEL B (39130168)** and **JEBIN GERALD J (39130185)** here by declare that the Project Report entitled " " **IOT BASED HOME INTRUDER ALERTING SYSTEM** " done by us under the guidance of **Dr. S . POORNAPUSHPAKALA, M.E., Ph.D.**, Associate Professor, Dept. of Electronics and Communication Engineering, Sathyabama institute of science and technology , Chennai, submitted partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE :27.04.23

PLACE :Chennai

SIGNATURE OF CANDIDATES

1.



2.





SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

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. Immanuel B. (39130168)** and **Mr. Jebin Gerald J. (39130185)** who carried out the project entitled **IOT Based Home Intruder Alerting System** under my supervision from January 2023 to April 2023.

Internal Guide

Dr. S. POORNAPUSHPAKALA 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, **IMMANUEL B.** (39130168) and **J. Jebin Gerald** (39130185) hereby declare that the Project Report on “**IOT BASED HOME INTRUDER ALERTING SYSTEM**” done by us under the guidance of **Dr. S. POORNAPUSHPAKALA** at Sathyabama Institute of Science and technology is submitted in partial fulfilment of the requirements of the award of Bachelor of Engineering degree in **Electronics and Communication Engineering**.

DATE:

SIGNATURE OF THE CANDIDATES

1.

2.

PLACE: Chennai

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** 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. NANDHITHA M.E., Ph. D, Dean**, School of Electrical and Electronics, **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. S. POORNAPUSHPAKALA M.E.,Ph.D**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase - 2 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) adds security to our daily lives. Technology helps us in security, ease of use, comfort and seclusion. Smartphones can also be used as a security alert device as the Smartphone is the most widely-used smart device in the world. In this work, we developed a smart home security system, in which, Arduino UNO acts as a security system which to record videos and capture images. The system has the capability to notify the user in case of any emergency by sound an alarm when an unauthorized person tries to enter inside the house. The GSM module sends a message to the admin giving them access to a web address to view the live stream of the camera placed on the door, for which we will be using an android device. This will enable the admin to take pictures of the intruder and use for future purposes. If he is a delivery boy then the system allows us to interact with the person accessing the android device's mic and camera through an existing android application.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	V
	LIST OF FIGURES	VII
	STANDARDS	IX
1	INTRODUCTION	1
	1.1 Basics of IOT	1
	1.1.1 History of IOT	3
	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	12
	1.1.3.5 Long-range Wireless	13
	1.1.3.6 Wired	13
	1.1.4 IOT Adoption Barriers	13
	1.2 Basics of face recognition	16

CHAPTER No.	TITLE	PAGE No.
	1.2.1 History of Face Recognition	17
	1.2.2 Techniques of Face Recognition	20
	1.2.3 Applications	20
2	LITERATURE SURVEY	25
3	AIM AND SCOPE OF THE WORK	29
	3.1 Aim	29
	3.2 Scope of the present Investigation	29
	3.3 Proposed project	29
4	SYSTEM ARCHITECTURE	31
	4.1 Hardware	31
	4.2 Software	34
	4.3 Algorithm Used	35
	4.4 Advantages	36
	4.5 Constrains	36
5	RESULTS AND DISCUSSION, PERFORMANCE ANALYSIS	37
	5.1 Results and discussion	39
6	SUMMARY AND CONCLUSION	41

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
3.1	Block diagram of proposed system	30
4.1	Hardware flowchart	31
4.2	Assembled view of hardware	31
4.3	Arduino UNO	32
4.4	Voice record and playback module (ISD 1820)	32
4.5	GSM Module	32
4.6	Speaker	33
4.7	Software flowchart	35
5.1	Training the model	37
5.2	Identifies authenticated person	38
5.3	Identifies unauthenticated person	38
5.4	Gives unknown person message	38
5.5	SMS received through GSM module	39
5.6	Live camera feed	40

STANDARDS

IEEE 802.11 (Wi-fi)

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires.

CHAPTER – 1

INTRODUCTION

1.1 Basics of IOT

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.

The Internet of things (IoT) describes the network of physical objects - “things” or object as shown in figure 1.1 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. 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.

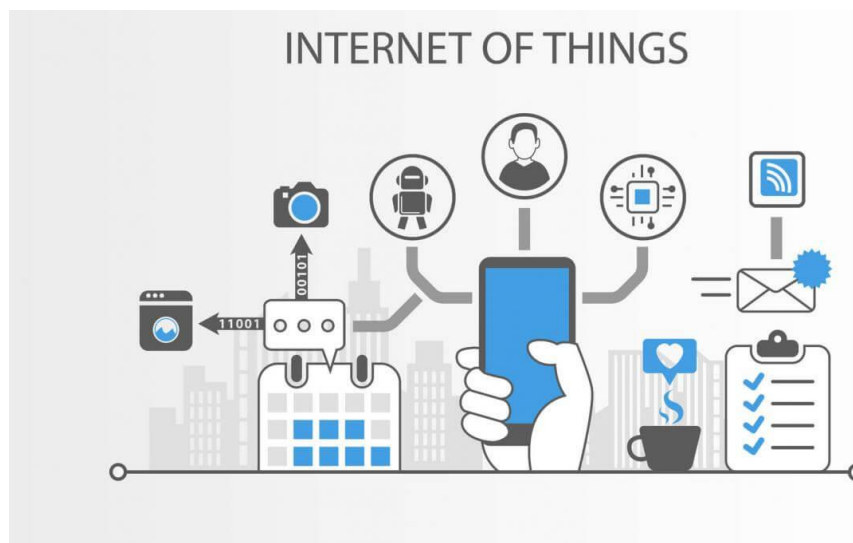


Fig 1.1: IOT [16]

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.

1.1.2.1.1 Smart home

IoT devices are a part of the larger concept of home automation as shown in figure 1.2, 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,



Fig 1.2: Smart Home [17]

1.1.2.1.2 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.

1.1.2.2.1 Medical and healthcare

The Internet of Medical Things (IoMT) is an application of the IoT for medical and health related purposes as shown in figure 1.3, 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 [18]

1.1.2.2.2.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.

1.1.2.2.3 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.

1.1.2.2.4 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.

1.1.1.3 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.

1.1.2.3.1 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 as shown in figure 1.4. 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.



Fig 1.4: IOT used for Manufacturing [19]

1.1.2.3.2 Agriculture

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content as shown in figure 1.5. 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.

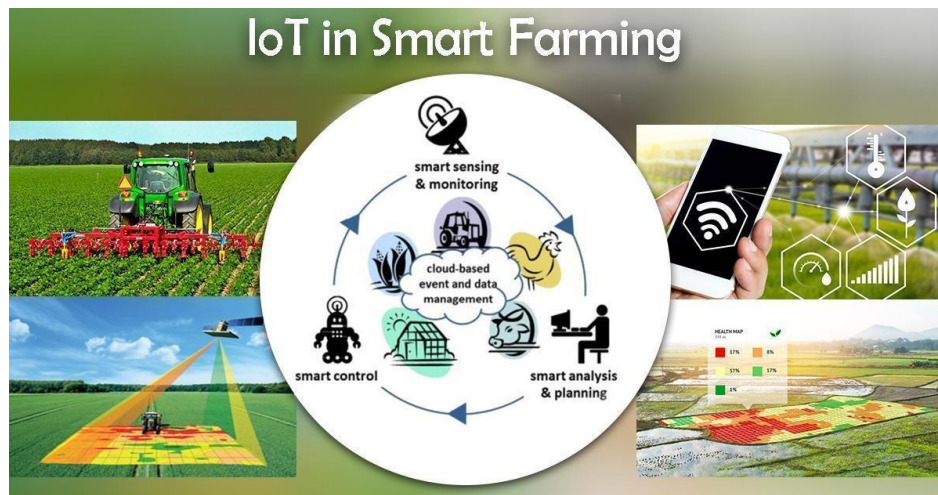


Fig 1.5: IOT in Agriculture [20]

1.1.2.3.3 Maritime

IoT devices are in use monitoring the environments and systems of boats and yachts as shown in figure 1.6. 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.

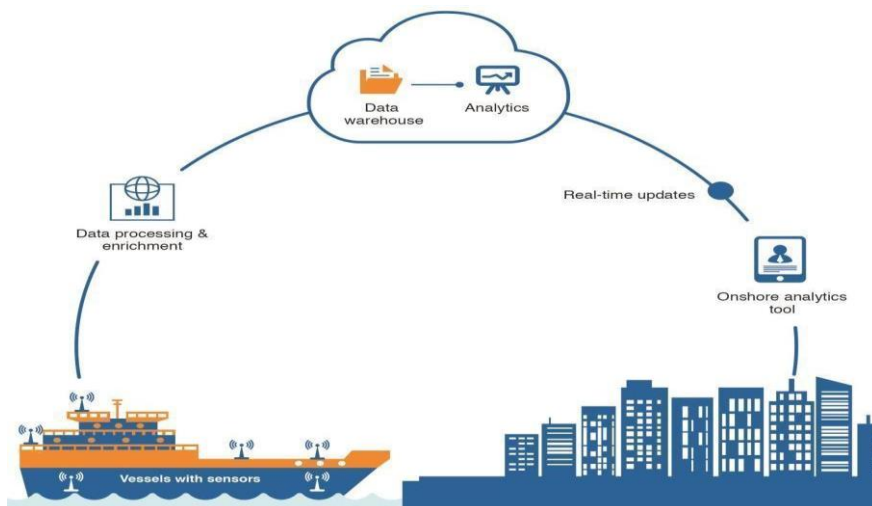


Fig 1.6: IOT in the Maritime Industry [21]

1.1.2 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:

1.1.2.1 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.

1.1.2.2 Application Layer

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

1.1.2.3 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

1.1.2.4 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.

1.1.2.5 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.

1.1.2.6 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".

The 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 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."

The traditional governance structure shows 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."

According to a study in 2018 regarding Business planning and project management, 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.

Some face traditional 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 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.

In 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.

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.

In 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 Application Social media

Founded in 2013, Lookery went on to raise money for its face modification app on Kickstarter. After successful crowdfunding, Lookery 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 Lookery

allowed augmented reality to live videos. In late 2015 SnapChat purchased Lookery, 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.

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.

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.

CHAPTER – 2

LITERATURE SURVEY

Xiaojun Bai et al (2020) presented the work on “Attendance system based on face recognition and android platform” . Aiming at the disadvantages of traditional manual attendance, this paper proposes a face recognition based attendance scheme. Through mobile platform and face recognition technology to optimize the manual attendance process. This design divides into the face recognition system of check on work attendance information input, attendance sign-in and attendance record three function module, and introduces a principle of face detection and classification, analyzes the process of the construction of the face recognition classifier, the last on the Android platform design and implement a face recognition system of check on work attendance, by comparing the experiment results of face recognition accuracy, verify the feasibility of this scheme.

Muhammed Tanriverdi et al (2017) presented the work on “Face Recognition-Based Mobile Automatic Classroom Attendance Management System”. Classroom attendance check is a contributing factor to student participation and the final success in the courses. Taking attendance by calling out names or passing around an attendance sheet are both time-consuming, and especially the latter is open to easy fraud. As an alternative, RFID, wireless, fingerprint, and iris and face recognition-based methods have been tested and developed for this purpose. Although these methods have some pros, high system installation costs are the main disadvantage. The present paper aims to propose a face recognition-based mobile automatic classroom attendance management system needing no extra equipment. To this end, a filtering system based on Euclidean distances calculated by three face recognition techniques, namely Eigenfaces, Fisherfaces and Local Binary Pattern, has been developed for face recognition. The proposed system includes three different mobile applications for teachers, students, and parents to be installed on their smart phones to manage and perform the real-time attendance-taking process. The proposed system was tested among students at Ankara University, and the results obtained were very satisfactory.

Luyang Wang (2021) presented the work on “Sign in with Face Recognition and Gesture Recognition Based on Raspberry Pi ”.This research adopts Raspberry Pi to implement this sign-in system based on deep learning and Baidu smart cloud platform. The human-computer interaction module is implemented in Python. Through the test, the accuracy of face recognition and gesture recognition is very high, and the system is very stable. This system can be used in the sign-in of universities and companies, which will improve the efficiency of sign-in and reduce the consumption of manpower and material resources. When the number of objects that need to be identified increases, the system can utilize a database to save the sign-in information, but the current system does not utilize a database, which can be added later as needed. However, one problem discovered in this system is that when a photo is used instead of a real person, it will also be regarded as a correct operation, which gives some people the opportunity to sign in instead of others. More research is needed to solve this problem.

M Shanthini et al (2020) presented the work on “IoT Enhanced Smart Door Locking System”. In recent trends, smart buildings have become the base for the Internet of Things (IoT). The usage of the internet is increased by connecting the devices in the homes to make the places more comfortable, provident, delightful, and secure. The proposed approach addresses a security aspect in smart home technologies, namely the door lock system. The door lock system determines the security by allowing the owner to monitor the buildings with a Smartphone-controlled, Bluetooth-connected system using Arduino UNO. Users can open or close the door lock by installing the developed android application in devices like tablets, smartphones, laptops, etc. by providing the login credentials like username and password which is verified in the database over the internet. If the credentials are invalid, the buzzer rings and an SMS alert is sent to the owner of the building which enhances the security. .

Sambasiva Rao Pinjala et al (2019) presented the work on “Remotely Accessible Smart Lock Security System with Essential Features”. A robust door lock system is the first and foremost thing to assure security to a home/building. Due to the ever increasing responsibilities and daily tasks, people spend most of the time away from their homes. In such situations, identifying a visitor and getting remote access

to their home is indispensable. A smart door lock which can be completely monitored and controlled from a remote location using an android application on a smartphone is proposed in this paper. When a visitor presses a calling bell/push button at the door, a Raspberry Pi with HD camera gets powered up and notifies the owner with a message and streams visitors' live identity on owner's mobile over the Internet. The owner, based on his willingness, can easily open/close the door remotely by entering a password that was preset. In addition, he can also convey an audio message to the visitor by entering the corresponding text in his smartphone app. The proof of concept provided in this paper emphasizes the real-time remote accessibility in the owner's hand (smartphone) on an interactive Graphical User Interface.

Amritha Purushothaman et al (2018) presented the work on "Pose and Illumination Invariant Face Recognition for Automation of Door Lock System". At home, security of door lock is one of the important aspects to be looked upon. Many a times the door lock fails to offer the required security. This paper proposes a door lock system which is based on face recognition. The proposed system will automatically give access to the door only if the system recognizes the face of the person trying to access the door. In case of unauthorized access, the door will remain closed. The algorithm used for face recognition is Local Binary Pattern Histogram(LBPH). This system detects and identifies the face for different pose and illumination. Hence using face recognition for door access is a great way to ensure security. In future, the system can be implemented in real time by using microcontroller instead of laptop. Also the owner can be given alert via SMS/email if any attempt of unauthorized access.

Hari Sri Rameasvar R et al (2021) presented the work on "Automated Home Security using Facial Recognition with IoT Remote Monitoring".The idea is to use facial recognition to automate a security system, which works by recognising users face data and allows security functions to happen without any hindrance. The proposed system has a camera which recognizes the face of the user who is trying to enter the building or pass through a door and if they are in the database, they are allowed passage. If the system doesn't recognize the supposed user, it marks the user as an intruder and doesn't allow them passage and passes a message to

the owner about the intruder with their photo, using internet connectivity. To implement two-stage protection automatic system shutdown and lockdown is implemented which makes the system open only after the user resets the system to use again, the user does not have to reset everything from the beginning as the previously stored data will not be deleted. The system is going to use a Raspberry pi micro-computer to do all the processing needed for the system to work. Since this is a prototype working project, only generally available technology and methods is used instead of sophisticated instruments.

CHAPTER 3

AIM AND SCOPE OF THE PRESENT INVESTIGATION

3.1 Aim

To create an IOT Based Face Recognition system using Arduino UNO.

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 prototype 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 people standing in front of the door and give them access by unlocking the door.

3.3 Proposed project

The camera captures an image of the person in front of the camera and undergoes a facial recognition algorithm and checks it with the database. The door unlocks and gives a voice message if it's a known face. If it's an unknown face, then it captures a photo and sends a message to the owner along with a voice message. The owner can click on the message through which the owner can watch the live stream of the camera and also interact with the person on the other end of the door if they choose to.

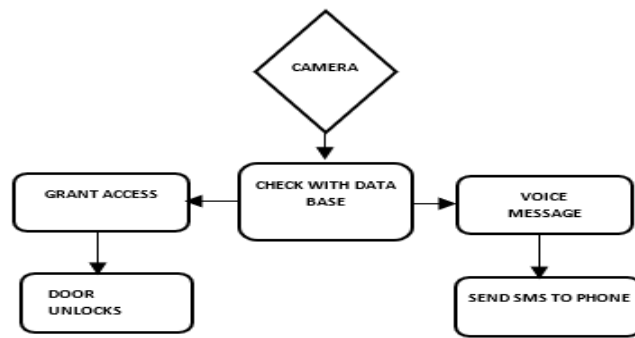


Fig 3.1: Block diagram of proposed system

CHAPTER – 4

SYSTEM ARCHITECTURE

4.1 Hardware

Various components used in this project to build the home security system. These components and sensors are attached to the Arduino UNO board as shown in figure 4.1.

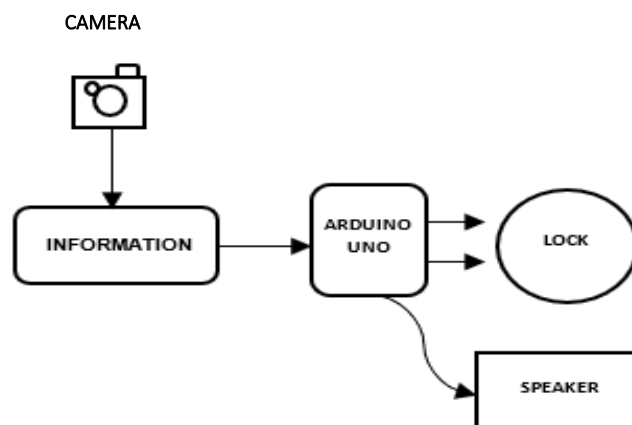


Fig 4.1: Hardware flowchart

Initially the existing methodologies were studied and from our understanding of the same, we have built a system as shown in figure 4.2 after selecting the required components like Arduino UNO, Voice record and playback module (ISD 1820) and GSM module (SUM900A)

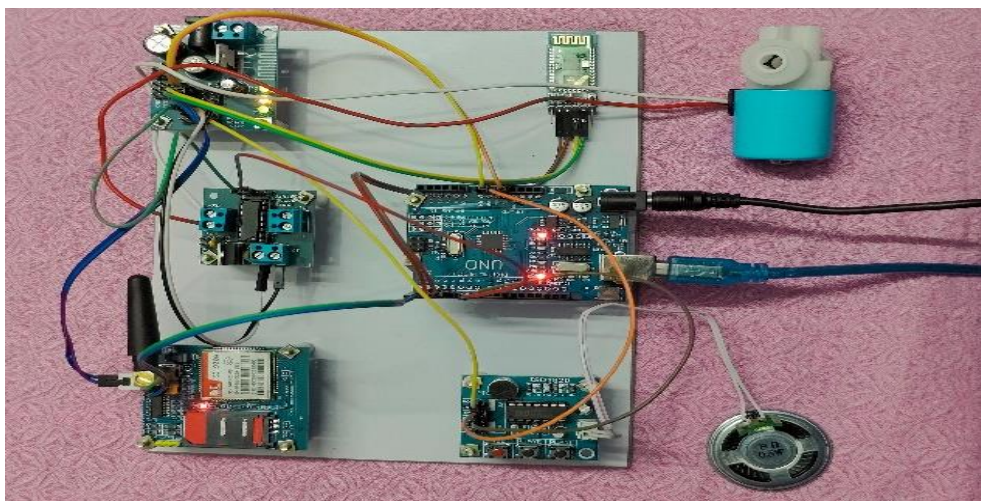


Fig 4.2: Assembled view of hardware

4.1.1: Arduino UNO:

The Arduino UNO as shown in figure 4.3 is a standard board of Arduino. Here UNO means 'one' in Italian. It was named as UNO to label the first release of Arduino Software. It was also the first USB board released by Arduino. It is considered as the powerful board used in various projects. Arduino.cc developed the Arduino UNO board. Arduino UNO is based on an ATmega328P microcontroller. It is easy to use compared to other boards, such as the Arduino Mega board, etc. The board consists of digital and analog Input/Output pins (I/O), shields, and other circuits. The Arduino UNO includes 6 analog pin inputs, 14 digital pins, a USB connector, a power jack, and an ICSP (In-Circuit Serial Programming) header. It is programmed based on IDE, which stands for Integrated Development Environment. It can run on both online and offline platforms. The IDE is common to all available boards of Arduino

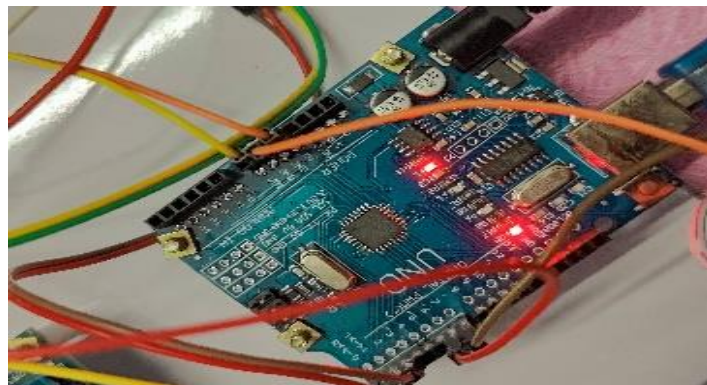


Fig 4.3: Arduino UNO

4.1.2: Voice record and playback module (ISD 1820)

Voice Record Module is base on ISD1820 as shown in figure 4.4, which a multiple-message record/playback device. It can offers true single-chip voice recording, no-volatile storage, and playback capability for 8 to 20 seconds. The sample is 3.2k and the total 20s for the Recorder. This module use is very easy which you could direct control by push button on board or by Microcontroller such as Arduino, STM32, ChipKit etc. From these, you can easy control record , playback and repeat and so on.

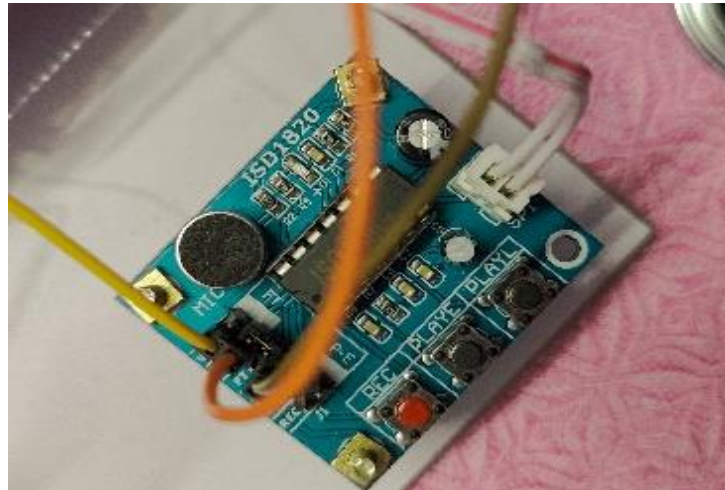


Fig 4.4: Voice record and playback module (ISD 1820)

4.1.3: GSM Module

A GSM modem as shown in figure 4.4 or GSM module is a device that uses GSM mobile telephone technology to provide a wireless data link to a network. GSM modems are used in mobile telephones and other equipment that communicates with mobile telephone networks. They use SIMs to identify their device to the network. It was created to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones and is now the default global standard for mobile communications with over 90% market share, operating in over 219 countries and territories.



Fig 4.5: GSM Module



Fig 4.6: Speaker

4.2: Software

Facial recognition is one of the biometric systems that is used to identify human faces from images, videos, or real-time. It works by comparing the real time image for instance with other image sets that are predefined in the database. This is mainly used in smartphones, airports and commercial offices. Facial recognition is carried out in three stages. First is face detection then face encoding and then finally face classification. This block diagram explains software stages of facial recognition as shown in figure 7. Both, the trained dataset image and the real-time face's image is applied to the facial recognition stage which compares both the images. The algorithm extracts the eigen values from both the images and comes to the conclusion. If the values are more or less the same then the faces match else the faces do not match. If the faces don't match, then it says that it's an unauthorized user and passes on the information to the hardware for further processes as shown in figure 4.6.

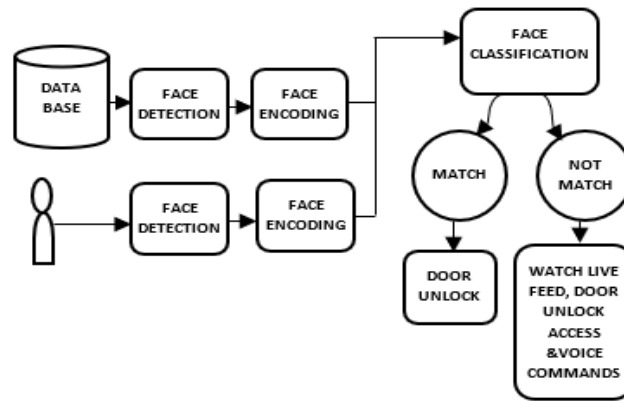


Fig 4.7: Software flowchart

4.3: Algorithm used

The algorithm we have opted for is XGBoost. It stands for eXtreme Gradient Boost. XGBoost dominates the machine learning methods mainly because of its large scalability. XGBoost also known as Generalization of AdaBoost is an influential tool for developing predictive models. The main aim of Gradient Boost is to reduce the loss function by adding weak learners using a gradient descent optimization algorithm. The main features of XGBoost are Regularized learning, Gradient tree boosting and Shrinkage and column subsampling. The algorithm is separated into four parts namely, Exact Greedy Algorithm, Approximate Algorithm, Weighted Quantile Sketch and Sparsity aware Split Finding. The main goal of XGBoost is their execution speed compared with other models from R, Python Spark etc. This algorithm is much faster than those. XGBoost is the best in structured or tabular datasets on classification and regression predictive modelling problems. XGBoost is an extension to Gradient Boosted Decision Trees (GBM) and designed exclusively for the best speed and performance.

XGBoost is an ensemble tree model improved by boosting. Compared with the traditional boosting algorithm, XGBoost can make full use of multi-core CPU for parallel computing and improve the running speed. The basic principle of XGBoost is to combine multiple tree models with lower accuracy into one model with higher accuracy [16]. Its objective function is

$$F(x) = \sum_{i=1}^n l(y_i, \hat{y}_i) + \sum_{k=1}^K \Omega(f_k)$$

The face recognition technology based on CNN, XGBoost and model fusion can be used to build the platform for safety management in power system, and its basic architecture is shown in Figure 7. Through the identification of ID card, reliable information such as name, image, post and qualification of personnel can be obtained from the authoritative information sources of human resource. At the same time, combined with the monitoring camera collecting the personnel face of operating site, face recognition can be carried out, so as to realize the following functions for safety management in power system:

The improvement of safety management capability of operating site in power system focuses on the application of face recognition technology. For face recognition technology, a face recognition model based on CNN, XGBoost and model fusion is proposed. The proposed model can take the advantage of CNN to fully dig the feature information of face, give full play to the classification advantage of XGBoost, and further improve the accuracy of face recognition by model fusion technology. Simulation results verify the highest accuracy of face recognition for the proposed model compared with other face recognition models. In addition, face recognition technology can be applied to the safety management of operating site in power system, such as qualification of special operators recognition and trajectory tracking of operators, so as to eliminate the potential safety hazards in operating site of power system and reduce management costs.

4.4 Advantages

It helps us to unlock the door without using our hands by increasing the security also by a mile. The voice alert can alert the neighbors and the picture that is sent to us via mail will help us to use it as an evidence in the future endeavors. If its a known friend standing in front of the door then we can save the embarrassment and let them in by controlling the lock remotely.

4.5 Constrains

This system can have certain issues when there is not enough lighting around the subject standing in front of the camera. There needs to be an uninterrupted internet connectivity for the microcontroller to run the face recognition algorithm and to send the images to the owner. Apart from these, a constant power supply is very much needed for the light to turn on in front of the camera.

CHAPTER – 5

RESULTS AND DISCUSSION, PERFORMANCE ANALYSIS

5.1: Results and discussion

The model first captures the image of the authenticated person and then the model is trained as shown in figure 5.1. The model can Identify the authenticated person, even if they have accessories like spectacles or sunglasses put on as shown in figure 5.2 with an average accuracy of 99.12%. If they stand in front of the camera and the entry time is marked in a separate file for future usage purposes. The system identifies the unknown person if an unauthenticated person is in front of the camera as shown in figure 5.3 and shows a message that it's an invalid person as shown in figure 5.4 and can further update the admin about the same.



Fig: 5.1: Training the model

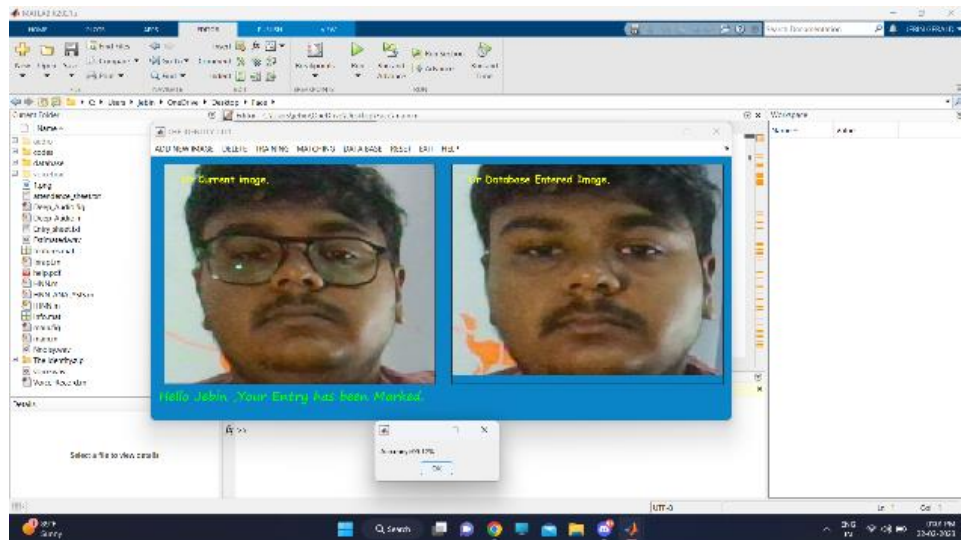


Fig: 5.2: Identifies authenticated person

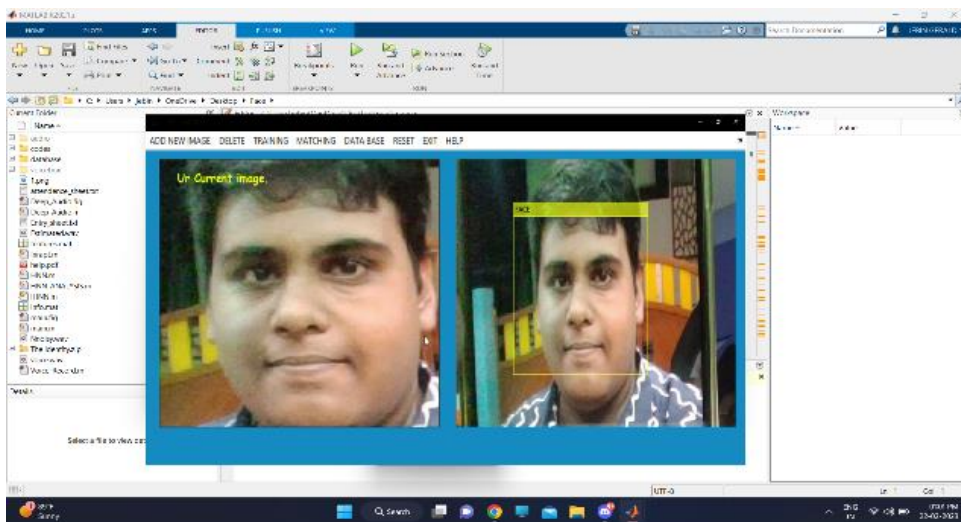


Fig: 5.3: Identifies unauthenticated person

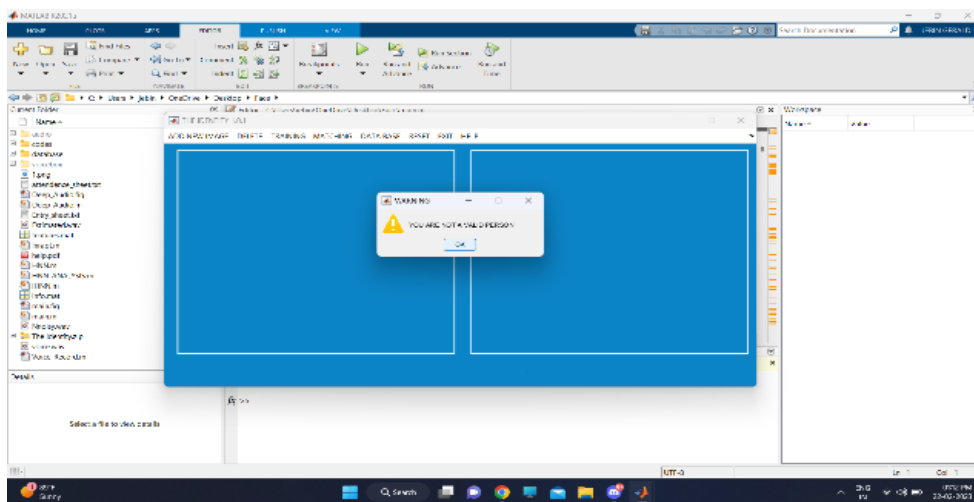


Fig: 5.4: Gives unknown person message

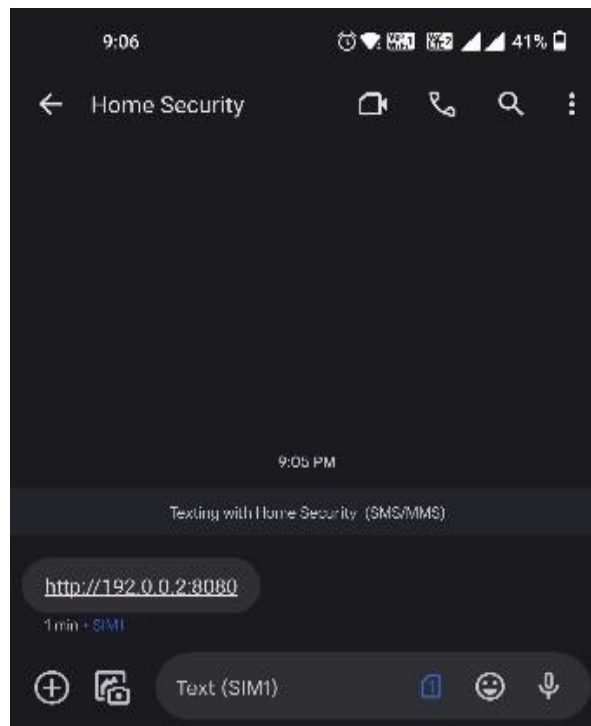


Fig: 5.5: SMS received through GSM module

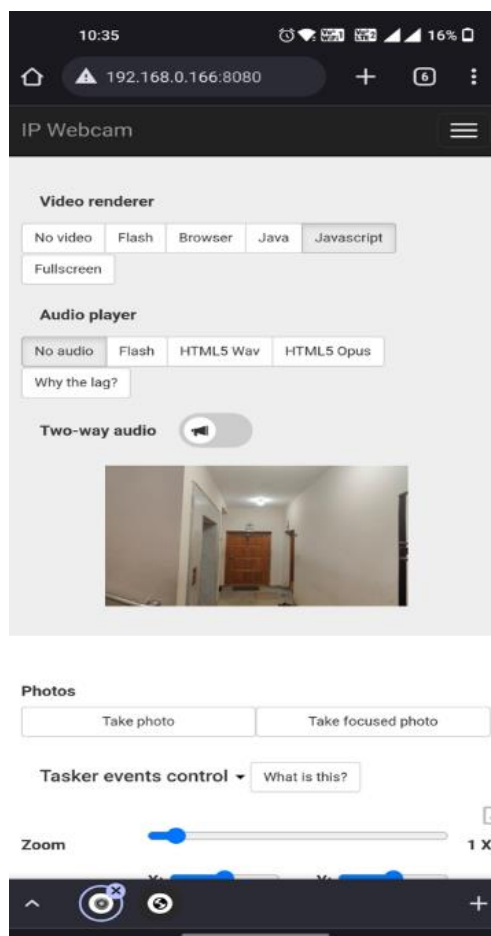


Fig: 5.6: Live camera feed

The information from the software is passed on to the Arduino UNO and the lock would unlock, if the person is an authenticated person. simultaneously giving out a voice message with a speaker and the UNO would allow the GSM module to send an SMS as shown in figure 5.5, to the registered mobile number if it's an unauthenticated person. This SMS contains a web address which will allow the admin to access the android device's camera enabling the admin to view the live feed of the camera and to interact with the unauthenticated person on the other as shown in figure 5.6.

CHAPTER – 6

SUMMARY AND CONCLUSION

The proposed methodology was successfully implemented by using face recognition algorithms to unlock the door using Arduino UNO. There is ample security methods to identify the intruder such as alerting the admin in case of emergency, being able to watch the live stream and interact through the live stream. This system provides comfort as the admin does not require keys to unlock the door as he can unlock the them by just standing in front of the door which is also an added security as it uses face recognition biometrics. The system can be further more enhanced by using sensors like LiDAR and Iris scanner for more accurate face recognition as supposed to just the camera as used in this methodology.

REFERENCES

- [1] Nagasree Y Lakshmi Venkata, Ch. Rupa, B Dharmika, Tja G Nithin, N Vineela, "Intelligent Secure Smart Locking System Using Face Biometrics" in 2021 International Conference on recent trends on electronics information, Communication & Technology (RTEICT).
- [2] Handayani Saptaji Winahyu, Eni Dwi Wardhani, Samuel Beta,, "Attendance system based on face recognition" in 2021 International Seminar on Application for Technology of information and Communication (Semantic), Publisher - IEEE.
- [3] 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).
- [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
- [7] conferences on Information Technology Information Systems and Electrical Engineering (ICITISEE), 2017.
- [8] A. Aftab et al., "LBPH based improved face recognition at low resolution", 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018.
- [9] 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.
- [10] 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.
- [11] 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.

[12] 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.

[13] S. Nico and W. Ridwan, "Design of Smart Home Security System using Object Recognition and PIR Sensor", Procedia Computer Science, vol. 135, 2018.

[14] 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 (ICASET 2017), March 2017.

[15] 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.

[16] https://www.scarlettcybersecurity.com/sites/default/files/styles/blog_1200x675/public/2021-07/What%20is%20an%20IoT%20Attack.jpg?itok=4UYFoDHN

[17] <https://www.spencerstv.com/blog/7-benefits-of-smart-home-appliances>

[18] <https://ehealth.eletsonline.com/2019/03/iot-to-redefine-healthcare-ecosystem/>

[19] <https://2wtech.com/iot-is-made-for-the-manufacturing-industry/>

[20] <https://data-flair.training/blogs/iot-applications-in-agriculture/>

[21] <https://www.linkedin.com/pulse/sensors-iot-shipping-industry-s-seetharaman/>