**CHAPTER 1**

**INTRODUCTION**

* 1. **INTERNET OF THINGS**

The Internet of Things (IoT) refers to the interconnection of various physical devices and objects embedded with sensors, software, and other technologies that enable them to collect and exchange data over the Internet. These devices can range from simple household appliances like smart thermostats and lights to more complex systems like smart cities, industrial machinery, and even autonomous vehicles.

The basic idea behind IoT is to make everyday objects "smart" by enabling them to gather and share data with other devices, people, and systems. By doing so, IoT can help improve efficiency, enhance convenience, and create new opportunities for innovation and growth in a wide range of industries.

One of the key benefits of IoT is that it can help organizations make more informed decisions by providing real-time data and insights. For example, a smart factory could use IoT sensors to monitor the performance of its machines and identify potential issues before they cause downtime or quality problems. Similarly, a smart city could use IoT devices to manage traffic flow, optimize energy usage, and improve public safety.

Overall, IoT is a rapidly growing field with immense potential for transforming the way we live and work. However, it also presents a number of challenges around security, privacy, and interoperability that must be addressed to ensure its continued success. IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are Radio Frequency Identification (RFID) and Near Field Communication (NFC), low energy Bluetooth, low-energy wireless, low-energy radio protocols, Long Term Evolution (LTE-A), and Wi-Fi Direct. These technologies are used to support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems. RFID technology employs 2-way radio transmitter-receivers to identify and track tags associated with objects. NFC consists of communication protocols for electronic devices, typically a mobile device and a standard device.

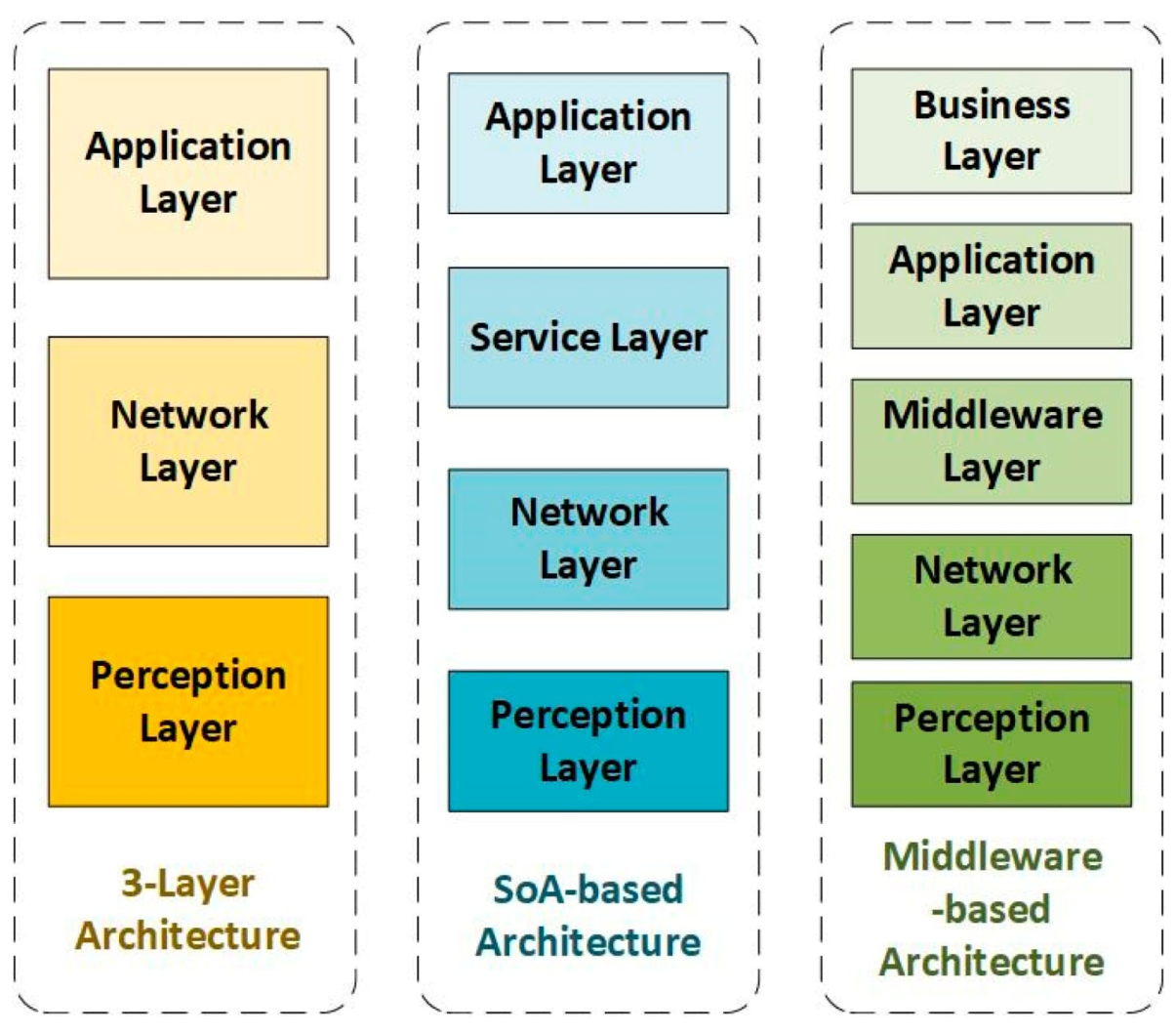


Fig.1.1 Architecture of IoT

* + 1. **Applications Of IoT**
       1. **Smart door automation system**

IoT-based smart door automation system is a technology that allows doors to be remotely controlled and monitored through a network of connected devices using the Internet of Things (IoT) technology. It is a system that uses a combination of hardware and software components to automate the door opening and closing process and provide enhanced security and convenience. In an IoT-based smart door automation system, the door is equipped with various sensors, such as motion or proximity sensors, that detect the presence of a person or object. These sensors are connected to a microcontroller that processes the data from the sensors and determines when to open or close the door. The system can also include other devices such as cameras, actuators, and access control mechanisms, depending on the specific application.

* + - 1. **Smart Cities**

Many major cities were supported by smart projects, like Seoul, New York, Tokyo, Shanghai, Singapore, Amsterdam, and Dubai. Smart cities may still be viewed as cities of the future and smart life, and by the innovation rate of creating smart cities today, it will become very feasible to enter IoT technology into city development. Smart cities demand requires careful planning in every stage, with the support of agreement from governments, and citizens to implement the Internet of Things technology in every aspect. With the IoT, cities can be improved on many levels, by improving infrastructure, enhancing public transportation reducing traffic congestion, and keeping citizens safe, healthy, and more engaged in the community.

* + - 1. **Smart Home and Buildings**

Wi-Fi technologies in home automation have been used primarily due to the networked nature of deployed electronics where electronic devices such as TVs, mobile devices, etc are usually supported by Wi-Fi. It has started becoming part of the home IP network due to the increasing rate of adoption of mobile computing devices like smartphones, tablets, etc. For example, networking to provide online streaming services or network at home, may provide a means to control the device functionality over the network. At the same time, mobile devices ensure that consumers have access to a portable controller for the electronics connected to the network. Both types of devices can be used as gateways for IoT applications.

* + - 1. **Smart Energy and the Smart Grid**

A smart grid is related to information and control and is developed to have smart energy management. A smart grid that integrates information and communications technologies (ICTs) into the electricity network will enable real-time, two-way communication between suppliers and consumers, creating more dynamic interaction on energy flow, which will help deliver electricity more efficiently and sustainably. Many applications can be handled due to the Internet of Things for smart grids, such as industrial, solar power, nuclear power, vehicles, hospitals, and city’s power control.

* + - 1. **Smart Health**

Close attention that is required to hospitalized patients whose physiological status should be monitored continuously can be constantly done by using IoT monitoring technologies. Smart health sensors are used to collect comprehensive physiological information and use gateways and the cloud to analyse and store the information and then send the analysed data wirelessly to caregivers for further analysis. It replaces the process of having a health professional come by at regular intervals to check the patient’s vital signs, instead providing a continuous automated flow of information. It simultaneously improves the quality of care through constant attention and lowers the cost of care by reducing the cost of traditional ways of care in addition to data collection and analysis.

* + - 1. **Cyber Attacks**

IoT devices expose an entire network and anything directly impacted to the risk of attacks. Though those connections deliver powerful integration and productivity, they also create the perfect opportunity for many of them like a hacked stove or fire safety sprinkler system. The best measures against this address the most vulnerable points, and provide custom protections such as monitoring and access privileges. Some of the most effective measures against attacks prove simple,

* **Built in Security**

Individuals and organizations should seek hardened devices, meaning those with security integrated into the hardware and firmware.

* **Encryption**

It must be implemented by the manufacturer and through user systems.

* **Risk Analysis**

Organizations and individuals must analyze possible threats in designing their systems or choosing them.

* **Authorization**

Devices, whenever possible, must be subject to privilege policies and access methods.

* + 1. **Advantages Of IoT**
       1. **Improved Customer Engagement**

Current analytics suffer from blind spots and significant flaws in accuracy and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

* + - 1. **Technology Optimization**

The same technologies and data which improve the customer experience also improve device use and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

* + - 1. **Reduced Waste**

IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.

* + - 1. **Enhanced Data Collection**

Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces and places it exactly where humans really want to go to analyse our world. It allows an accurate picture of everything.

* + 1. **DISADVANTAGES OF IoT**
       1. **Security Breaches**

The biggest disadvantage of IoT is the security risk it poses. As more devices become interconnected, there is an increased risk of cyber-attacks and data breaches.

* + - 1. **Privacy Concern**

IoT devices collect and store large amounts of data about users, and there are concerns about how this data is used and who has access to it.

* + - 1. **The complexity of the system**

The designing, developing, maintaining, and enabling the extensive technology to IoT systems is quite complicated.

* + - 1. **High Dependency on the Internet**

They rely heavily on the internet and cannot function effectively without it. With IoT devices becoming increasingly integrated into our lives, we run the risk of becoming overly dependent on technology and losing important skills and abilities.

* 1. **INTRODUCTION TO WEB APPLICATION**
* **Definition:** A web application is a software program that is accessible through a web browser over the internet or an intranet.
* **Accessible from anywhere:** Since web applications are hosted on the internet, users can access them from any location with an internet connection.
* **Platform independence:** Web applications can be accessed from any device that has a web browser, regardless of the operating system or hardware specifications.
* **Client-server architecture:** Web applications typically follow a client-server architecture, where the server provides resources and services, while the client requests and consumes them.
* **Interactive user interface:** Web applications offer an interactive user interface that allows users to perform various tasks and interact with the system.
* **Data storage and retrieval:** Web applications store and retrieve data from databases or other storage mediums, allowing users to access their data from anywhere.
* **Scalability:** Web applications can easily scale up or down to accommodate changes in user traffic or data volume.
* **Integration with other systems:** Web applications can integrate with other systems or services through APIs, allowing for seamless data exchange and communication.
* **Security:** Web applications must be designed with security in mind to protect sensitive user data and prevent unauthorized access.
* **Maintenance and updates:** Web applications require regular maintenance and updates to ensure they remain secure, efficient, and functional.
  1. **OBJECTIVE OF THE PROJECT**

The objective is to design an innovative and convenient solution for controlling access to a building. This system should allow authorized users to remotely open and close doors with the touch of a button on their mobile devices. The system should also have the capability to restrict access to unauthorized users, ensuring security and privacy. The objective is to provide a seamless, time-efficient, and user-friendly experience for authorized users. Easy to install, use, and maintain, cost-effective for building administrators, and also improving the overall efficiency and security of the system.

* 1. **PROBLEM STATEMENT**

The current door lock systems have limitations in terms of security, accessibility, and convenience. Traditional locks can be easily picked or tampered with, and lost keys can pose security risks. Additionally, traditional locks may be difficult for people with disabilities or mobility issues to use, leading to accessibility challenges. Further, there is no easy way to monitor who enters or leaves the building, which can be a security concern. The solution should be reliable, easy to use, and cost-effective.

**CHAPTER 2**

**LITERATURE SURVEY**

**2.1 ADVANCED COMPUTING IN IoT FOR DOOR LOCK AUTOMATION**

[1] Baby Chitra et. proposed a model in which they are using the raspberry pi microprocessor as the processing unit. The proposed model has two input nodes. The first node provides voice recognition and is integrated with google assistant, whereas the second node is a face recognition module, consisting of a USB camera. The analysis of face recognition s achieved using python based OpenCV module. When the authorized person is identified, the microprocessor will trigger the relay, which in turn will complete the magnetic lock circuit and open the door. The same principle is used to trigger various appliances such as lights, fans, etc. using voice commands. The database in the raspberry pi can be connected to a government identification system to monitor and identify if any unknown person arrives. The same communication can be sent to the owner’s phone to provide the required access to the new person. This proposed method will help the owner to give access to the online delivery personnel, when he is not at home so that he can place their package inside the compound, without any necessity to open the door.

**2.2 A SMART LOCK SYSTEM USING Wi-Fi SECURITY**

[2] A. Kassemet.al proposed a digital door lock system that uses digital information such as a secret code instead of the legacy key system. In this proposed system, a Central Control module is embedded in the door itself, this is required to prevent additional complications and a more robust mechanism for the door as a whole. Technically, this system embeds itself in the Local Area Network of the house. This adds extra security layers and prevents access to the system only through the network. Furthermore, the biggest advantage of the proposed system over existing ones is that it can be easily installed with minimal requirement of infrastructures and planning.

**2.3 AUTOMATED DOOR CONTROL SYSTEM FOR OFFICE BUILDINGS**

[3] M. Lianget. al proposed a system that is designed to be highly flexible and customizable, allowing building managers to easily adjust access control policies and settings to suit the changing needs of the building. The system also includes advanced features such as real-time monitoring, automated alerts, and remote access control, which provide added security and convenience for building occupants and administrators.

The implementation of the system involves the installation of sensors and access control systems at strategic points throughout the building, as well as the development of custom software to manage and control the various components of the system. The system is designed to be highly scalable, allowing it to be easily expanded or modified as the building's needs change over time.

Overall, the proposed automated door control system represents a significant improvement over traditional access control systems, providing greater security, convenience, and flexibility for modern office buildings**.**

**2.4 SMART DOOR SYSTEM USING ARDUINO**

[4] N. Kaur et.al proposed a system based on the internet using biometric and Zigbee technology that would use a combination of biometric sensors, such as fingerprint or facial recognition, and Zigbee wireless communication technology to provide secure access to authorized personnel.

In proposed smart door access control system based on the internet using biometric and Zigbee technology has the potential to provide a high level of security and convenience for building owners and managers, while also offering the flexibility to remotely manage access to the building or room. However, careful consideration should be given to the selection and use of biometric sensors, as well as the protection and privacy of biometric data.

**2.5 SMART DOOR ACCESS CONTROL SYSTEM BASED ON INTERNET**

[5] Y. Wanget.al proposed a system using Arduino, a project that involves the use of an Arduino microcontroller to create an intelligent and secure access control system for a door. The system uses various sensors and actuators to detect the presence of authorized individuals and allow them to access the door while denying access to unauthorized persons. The project involves designing and building a circuit that includes an Arduino board, a motor or servo motor, an RFID reader or a keypad, and other necessary components. The Arduino board will control the motor, read the RFID or keypad inputs, and manage the system's logic.

The system's operation is straightforward. Authorized individuals will present their RFID card or enter the correct code on the keypad, and the system will verify their credentials and open the door. If an unauthorized person tries to gain access, the system will deny entry and notify the owner of the attempted breach.

**2.6 DEVELOPMENT OF A SMART DOOR LOCK SYSTEM USING FINGERPRINT AND MOBILE APPLICATION**

[6] S. Choi et.al proposed a system where user will enter fingerprint in the fingerprint scanner which is connected to the door latch through the microcontroller. After scanning the print, the system runs its database and looks for a match. If any match is found, the latch opens and thus the door gets unlocked. Same thing happens when user wants to lock the door. Correct fingerprint makes the latch to close, locking the door behind the user.

If wrong fingerprint is given, the system beeps the buzzer showing Try again in the LCD display. If consecutive 5 or more wrong fingerprints are given, i.e., if anyone tries to break in continuously, the system enters a secured mode where it rings the alarm showing Panic Mode on the LCD screen. A message gets delivered to the owner notifying that there has been an attempt to break in.

**2.7 SMART DOOR LOCK SYSTEM USING NFC AND QR CODE**

[7] M. H. Leeet.al proposed a system consisted of Raspberry Pi B+ as microcontroller, solenoid electromagnetic lock as an output, QR scanner, Pi Camera for input and relay module as switch. The inputs of this system which are the QR scanner and camera. The bottom side of the block diagram shows the outputs;

Electromagnetic lock and Database Table. The electromagnetic lock is used to open and close the door. The inputs and outputs are connected to the Raspberry Pi ports and the operation is programmed in Raspbian operating system. The QR scanner will detect the QR card from the user and the lock will open if the data inside the QR code matched with the database. The buzzer is used to inform the user that QR card has been read by QR scanner. The data and image captured by camera Pi is collected through the process

and are sent to PHPMYADMIN database via the local internet provided by the Raspberry Pi to be recorded.

**2.8 DESIGN AND IMPLEMENTATION OF A SMART DOOR LOCK SYSTEM BASED ON Wi-Fi AND BLUETOOTH**

[8] L. Wang, et.al proposed a system that uses both Wi-Fi and Bluetooth technologies to provide easy and reliable access control. The system consists of a physical door lock that is controlled by a mobile application. The mobile application communicates with the lock via Wi-Fi or Bluetooth, depending on the proximity of the user to the door.

The door lock is designed to be easy to install and can be retrofitted to most existing door locks. It is battery-powered and can be controlled remotely using the mobile application. The mobile application allows the user to create access codes for friends and family, grant temporary access to guests, and revoke access at any time. The application also provides real-time notifications when someone unlocks the door or attempts to enter an incorrect access code.

The Smart Door Lock System is secure and uses strong encryption algorithms to protect access codes and communication between the lock and the mobile application. The system is designed to be highly scalable and can support multiple users and locks. The lock also has a backup physical key in case of an emergency.

**2.9 DESIGN AND IMPLEMENTATION OF SECURE SMART DOOR LOCK SYSTEM**

[9] J. J. Tan et.al proposed a system that involves the design and implementation of a secure smart door lock system using RFID technology. The system is designed to provide secure and convenient access control for homes and businesses. The system consists of an RFID reader, a door lock mechanism, RFID tags, and a software interface. The RFID reader is used to read the RFID tags, which are used to identify authorized users. The door lock mechanism is then activated to allow access to the user. The software interface provides an easy-to-use interface for managing the system and configuring the security features. The system is tested for security vulnerabilities and is deployed once it is deemed safe and functional. The maintenance of the system is also considered to ensure long-term operation. With the proper implementation, this system can provide a reliable and secure access contro l solution.

**2.10 DESIGN AND CONSTRUCTION OF DOOR LOCKING SECURITY SYSTEMS USING GSM**

[10] Ushie James Ogriet. al proposed a system that works on GSM based Door Lock System that is designed and constructed by interfacing to an ATMEGA328P microcontroller a keypad for entering lock and unlock passcode into the system; a liquid crystal display (LCD) for display numbers keyed in and door status; a SIM800L GSM module for receiving lock and unlock passcode text messages from the remote cell phone and also sending alert and feedback text messages to cell phone; a relay mechanism for driving a DC motor clockwise or counter clockwise for locking and unlocking of door.

**2.11 DOOR AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE**

[11] Kamelia, Lia et.al proposed a door automation system using Bluetooth-based Android for mobile phones a smart system that enables users to remotely control their doors using an Android smartphone that is equipped with Bluetooth connectivity. The system consists of two main components: a Bluetooth-based controller and an Android mobile application. The Bluetooth-based controller is responsible for receiving commands from the Android application and controlling the door's mechanism. The controller can be connected to the door's locking mechanism, and it can be programmed to recognize specific Bluetooth signals from the user's smartphone. The Android mobile application is designed to send commands to the Bluetooth-based controller. Users can download the application to their smartphones and connect it to the Bluetooth-based controller. Once connected, they can open or close the door remotely using their smartphones.

**CHAPTER 3**

**SYSTEM REQUIREMENTS**

**3.1 HARDWARE CONFIGURATION**

Processor : Intel Pentium IV

Microcontroller : Atmega328P

Hard Disk Space : 40 GB

Monitor : 14’’

Internal Memory Capacity : 256 Mb

Battery : 3.7V

Toolkit : Arduino UNO, GSM module

Wi-Fi module : ESP8266

Camera module : ESP32 module

Sensor : PIR HC SR505

**3.2 SOFTWARE CONFIGURATION**

Operating System : Windows

Language : C, Html, CSS

**CHAPTER 4**

**METHODOLOGY**

**4.1 EXISTING SYSTEM**

The existing syatem proposes a home automation model which provides lock protection. In this proposed model we are using the raspberry pi microprocessor as the processing unit. The proposed model has two input nodes. The first node provides voice recognition and it is integrated with google assistant, whereas the second node is a face recognition module, consisting of a USB camera. The analysis for face recognition is achieved using python based OpenCV module. When the authorized person is identified, the microprocessor will trigger the relay, which in turn will complete the magnetic lock circuit and open the door. The same principle is used to trigger the various appliances such as light, fan, etc. using voice commands. The database in the raspberry pi can be connected to a government identification system to monitor and identify if any unknown person arrives. The same communication can be sent to the owner’s phone to provide the required access to the new person. This proposed method will help the owner to give access to the online delivery personnel, when he is not at home so that he can place their package inside the compound, without any necessary to open the door.

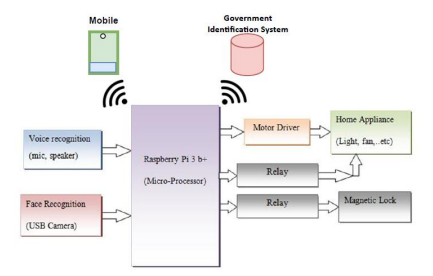


Fig.4.1 Block Diagram of Existing System

**4.1.1 DRAWBACKS OF THE EXISTING SYSTEM**

* Dependence on Technology: Smart door automation systems rely on technology, such as Wi-Fi, to function. If your internet or power goes out, you may not be able to access or control your smart lock.
* Some smart door automation systems may not be compatible with all types of door hardware, which can limit your options and require additional costs for new hardware.
* There is always a risk of hacking or other security breaches.
* Smart locks require batteries to operate, and if the batteries die or run out of power, you may not be able to unlock your door without a physical key.
* Smart door automation systems can be more expensive than traditional locks, and additional costs may be incurred for installation, maintenance, or subscription services.

**4.2 PROPOSED SYSTEM**

A smart door automation system using GSM, cam, and PIR (Passive Infrared) sensor is an advanced security system that combines several technologies to provide enhanced security and convenience to homeowners. This system enables remote control of access to a property, captures video footage of visitors, and detects motion within a property. The system typically consists of a door lock mechanism, a GSM module, a camera, a PIR sensor, and a microcontroller. The microcontroller serves as the brain of the system and controls the lock mechanism, camera, and PIR sensor. The GSM module enables the communication between the microcontroller and authorized individuals' mobile devices or computers, allowing them to remotely open or close the door and receive real-time notifications when someone enters or exits the property. The camera captures video footage of visitors, which can be viewed remotely by the homeowner or authorized individuals using a mobile application or computer connected to the internet. The PIR sensor detects motion within the property, triggering the camera to record video footage and sending alerts to the homeowner or authorized individuals' mobile devices when motion is detected.

Smart door automation systems using GSM, cam, and PIR sensor offer several benefits over traditional locking systems, including increased security, convenience, and peace of mind. Homeowners can remotely monitor their property and control access from anywhere in the world, while also receiving real-time alerts when someone enters or exits the property or when motion is detected.

Overall, smart door automation systems using GSM, cam, and PIR sensor provide a robust and reliable security solution that combines advanced technology with ease of use and accessibility, making them an attractive option for homeowners looking to enhance their property's security and convenience.

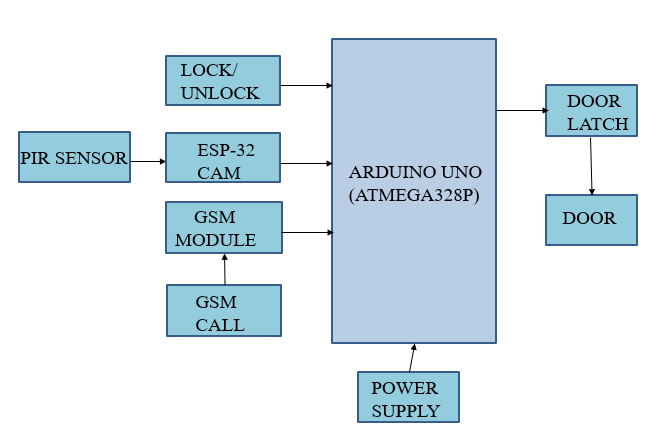


Fig.4.2 Block Diagram of Smart Door Automation System

**4.2.1 ADVANTAGES OF THE PROPOSED SYSTEM**

* **Remote Access:** With the GSM module, users can access the smart door system from anywhere in the world. They can remotely unlock the door and monitor the entrance through the ESP cam.
* **Security**: The PIR sensor detects motion and triggers the system to take action, such as sounding an alarm or sending a notification to the user's smartphone. This enhances security and helps to deter unauthorized access.
* **Integration:** The integration of multiple modules (GSM, WiFi, ESP cam, and PIR sensor) provides a comprehensive and reliable system that can be easily customized to meet the user's specific needs.
* **Convenience:** Smart door automation eliminates the need for physical keys, which can be lost or stolen. Users can simply use their smartphone to unlock the door, which is more convenient and less hassle.
* **Energy Efficiency:** The system can be programmed to turn off the lights and air conditioning when the door is locked, saving energy and reducing utility bills.
* **Increased Property Value:** Smart home technology is becoming increasingly popular among homeowners, and installing a smart door system can increase the value of the property.

**CHAPTER 5**

**SYSTEM IMPLEMENTATION**

* 1. **PIR SENSOR**

PIR (Passive Infrared) sensors are motion sensors. When a PIR sensor is placed near the door to detect the presence of a person approaching the door. Then it sends a signal to the control system, which can then trigger the GSM module. PIR sensors are commonly used in smart door automation systems due to their cost-effectiveness, ease of installation, and high accuracy.



Fig.5.1 PIR sensor

* 1. **ARDUINO UNO**

Arduino plays a critical role in smart door automation systems by providing a programmable control system that can interact with various sensors and actuators. The Arduino board is connected to motion sensors to detect the state of the door and the environment around it. Using Arduino, you can program the logic to perform certain actions based on the input from the sensors, such as unlocking the door.



Fig.5.2 Arduino UNO

* 1. **GSM MODULE**

A GSM (Global System for Mobile Communications) module is a device that allows a smart door automation system to communicate with the user's mobile device or remotely with a server using a cellular network. Using a GSM module, the smart door automation system can send and receive text messages or phone calls to and from the user's mobile phone. The user can remotely send commands to the system to lock or unlock the door, receive notifications if the door is opened or closed, or even view a live video stream of the area around the door. They provide a reliable and secure means of communication that is not affected by the availability or quality of a local Wi-Fi network.

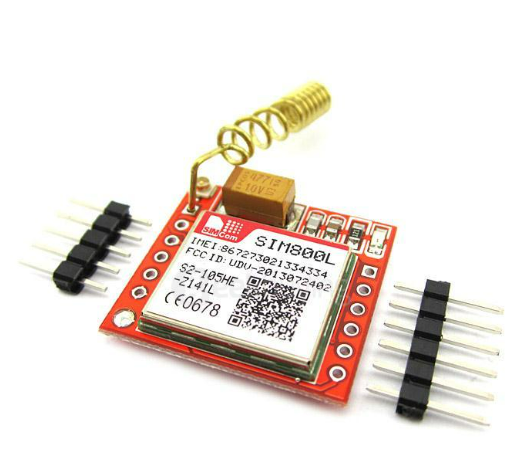


Fig.5.3 Arduino UNO

* 1. **ESP32-CAM MODULE**

It is a low-cost, Wi-Fi-enabled microcontroller with a built-in camera that is commonly used in smart door automation systems. It allows for remote monitoring and control of the door using a web browser or mobile app. The ESP32-CAM module is programmed to send a notification to the user's smartphone automatically when a face is detected. It can enhance security and convenience by allowing for remote monitoring and control of the door using a web browser or mobile app and by capturing images or streaming live video of the area around the door.



Fig.5.4 ESP32 CAM module

* 1. **RELAY MODULE**

Relays are commonly used in smart door automation systems to switch power to the door lock. The relay acts as a switch, allowing the microcontroller to control the lock's power supply. This enables the microcontroller to unlock or lock the door remotely through a smartphone app or other control interface. The relay can be connected to sensors to trigger actions based on events such as the door opening or closing.

****

Fig.5.5 Relay

* 1. **ESP8266 MODULE**

ESP8266 is a Wi-Fi-enabled microcontroller. It can be used to connect the door lock to the internet, allowing it to be remotely controlled and monitored. With the help of sensors and actuators, the ESP8266 can detect when the door is opened or closed and trigger actions accordingly, such as sending notifications to a smartphone app. It can be integrated with other smart home devices, such as voice assistants, to provide a seamless and interconnected experience.

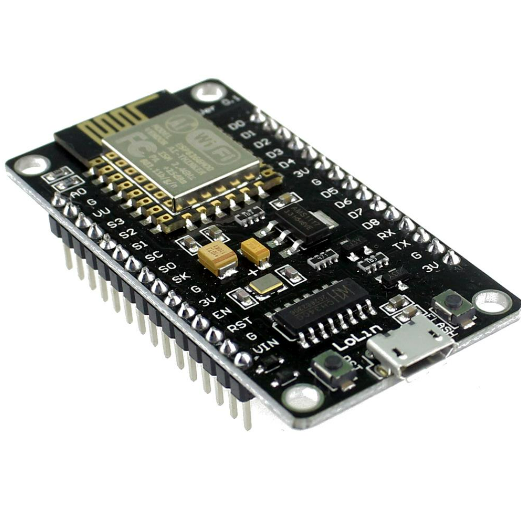


Fig.5.6 ESP8266 Wi-Fi module

**CHAPTER 6**

**RESULT**

**6.1 RESULT AND DISCUSSION**

Smart door automation system allows users to control the door remotely using a smartphone eliminating the need for a physical key. A smart door automation system can also be used to control who has access to a property. Finally, a smart door automation system can be used to provide alerts and notifications when certain events occur. The proposed system is expected to have several benefits, including enhanced security, Convenience and automation., Remote access and control, Customizable to meet specific requirements and Improved energy efficiency.

**CHAPTER 7**

**CONCLUSION AND FUTURE ENHANCEMENT**

**7.1 CONCLUSION**

The development of an IoT-based smart door automation system using PIR sensors and GSM has the potential to improve security in the workplace or anywhere. The system will enable real-time detection of visitors, faster response time, and provides easy access to control the door. The hardware for the project is implemented and the output results are verified successfully.

* 1. **FUTURE ENHANCEMENT**

Artificial Intelligence (AI): AI can be used to improve the performance of the system by analysing data from the sensors and making decisions based on that data. This can help to optimize the system's operation, reduce energy consumption, and improve security.

Real-time Analytics: Real-time analytics can be used to provide insights into the performance of the system and identify areas for improvement. This can help to optimize the system's operation, improve security, and reduce energy consumption.

Voice Recognition: Voice recognition technology can be used to provide a more convenient access control mechanism, allowing authorized personnel to unlock the door using their voice.

**REFERENCES**

[1] Ajay Sudhir, Baby Chithra, Anish Sagar Naidu, Salna Joy “Advanced Computing in IoT for Door Lock Automation” (2022) International Conference on Electronics and Renewable Systems(ICEARS 2022) IEEE Xplore Part Number: CFP22AV8-ART; ISBN: 978-1-6654-8425-1

[2] Md Shahin Ali, Md Sipon Miah, Jahurul Haque, Md Mahbubur Rahman, Md Khairul Islam “An enhanced technique of skin cancer classification using deep convolutional neural network with transfer learning models (2021) ”, in Elsevier Machine Learning with Applications, Volume 5, 15 September 2021.

[3] 10.1109/ACTEA.2016.7560143. A. Kassem, S. E. Murr, G. Jamous, E. Saad and M. Geagea, "A smart lock system using Wi-Fi security," (2016) 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA), 2016, pp. 222-225.

[4] 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, pp. 1-6, doi: 10.1109/ICCPCT.2015.7159473.

[5] Asst. Prof. T.A. More et al, “Smart Bank Locker Access System Using Iris, Fingerprints, Face Recognition Along with Password Authentication and Billing System”. (2015) Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 5, Issue 3, (Part - 3) March 2015.

[6] Ushie James Ogri, Donatus Enang Bassey Okwong, AkaisoEtim, “Design and construction of door locking security system using GSM”. (2013) International Journal Of Engineering And Computer ScienceISSN:2319-7242 Volume 2 Issue 7 (July 2013), Page No. 2235-2257

[7] A. B. Thabet and N. B. Amor, "Enhanced smart doorbell system based on face recognition". (2015)16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2015, pp. 373-377, doi: 10.1109/STA.2015.7505106.

[8] J. Chaikin and S. Kenter, “Biometric lock”, N. A Anu, and D. Bhatia, "A smart door access system using fingerprint biometric system,". (2008)International Journal ofMedical Engineering and Informatics, vol. 6, no. 3, pp. 274-280, 2014, doi: 10.1504/IJMEI.2014.063175

[9] M. A. Kader, M. Y. Haider, M. R. Karim, M. S. Islam, and M. M. Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint.,". (2016) International Conference on Innovations in Science, Engineering and Technology(ICISET)pp. 1-5, doi: 10.1109/ICISET.2016.7856484.

**REFERENCES(CONTD…)**

[10] Kamelia, Lia & Noorhassan, S.R. & Sanjaya, W. S. Mada & Mulyana,“Door-automation system using bluetooth-based android for mobile phone”. (2014) 9. 1759-1762