Smart Door Locking System with Intrusion Detection

by

Harshal Shirke	TE5-D-67
Tirth Thoria	TE5-D-75
Vivek Vadhiya	TE5-D-78

Under the Guidance of
Prof. Dhwaniket Kamble

DEPARTMENT OF INFORMATION TECHNOLOGY
SHAH AND ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR, MUMBAI-400088

2020-21

Approval for Project Report for IoT Lab semester VI

This project report entitled "SMART DOOR LOCKING SYSTEM WITH INTRUSION DETECTION" by Harshal Shirke, Tirth Thoria and Vivek Vadhiya is approved for semester VI in partial fulfillment of the requirement for the Sensor Network Lab of T.E. Engineering.

Examiners

1._____

2._____

Guide

1._____

2._____

ABSTRACT

In this digital age, IoT based systems have become a common thing in the society. Most of the electronics nowadays have some or the other form of IoT technology embedded in it. Leveraging various wireless technologies provided by IoT can aid at creating efficient and effective machines. One of the sensors, which is an IR receiver diode with the help of a remote can help in creating various wireless electronic smart devices. ESP8266, the Wi-Fi module provided by IoT as well, enables one to connect to the internet via Wi-Fi. Utilizing these two sensors in this project, we can create a secure IoT based Smart Door Locking system which can detect intruders as well, with the help of PIR sensor. This module provides an extra layer of security, overcoming the various challenges of traditional door locking systems.

CHAPTER 1: INTRODUCTION

Definition:

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc.

1.1 What is wireless sensor network

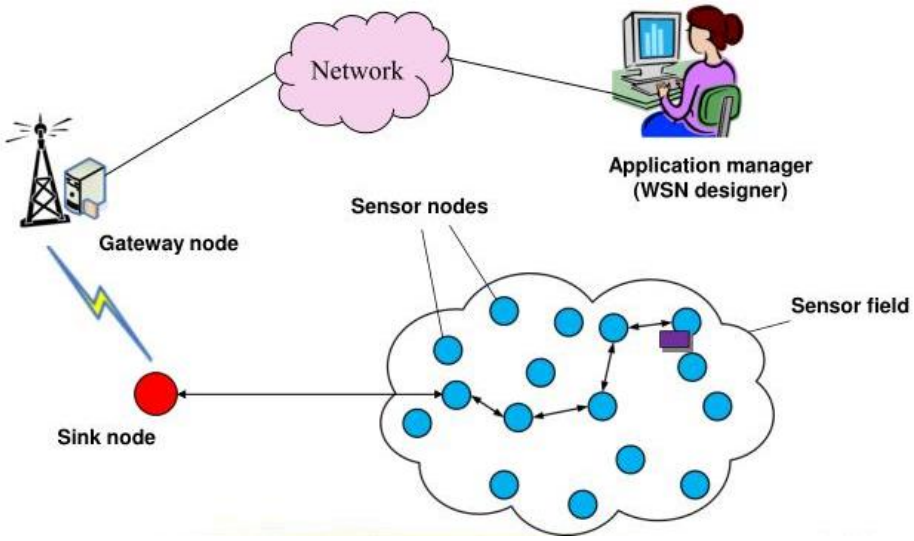

Fig. 1.1 WSN

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.

1.2 Enabling Technologies of WSN:

1.2.1 Components of WSN:

i. Sensors:

Sensors in WSN are used to capture the environmental variables and which are used for data acquisition. Sensor signals are converted into electrical signals.

ii. Radio Nodes:
It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

iii. WLAN Access Point:
It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

iv. Evaluation Software:
The data received by the WLAN Access Point is processed by a software called Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

According to technologists and researchers, Wireless Sensor Networks as an entity is an important technology for the twenty first century. Recent developments in MEMS Sensors (Micro Electro Mechanical System) and Wireless Communication has enabled cheap, low power, tiny and smart sensors, which can be deployed in a wide area and can be interconnected through wireless links and internet for various civilian and military applications.

A Wireless Sensor Network consists of Sensor Nodes (we will see about this later) that are deployed in high density and often in large quantities and support sensing, data processing, embedded computing and connectivity.

1.2.2 Motivation for Wireless Sensor Networks

The recent developments in engineering, communication and networking has led to new sensor designs, information technologies and wireless systems. Such advanced sensors can be used as a bridge between the physical world with the digital world.

Sensors are used in numerous devices, industries, machines and environment and help in avoiding infrastructure failures, accidents, conserving natural resources, preserving wildlife, increasing productivity, providing security etc.

The use of distributed sensor networks or systems has also been contributed by the technological advances in VLSI, MEMS and Wireless Communication.

With the help of modern semiconductor technology, you can develop more powerful microprocessors that are significantly smaller in size when compared to the previous generation

products. This miniaturization of processing, computing and sensing technologies has led to tiny, low-power and cheap sensors, controllers and actuators.

i. Elements of WSN

A typical wireless sensor network can be divided into two elements. They are:

- Sensor Node
- Network Architecture

ii. Sensor Node

A Sensor Node in a WSN consists of four basic components. They are:

- Power Supply
- Sensor
- Processing Unit
- Communication System

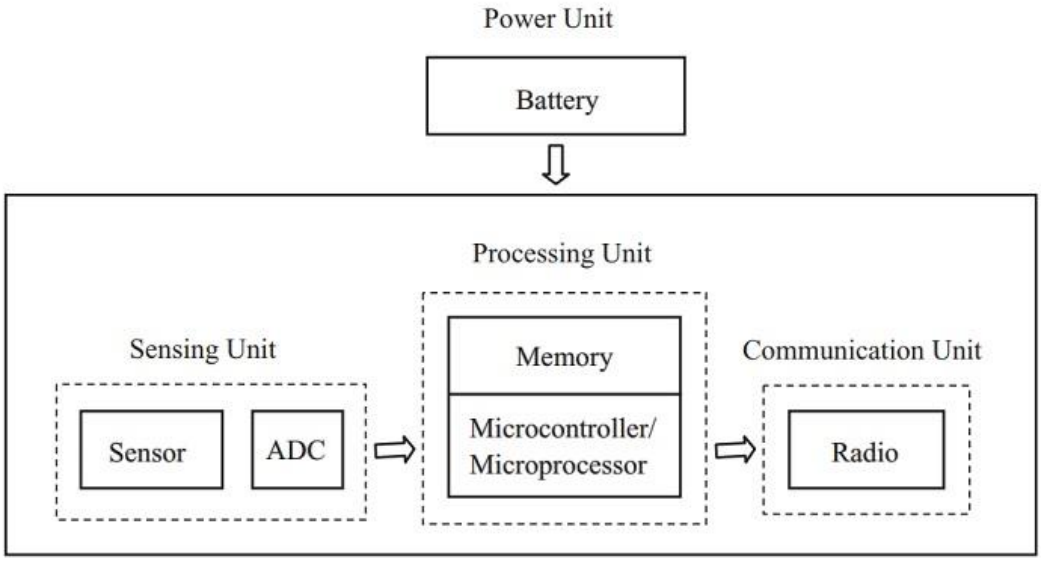

Fig. 1.2.1 Sensor Node

The sensor collects the analog data from the physical world and an ADC converts this data to digital data. The main processing unit, which is usually a microprocessor or a microcontroller, performs intelligent data processing and manipulation.

Communication system consists of a radio system, usually a short-range radio, for data transmission and reception. As all the components are low-power devices, a small battery like CR-2032, is used to power the entire system.

Despite the name, a Sensor Node consists of not only the sensing component but also other important features like processing, communication and storage units. With all these features, components and enhancements, a Sensor Node is responsible for physical world data collection, network analysis, data correlation and fusion of data from other sensors with its own data.

iii. Network Architecture

When a large number of sensor nodes are deployed in a large area to cooperatively monitor a physical environment, the networking of these sensor nodes is equally important. A sensor node in a WSN not only communicates with other sensor nodes but also with a Base Station (BS) using wireless communication.

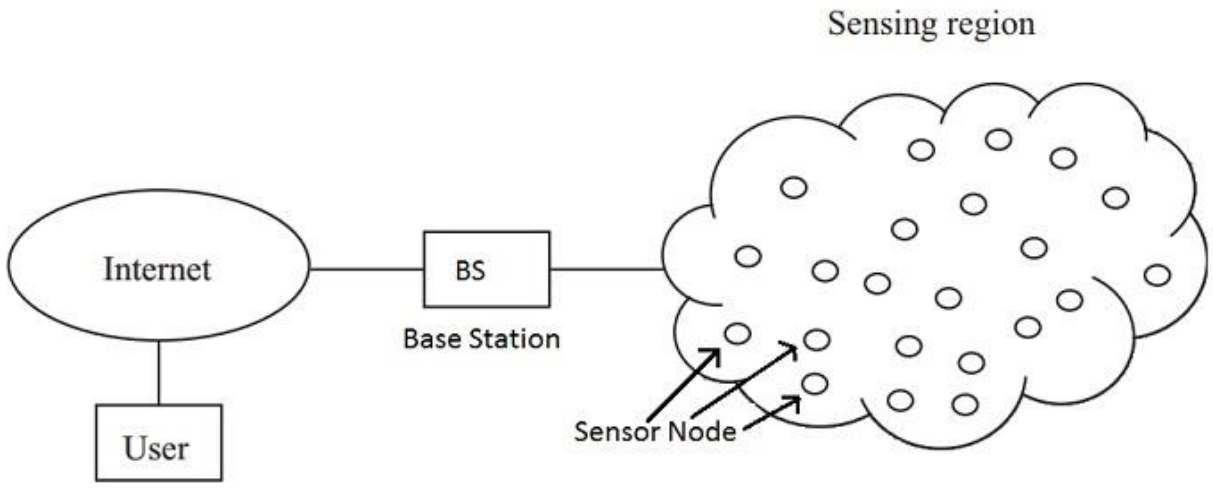

Fig. 1.2.2 Network Architecture

The base station sends commands to the sensor nodes and the sensor nodes perform the task by collaborating with each other. After collecting the necessary data, the sensor nodes send the data back to the base station.

A base station also acts as a gateway to other networks through the internet. After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using the internet.

If each sensor node is connected to the base station, it is known as Single-hop network architecture. Although long distance transmission is possible, the energy consumption for communication will be significantly higher than data collection and computation.

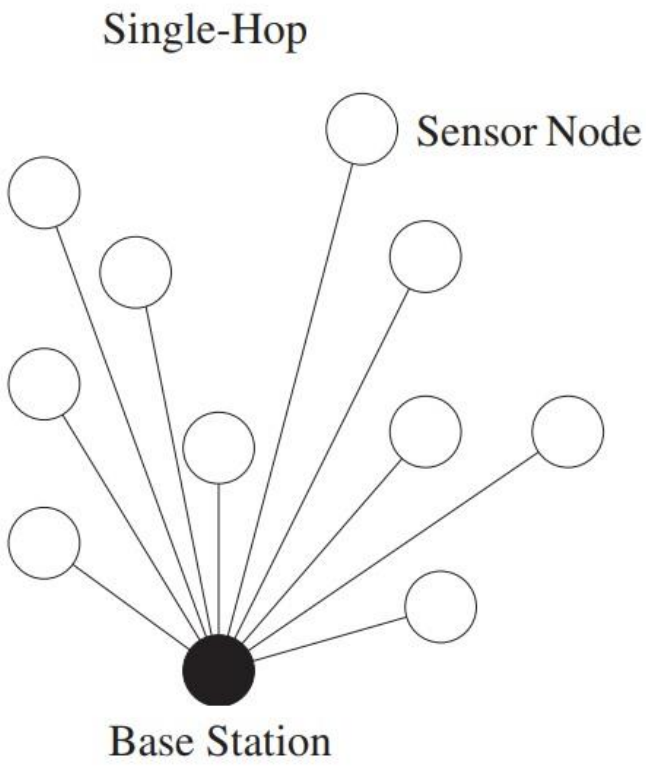

Fig. 1.2.3 Single-hop Network Architecture

Hence, Multi-hop network architecture is usually used. Instead of one single link between the sensor node and the base station, the data is transmitted through one or more intermediate node.

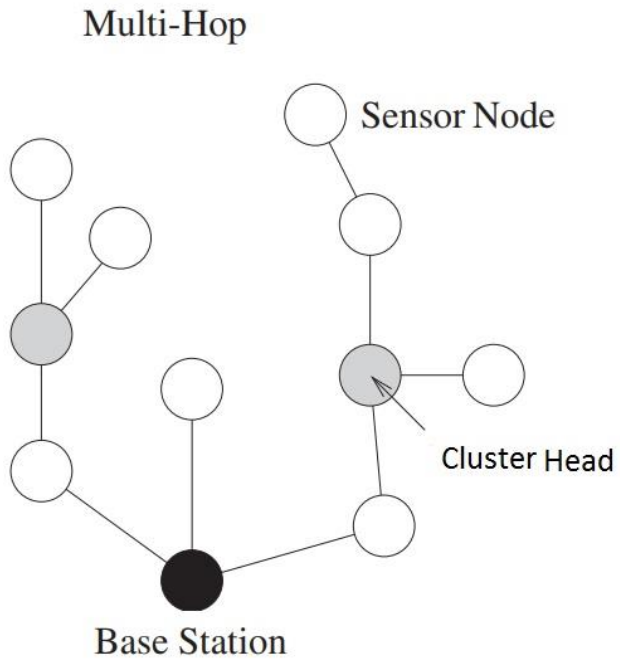

Fig.1.2.4 Multi-hop Network Architecture

This can be implemented in two ways. Flat network architecture and Hierarchical network architecture. In flat architecture, the base station sends commands to all the sensor nodes but the sensor node with matching query will respond using its peer nodes via a multi-hop path.

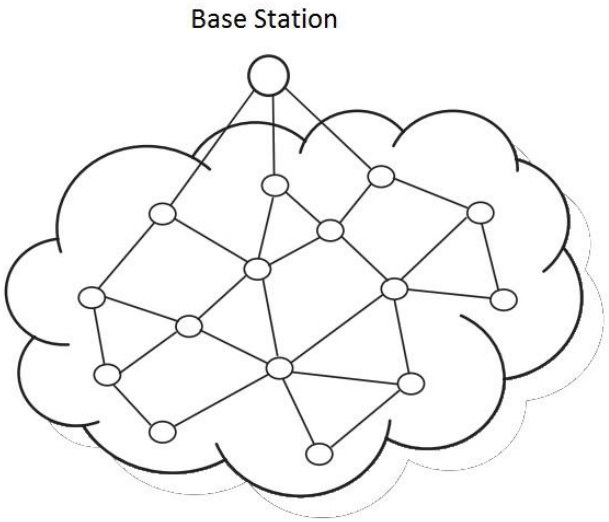

Fig. 1.2.5 Flat Network Architecture

In hierarchical architecture, a group of sensor nodes are formed as a cluster and the sensor nodes transmit data to corresponding cluster heads. The cluster heads can then relay the data to the base station.

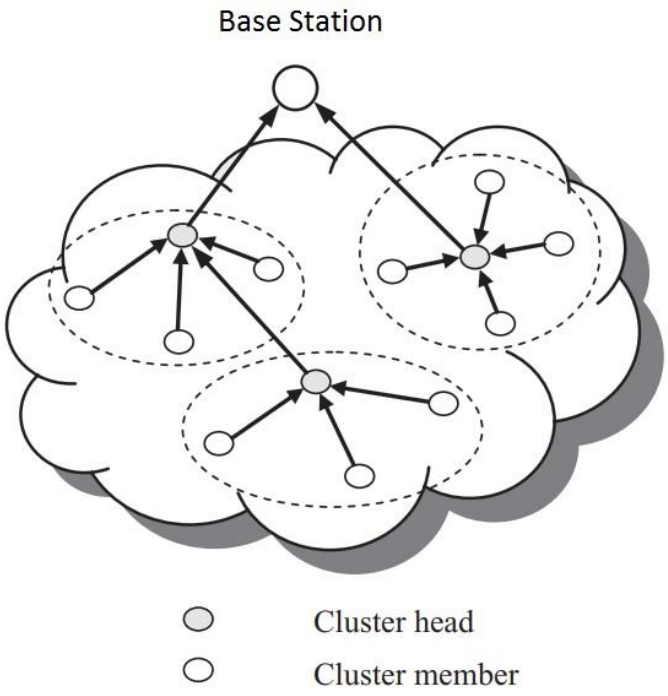

Fig. 1.2.6 Hierarchical Network Architecture

1.3 Classification of Wireless Sensor Networks

Wireless Sensor Networks are extremely application specific and are deployed according to the requirements of the application. Hence, the characteristics of one WSN will be different to that of another WSN.

Irrespective of the application, Wireless Sensor Networks in general can be classified into the following categories.

- Static and Mobile WSN
- Deterministic and Nondeterministic WSN

- Single Base Station and Multi Base Station WSN
- Static Base Station and Mobile Base Station WSN
- Single-hop and Multi-hop WSN
- Self – Reconfigurable and Non – Self – Configurable WSN
- Homogeneous and Heterogeneous WSN

Applications of Wireless Sensor Networks

- Theoretically speaking, the possible applications of Wireless Sensor Networks are unlimited. Some of the commonly used applications of wireless sensor networks are listed below.
- Air Traffic Control (ATC)
- Heating Ventilation and Air Conditioning (HVAC)
- Industrial Assembly Line
- Automotive Sensors
- Battlefield Management and Surveillance
- Biomedical Applications
- Bridge and Highway Monitoring
- Disaster Management
- Earthquake Detection
- Electricity Load Management
- Environment Control and Monitoring
- Industrial Automation
- Inventory Management
- Personal Health Care
- Security Systems
- Tsunami Alert Systems
- Weather Sensing and Monitoring

1.4 Network Topologies in WSN

We have already seen that a WSN can be either a single-hop network or a multi-hop network. The following are a few different network topologies that are used in WSNs.

A. Star Topology

In star topology, there is a single central node known as hub or switch and every node in the network is connected to this hub. Star topology is very easy to implement, design and expand. As all the data flows through the hub, it plays an important role in the network and a failure in the hub can result in failure of the entire network.

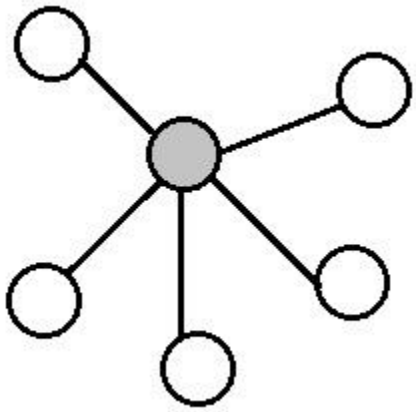

Fig. 1.4.1 Star Topology

B. Tree Topology

A tree topology is a hierarchical network where there is a single root node at the top and this node is connected to many nodes in the next level and this continues. The processing power and energy consumption is highest at the root node and keeps on decreasing as we go down the hierarchical order.

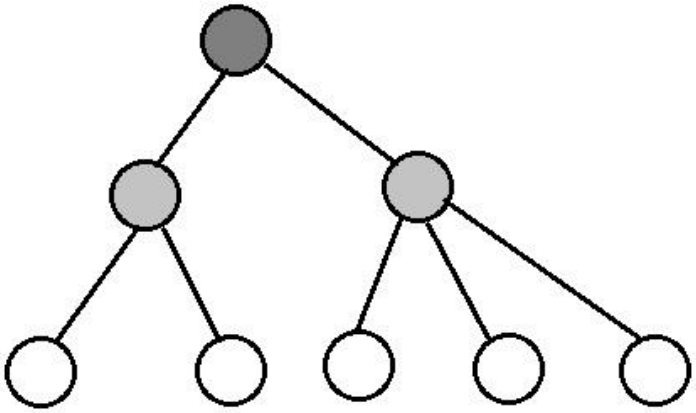

Fig. 1.4.2 Tree Topology

C. Mesh Topology

In mesh topology, apart from transmitting its own data, each node also acts as a relay for transmitting data of other connected nodes. Mesh topologies are further divided into Fully Connected Mesh and Partially Connected Mesh.

In fully connected mesh topology, each node is connected to every other node while in partially connected mesh topology, a node is connected to one or more neighbouring nodes.

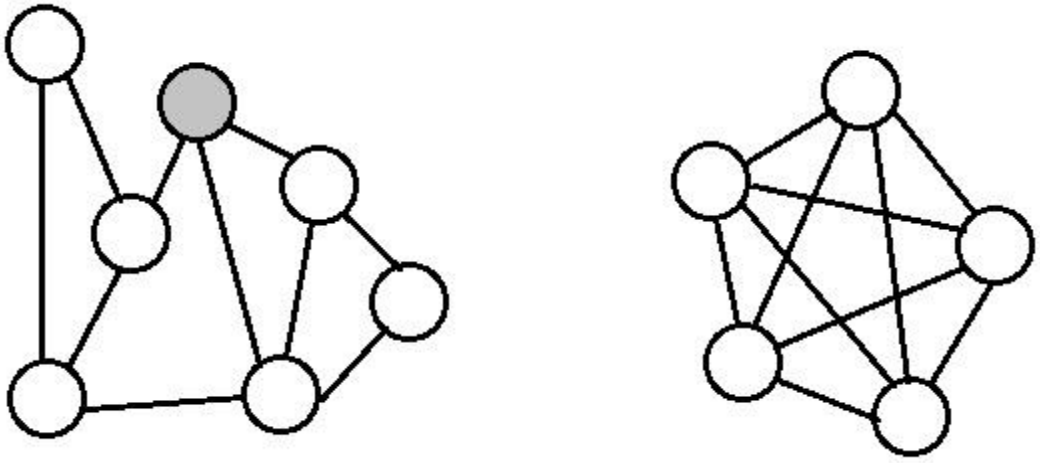

Fig. 1.4.3 Mesh Topology

D. Bus Topology

A bus topology consists of a single cable with the terminator at each end. All present nodes are connected to the single cable. There is no limit to the no: of nodes that can be attached to this network, but the no: of connected nodes can actually affect the performance of the network.

In a bus topology, one of the nodes acts as the server and transmits the data from one end to the other in a single direction. When the data reaches the extreme end, the terminator removes the data from the line.

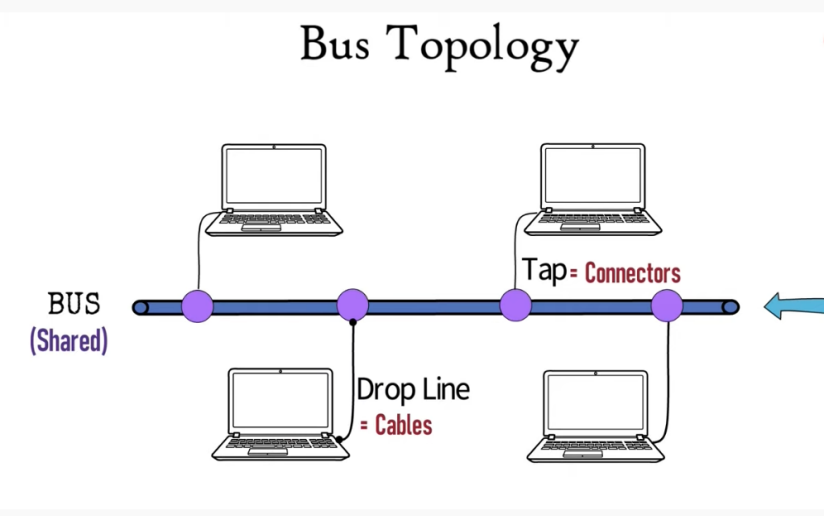

Fig. 1.4.4 Bus Topology

In a bus topology, one main cable acts as the backbone for the entire network. The bus topology carries the transmitted data along the cable. As the data reaches each node, the node checks the destination address (MAC/IP address) to see if it matches their address. If the address doesn't match, the node does nothing more. But if the node addresses match to the address contained in the data then they process the information.

Project Domain: Security

1.5 Security Issues in Wireless Sensor Networks

Due to inherent limitations in wireless sensor networks, security is a crucial issue. While research in WSN security is progressing at tremendous pace, no comprehensive document lists the security issues and the threat models which pose unique threats to the wireless sensor networks. Security goals in sensor networks depend on the need to know what we are going to protect. We determine four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (CIAA).

Confidentiality: It is the ability to conceal messages from a passive attacker, where the message communicated on sensor networks remains confidential. Integrity: It refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network. Authentication: It needs to know if the messages are from the node it claims to be from, determining the reliability of the message's origin. Availability: It is to determine if a node has the ability to use the resources and the network is available for the messages to move on. Attack types:

Subversion attack, Malicious Node, Wormhole, Sinkholes, Sybil, Routing loops, Link layer jamming, DoS and Node capture attack.

1.6 WSN design methodology

Since a large number of battery-driven nodes are deployed in a WSN, energy efficiency, fault tolerance, and scalability should be taken into account in designing a WSN architecture. These factors need to be well considered also in such a WSN as is assumed in the previous subsection. However, in the event of an emergency, urgent information must be transmitted as fast and reliable as possible, thus reliability and low latency are primary concerns. Therefore, we need a WSN architecture which satisfies requirements in both normal and emergency conditions. It means that a WSN operates on a data gathering scheme in the normal situation. Once an emergency occurs, an appropriate series of actions take place to deliver urgent information to the Base station. Those nodes which are not involved in the emergency should keep their normal operation. In summary, our design objectives of a WSN architecture for transmission of urgent sensor information are:

1) High reliability and low latency

The reliability and latency of transmission of urgent information are the most important issues. Urgent information should be differentiated from other information and receive preferential controls according to their importance. We consider that energy efficiency can be sacrificed to some extent for transmission of urgent information.

2) Self-organizing and localized behavior

The type and scale of an emergency and the number of simultaneous emergency events are unpredictable and dynamically change as time passes. A centralized architecture is infeasible in an emergency due to variations of traffic pattern and the level of congestion. Therefore, we need an architecture which is fully-distributed, self-organizing, and adaptive to dynamically changing conditions. As a consequence of localized reactions of each sensor node to the surroundings and local interactions among nodes, a globally-organized behavior of a WSN against detected emergencies emerges as a whole.

3) Simplicity

Since a node has limited computational capacity and a small amount of memory, mechanisms to support fast and reliable transmission of urgent information must be simple enough. Simplicity also contributes to low energy consumption and less programming errors. To satisfy the above requirements, we propose a design methodology to combine several simple control mechanisms

which function in different temporal and spatial levels. A typical control mechanism is arranged in accordance with their temporal and spatial effect. In general, larger the spatial area where a mechanism influences is, longer the time required to achieve effective control is. In the methodology, at least one mechanism is chosen for each of spatial levels.

1.7 Levels of Networking:

1) 802.11ah

Also known as Wi-Fi HaLow, 802.11ah defines operation of license-exempt networks in frequency bands below 1GHz (typically the 900 MHz band), excluding the TV White Space bands. In the U.S., this includes 908-928MHz, with varying frequencies in other countries. The purpose of 802.11ah is to create extended-range Wi-Fi networks that go beyond typical networks in the 2.4GHz and 5GHz space (remember, lower frequency means longer range), with data speeds up to 347Mbps. In addition, the standard aims to have lower energy consumption, useful for Internet of Things devices to communicate across long ranges without using a lot of energy. But it also could compete with Bluetooth technologies in the home due to its lower energy needs. The protocol was approved in September 2016 and published in May 2017.

2) 802.11ad

Approved in December 2012, 802.11ad is very fast - it can provide up to 6.7Gbps of data rate across the 60 GHz frequency, but that comes at a cost of distance – you achieve this only if your client device is situated within 3.3 meters (only 11 feet) of the access point.

3) 802.11ac (Wi-Fi 5)

Current home wireless routers are likely 802.1ac-compliant, and operate in the 5 GHz frequency space. With Multiple Input, Multiple Output (MIMO) – multiple antennas on sending and receiving devices to reduce error and boost speed – this standard supports data rates up to 3.46Gbps. Some router vendors include technologies that support the 2.4GHz frequency via 802.11n, providing support for older client devices that may have 802.11b/g/n radios, but also providing additional bandwidth for improved data rates.

4) 802.11n (Wi-Fi 4)

The first standard to specify MIMO, 802.11n was approved in October 2009 and allows for usage in two frequencies - 2.4GHz and 5GHz, with speeds up to 600Mbps. When you hear wireless LAN

vendors use the term “dual-band”, it refers to being able to deliver data across these two frequencies.

5) 802.11g

Approved in June 2003, 802.11g was the successor to 802.11b, able to achieve up to 54Mbps rates in the 2.4GHz band, matching 802.11a speed but within the lower frequency range.

6) 802.11a

The first “letter” following the June 1997 approval of the 802.11 standard, this one provided for operation in the 5GHz frequency, with data rates up to 54Mbps. Counterintuitively, 802.11a came out later than 802.11b, causing some confusion in the marketplace because people expected that the standard with the "b" at the end would be backward compatible with the one with the "a" at the end.

7) 802.11b

Released in September 1999, it’s most likely that your first home router was 802.11b, which operates in the 2.4GHz frequency and provides a data rate up to 11 Mbps. Interestingly, 802.11a products hit the market before 802.11a, which was approved at the same time but didn’t hit the market until later.

8) 802.11-1997

The first standard, providing a data rate up to 2 Mbps in the 2.4GHz frequency. It provided a range of a whopping 66 feet indoors (330 feet outdoors), so if you owned one of these routers, you probably only used it in a single room.

Pending Wi-Fi standards

1) 802.11aj

Also known as China Millimeter Wave, this defines modifications to the 802.11ad physical layer and MAC layer to enable operation in the China 59-64GHz frequency band. The goal is to maintain backward compatibility with 802.11ad (60GHz) when it operates in that 59-64GHz range and to operate in the China 45GHz band, while maintaining the 802.11 user experience. Final approval was expected in November 2017.

2) 802.11ak

There are some products in the home-entertainment and industrial-control spaces that have 802.11 wireless capability and 802.3 Ethernet function. The goal of this standard is to help 802.11 media provide internal connections as transit links within 802.1q bridged networks, especially in the areas of data rates, standardized security and quality-of-service improvements. It reached draft status in November 2017.

3) 802.11ax (Wi-Fi 6)

Known as High Efficiency WLAN, 802.11ax aims to improve the performance in WLAN deployments in dense scenarios, such as sports stadiums and airports, while still operating in the 2.4GHz and 5GHz spectrum. The group is targeting at least a 4X improvement in throughput compared to 802.11n and 802.11ac., through more efficient spectrum utilization. Approval is estimated to be in July 2019.

4) 802.11ay

Also known as Next Generation 60GHz, the goal of this standard is to support a maximum throughput of at least 20Gbps within the 60GHz frequency (802.11ad currently achieves up to 7Gbps), as well as increase the range and reliability. The standard is expected to be approved between September and November 2019.

5) 802.11az

Called Next Generation Positioning (NGP), a study group was formed in January 2015 to address the needs of a "Station to identify its absolute and relative position to another station or stations it's either associated or unassociated with." The goals of the group would be to define modifications to the MAC and PHY layers that enable "determination of absolute and relative position with better accuracy with respect to the Fine Timing Measurement (MTM) protocol executing on the same PHY-type, while reducing existing wireless medium use and power consumption, and is scalable to dense deployments." The current estimate on approval of this standard is March 2021.

6) 802.11ba

Otherwise known as "Wake-Up Radio" (WUR), this isn't a crazy morning zoo-crew thing, but rather a new technology aimed at extending the battery life of devices and sensors within an Internet of Things network. The goal of the WUR is to "greatly reduce the need for frequent

recharging and replacement of batteries while still maintaining optimum device performance." This is currently expected to be approved in July 2020.

CHAPTER 2: LITERATURE REVIEW

Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy, [4]. This venture is proposed to build up a savvy locking framework utilizing the Internet of Things. Utilizing conventional keyed locks is basic since the start of humankind, anyway there is a high risk of keys being lost or getting into inappropriate hands. Subsequently, many individuals prefer biometric locks over traditional keyed locks to improve the security of their homes or workplaces. In contrast to the conventional lock, a cutting-edge biometric lock requires no key to bolt or open the door and instead uses a biometric sensor. Their project is an Arduino nano based adaptable working device that provides physical security utilizing the biometric sensor which is available in a smartphone.

Jeong-ile Jeong, [5]. The proposed method in this study uses the IoT technology and the application of smartphone communication technology to conventional devices (door lock) to open or close a door remotely through authentication. In particular, this study proposes the Smart Door Lock System based security enhancement plan for the safety issue caused by the physical key used in unmanned automation machines, such as ATMs, KIOSKs, and vending machines.

Dae Gyu Seo et al, [6]. In this paper, the Digital DoorLock by Internet of Things (DDiT) is introduced. In order to implement DDiT, an integrated micro-controller platform, Arduino is used to control an existing digital door lock and an android type smart phone is adopted as a mobile platform. One of the advantages of DDiT is that it can be added to an existing digital door lock and a smartphone application is used as a digital key. Owing to the smartphone application, several other types of applications could also be made. Therefore, DDiT could be used effectively and conveniently in ordinary homes as well as in high security applications such as in hotels, institutes, and companies.

Sanjana Prasad, P. Mahalakshmi, A.John Clement Sunder, R Swathi, [7]. This paper deals with the design and implementation of Smart surveillance monitoring system using Raspberry pi and PIR sensor for mobile devices. It increases the usage of mobile technology to provide essential security to our homes and for other control applications . The proposed home security system captures information and transmits it via a 3G Dongle to a Smart phone using web application. Raspberry pi operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video and records it for future playback.

Trio Adiono et al, [8]. This paper covers the design of a prototype for IoT and GPS enabled door lock systems. The aim of this research is to design a door lock system that does not need manual input from the user for convenience purposes while also remaining secure.

Firza Fadlullah Asman, Endi Permata, Mohammad Fatkhurrokhman, [9]. This study has aimed at creating a prototype house with an automatic safety system installed. This system can be controlled with either an android or iOS application. This paper has proposed the use of a solenoid lock which can be used for locking doors electronically. This paper also shows that a PIR sensor can be used to detect motion around the security zone.

Dr Abbas M. Al. Bakry, Rajaa D. Resan, [10]. Security is considered an important issue especially in designing smart homes. In this paper, they have focused on an authentication problem in designing smart door locks by using RC4 cipher stream for encryption/decryption of smart-phone information which contains unique data. This work contains two main parts, Android application (remote control) and control circuit using Arduino UNO, also the communication medium is Bluetooth technology used transceiver information and commands in this work. The main purpose of the design smart door lock using RC4 algorithm is to enforce security based on personal smart-phone information, and the results show more strength authentication for access in real time.

CHAPTER 3: PROBLEM STATEMENT

In the current digital age, security of highly sensitive places is of utmost importance. Newer and newer technologies enable the thieves to get past most of the digital security hurdles. This has led to the need for an effective IoT based solution to the area of security for doors. In order to safeguard locations such as banks, ATMs, financial institutions, government offices, etc, it is important to implement an effective security barrier so that intruders cannot access the money/ documents. Implementation of the same using various sensors provided by IoT along with various wireless sensors can prove effective in this scenario.

CHAPTER 4: OBJECTIVES

- To overcome the shortcomings of traditional lock systems.
- To create a secure door locking system.
- To notify users of any intruders.
- To add an extra layer of security using the PIR motion sensor.
- To create a cost effective solution for securing sensitive facilities.
- To leverage ThingSpeak cloud for easy interfacing with the lock using wireless technologies.

CHAPTER 5: SYSTEM DETAILS

Working

1. The microcontroller used for the project is Arduino UNO. The wireless sensors used for the project are ESP8266 and IR Receiver Diode. A PIR sensor for detecting motions is used. Some LEDs, along with LCD and a 12V DC Solenoid Lock are used for output purposes.
2. Initially, the device will be in "locked" state, ie, the Solenoid Lock would be activated and the LCD will display the "Enter PIN:" message. The PIR sensor will be active, ie, whenever a person loiters around the apparatus, in this case a security door, the PIR sensor will detect the movement and the Red LED will start blinking. Whenever the movement stops, the LED stops blinking.
3. The owner will have a remote control, from which he can perform a number of actions. The first action is disabling the motion detector. This can be performed by pressing the power button on the remote control. As soon as the user presses the power button, the PIR Sensor stops detecting any motions and the Green LED lights up. This will indicate it is safe to approach the apparatus.
4. The LCD will constantly ask for the PIN while the device is in locked state. Whenever the user enters an incorrect PIN and presses the submit button, the Red LED will blink for a bit and the message "Wrong Password!!" will display on LCD for some time.
5. When the user enters the correct PIN and presses the submit button, the LCD will display the message "Door Unlocked!!" and the Solenoid Lock will open, along with disabling the PIR sensor, if not already disabled, thus giving the owner access through the door. The Green LED will also light up, thus having multipurposes, one indicating that the PIR sensor is disabled, and the other being that the door is unlocked.
6. Whenever the person wishes to lock the door again, they just have to press the power button, which re-enables the solenoid lock, and the LCD starts asking for PIN again. The PIR sensor is also reactivated, thus locking the door securely.
7. The ESP8266 sensor can connect to a Wifi network and transmit any break-in attempts detected by the PIR sensor to the ThingSpeak Cloud, which can be accessed by the owner.

CHAPTER 6: CIRCUIT DIAGRAM

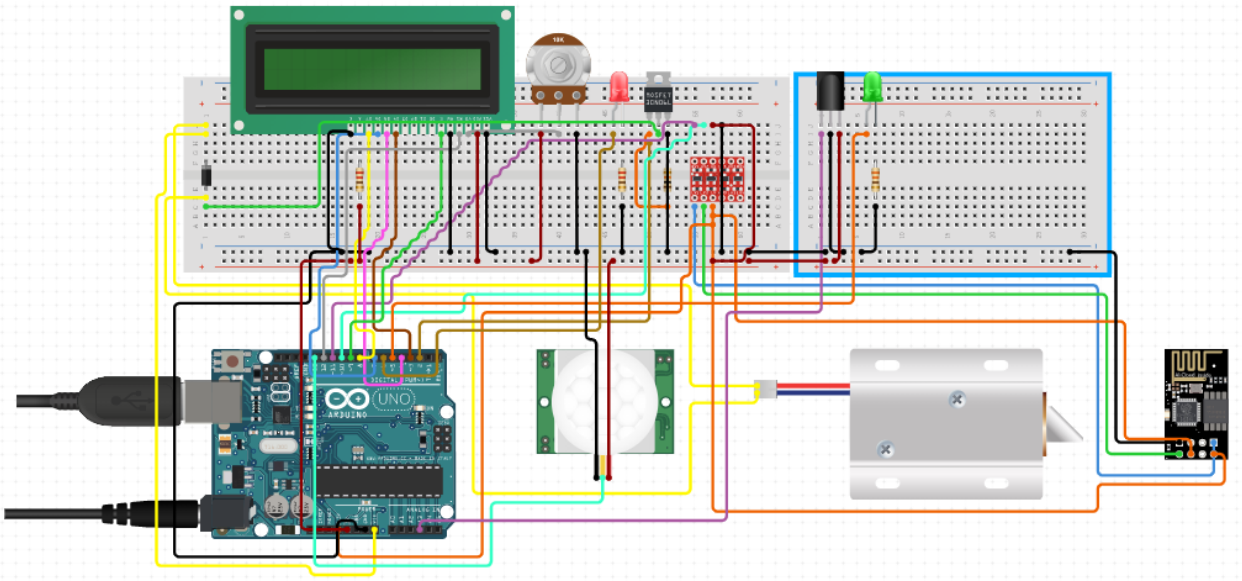

Fig. 6.1 Smart Door Locking System With Intrusion Detection

CHAPTER 7: HARDWARE AND SOFTWARE REQUIREMENTS

7.1 Hardware Requirements:

1. Arduino Uno

Arduino/Genuino Uno is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.. You can tinker with your UNO without worrying too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again.

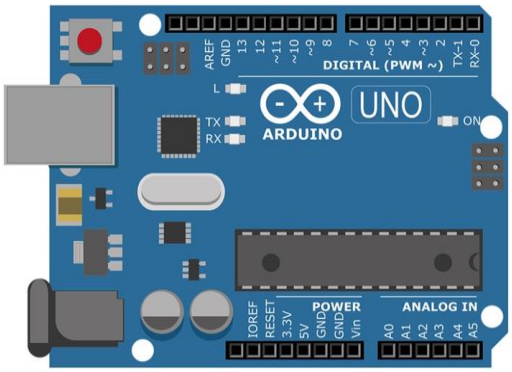

Fig. 7.1.1 Arduino Uno

2. PIR Sensor

PIR sensor detects a human being moving around within approximately 10m from the sensor. This is an average value, as the actual detection range is between 5m and 12m.PIR is fundamentally made of a pyro electric sensor, which can detect levels of infrared radiation. For numerous essential projects or items that need to discover when an individual has left or entered the area. PIR sensors are incredible, they are flat control and minimal effort, have a wide lens range, and are simple to interface with.

Fig. 7.1.2 PIR Sensor

3. IR Receiver Diode

Infrared receivers are also called as infrared sensors as they detect the radiation from an IR transmitter. IR receivers come in the form of photodiodes and phototransistors. Infrared Photodiodes are different from normal photo diodes as they detect only infrared radiation. Different types of IR receivers exist based on the wavelength, voltage, package, etc. When used in an infrared transmitter – receiver combination, the wavelength of the receiver should match with that of the transmitter.

Fig. 7.1.3 IR Receiver Diode

4. ESP8266 Wifi Module

ESP8266 is Wi-Fi enabled system on chip (SoC) module developed by Espressif system. It is mostly used for the development of the Internet of Things (IoT) embedded applications. The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability produced by Shanghai-based Chinese manufacturing company Espressif Systems. The ESP8266 is capable of either hosting an application or offloading all the Wi-Fi networking functions from another application processor. Each ESP8266 Wi-Fi module comes pre-programmed with an AT command set firmware, now you can simply hook this up to your Arduino device and get as much Wi-Fi ability as a Wi-Fi Shield offers.

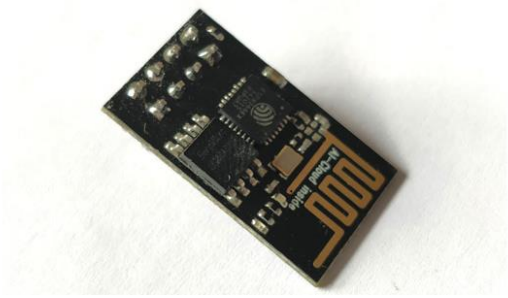

Fig. 7.1.4 ESP8266 Wifi Module

5. 12VDC Lock-Style Solenoid

Solenoids are basically electromagnets: they are made of a big coil of copper wire with an armature (a slug of metal) in the middle. When the coil is energized, the slug is pulled into the center of the coil. This makes the solenoid able to pull from one end. This solenoid in particular is nice and strong, and has a slug with a slanted cut and a good mounting bracket. It's basically an electronic lock, designed for a basic cabinet or safe or door. Normally the lock is active so you can't open the door because the solenoid slug is in the way. It does not use any power in this state. When 9-12VDC is applied, the slug pulls in so it doesn't stick out anymore and the door can be opened. The solenoids come with the slanted slug as shown above, but you can open it with the two Phillips-head screws and turn it around so it's rotated 90, 180 or 270 degrees so that it matches the door you want to use it with.

Fig. 7.1.5 12VDC Lock-Style Solenoid

6. General LEDs

LED, in full light-emitting diode, in electronics, a semiconductor device that emits infrared or visible light when charged with an electric current. Visible LEDs are used in many electronic devices as indicator lamps, in automobiles as rear-window and brake lights, and on billboards and signs as alphanumeric displays or even full-colour posters. Infrared LEDs

are employed in autofocus cameras and television remote controls and also as light sources in fibre-optic telecommunication systems.

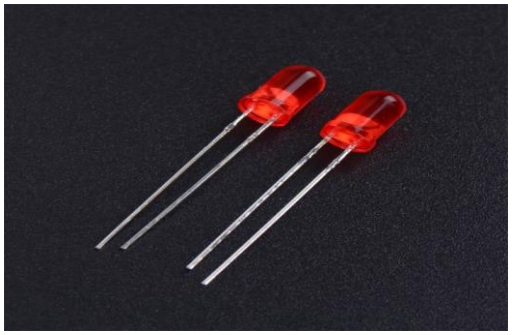

Fig. 7.1.6 General LEDs

7. 16x2 LCD

The term LCD stands for liquid crystal display. It is one kind of electronic display module used in an extensive range of applications like various circuits & devices like mobile phones, calculators, computers, TV sets, etc. These displays are mainly preferred for multi-segment light-emitting diodes and seven segments. The main benefits of using this module are inexpensive; simply programmable, animations, and there are no limitations for displaying custom characters, special and even animations, etc.

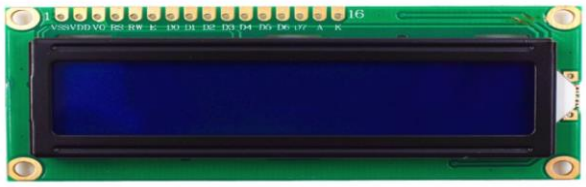

Fig. 7.1.7 16x2 LCD

8. IR Remote

In electronics, a remote control or clicker is an electronic device used to operate another device from a distance, usually wirelessly. In consumer electronics, a remote control can be used to operate devices such as a television set, DVD player or other home appliance. A remote control can allow operation of devices that are out of convenient reach for direct operation of controls. They function best when used from a short distance. This is primarily a convenience feature for the user. In some cases, remote controls allow a person to operate a device that they otherwise would not be able to reach, as when a garage door opener is triggered from outside.

Fig. 7.1.8 IR Remote

7.2 Software Requirements:

1. Tinkercad

Tinkercad is a browser-based 3D design and modeling program created to provide a way for a variety of users (beginners to experts) to create projects. Conventional CAD software options are not only expensive, but they're also often quite complicated to learn. These programs often have many features that you won't even use for something as simple as a custom case.

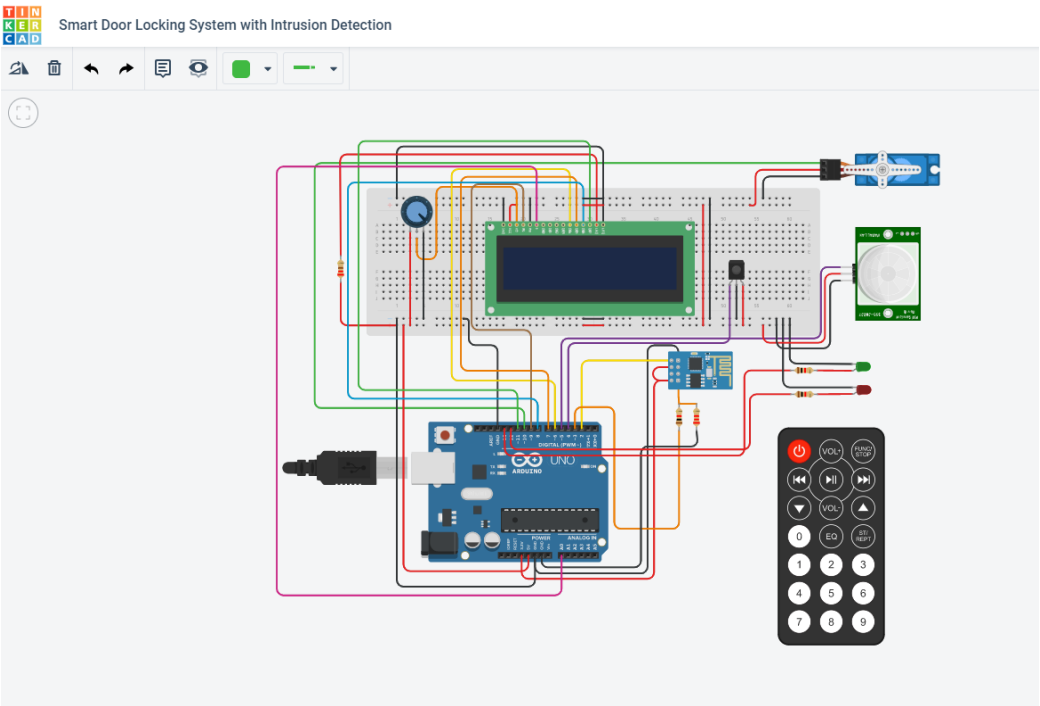

Fig. 7.2.1 Tinkercad

2. Arduino IDE

Arduino IDE is an open source software that is mainly used for writing and compiling the code into the Arduino Module.It is an official Arduino software, making code compilation so easy that even a common person with no prior technical knowledge can get their feet wet with the learning process.It is easily available for operating systems like MAC, Windows, Linux and runs on the Java Platform that comes with inbuilt functions and commands that play a vital role for debugging, editing and compiling the code in the environment.

A range of Arduino modules available including Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Micro and many more.The main code, also known as a sketch, created on the IDE platform will ultimately generate a Hex File which is then transferred and uploaded in the controller on the board.The IDE environment mainly contains two basic parts: Editor and Compiler where former is used for writing the required code and later is used for compiling and uploading the code into the given Arduino Module.This environment supports both C and C++ languages.

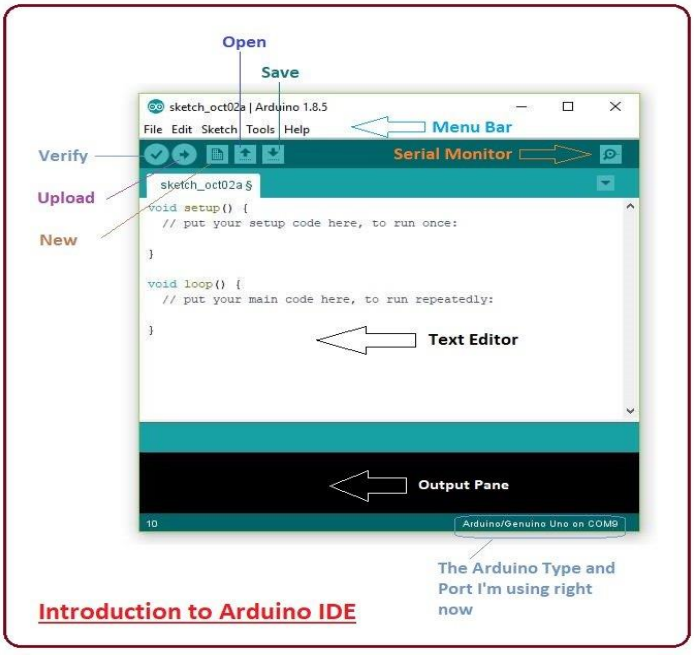

Fig. 7.2.2 Arduino IDE

3. C (Programming Language)

C is a general-purpose programming language that is extremely popular, simple, and

flexible to use. It is a structured programming language that is machine-independent and extensively used to write various applications, Operating Systems like Windows, and many other complex programs like Oracle database, Git, Python interpreter, and more.

CHAPTER 8: IMPLEMENTATION

Code:

```
#include <LiquidCrystal.h>
#include <IRremote.h>
#include <Servo.h>

// Definition of PINS
#define RS 9
#define E A0
#define D4 6
#define D5 7
#define D6 8
#define D7 11
#define GLED 13
#define RLED 12
#define PIR 5
#define IR 4
#define SERVO 10

const long int POWER = 0xFD00FF;
const long int ZERO = 0xFD30CF;
const long int ONE = 0xFD08F7;
const long int TWO = 0xFD8877;
const long int THREE = 0xFD48B7;
const long int FOUR = 0xFD28D7;
const long int FIVE = 0xFDA857;
const long int SIX = 0xFD6897;
const long int SEVEN = 0xFD18E7;
const long int EIGHT = 0xFD9867;
const long int NINE = 0xFD58A7;
const long int ENTER = 0xFDA05F;

LiquidCrystal lcd = LiquidCrystal(RS, E, D4, D5, D6, D7);
Servo servo;
int val = 0;
bool deactivated = false;
bool unlocked = false;
```

```
IRrecv irrecv(IR);
decode_results results;

int count = 0;
int PASSWORD[4] = {1, 2, 3, 4};
int buffer[4] = {0, 0, 0, 0};

void setup() {
  lcd.begin(16, 2);
  pinMode(RLED, OUTPUT);
  pinMode(GLED, OUTPUT);
  pinMode(PIR, INPUT);
  irrecv.enableIRIn();
  servo.attach(SERVO);
  Serial.begin(9600);
}

void loop() {
  if (unlocked) {
    lcd.setCursor(0, 0);
    lcd.print("Door");
    lcd.setCursor(0, 1);
    lcd.print("Unlocked!!");
    servo.write(-90);
  } else {
    lcd.setCursor(0, 0);
    lcd.print("Enter PIN:");
  }

  val = digitalRead(PIR);
  if (val && !deactivated) {
    blinkRed();
  } else {
    digitalWrite(RLED, LOW);
  }
  if (deactivated) {
    digitalWrite(GLED, HIGH);
  } else {
    digitalWrite(GLED, LOW);
  }
```

```
if (irrecv.decode( & results)) {
  switch (results.value) {
  case POWER:
    deactivated = !deactivated;
    if (unlocked) {
      unlocked = !unlocked;
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Door");
      lcd.setCursor(0, 1);
      lcd.print("Locked!!");
      digitalWrite(RLED, HIGH);
      delay(1000);
      digitalWrite(RLED, LOW);
      lcd.clear();
      servo.write(90);
    }
    break;
  case ONE:
    writePin(1);
    break;
  case TWO:
    writePin(2);
    break;
  case THREE:
    writePin(3);
    break;
  case FOUR:
    writePin(4);
    break;
  case FIVE:
    writePin(5);
    break;
  case SIX:
    writePin(6);
    break;
  case SEVEN:
    writePin(7);
    break;
```

```
    case EIGHT:
      writePin(8);
      break;
    case NINE:
      writePin(9);
      break;
    case ZERO:
      writePin(0);
      break;
    case ENTER:
      lcd.clear();
      if (isEqual(PASSWORD, buffer)) {
        unlocked = true;
        deactivated = true;
      } else {
        unlocked = false;
        lcd.setCursor(0, 0);
        lcd.print("Wrong");
        lcd.setCursor(0, 1);
        lcd.print("Password!!");
        count = 0;
        blinkRed();
        delay(400);
        lcd.clear();
      }
      break;
    default:
      Serial.println("Unknown Key");
      break;
    }
    irrecv.resume();
  }
  delay(100);
}

void writePin(int num) {
  if (!unlocked) {
    if (count == 4) {
      count = -1;
      lcd.clear();
```

```
    } else {
      buffer[count] = num;
      lcd.setCursor(count, 1);
      lcd.print(num);
    }
    count++;
  }
}

bool isEqual(int a[], int b[]) {
  bool flag = true;
  for (int i = 0; i < 4; i++) {
    if (PASSWORD[i] != buffer[i]) {
      flag = false;
      break;
    }
  }
  return flag;
}

void blinkRed() {
  digitalWrite(RLED, HIGH);
  delay(100);
  digitalWrite(RLED, LOW);
}
```

CHAPTER 9: TESTING

Test Case 1:

Door is **locked** and motion **is not** detected. PIR sensor is **enabled**.

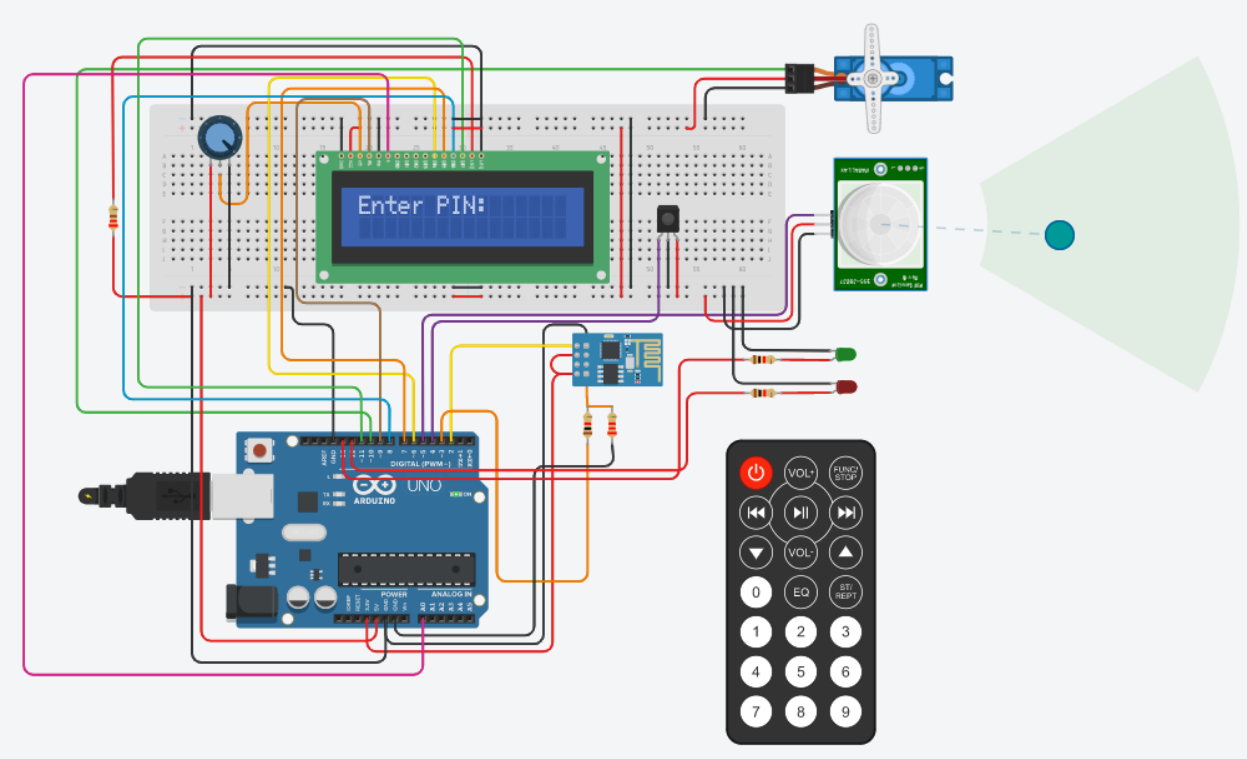

Fig. 9.1 Test Case 1

Test case 2:

Door is **locked** and motion **is** detected. PIR sensor is **enabled.**

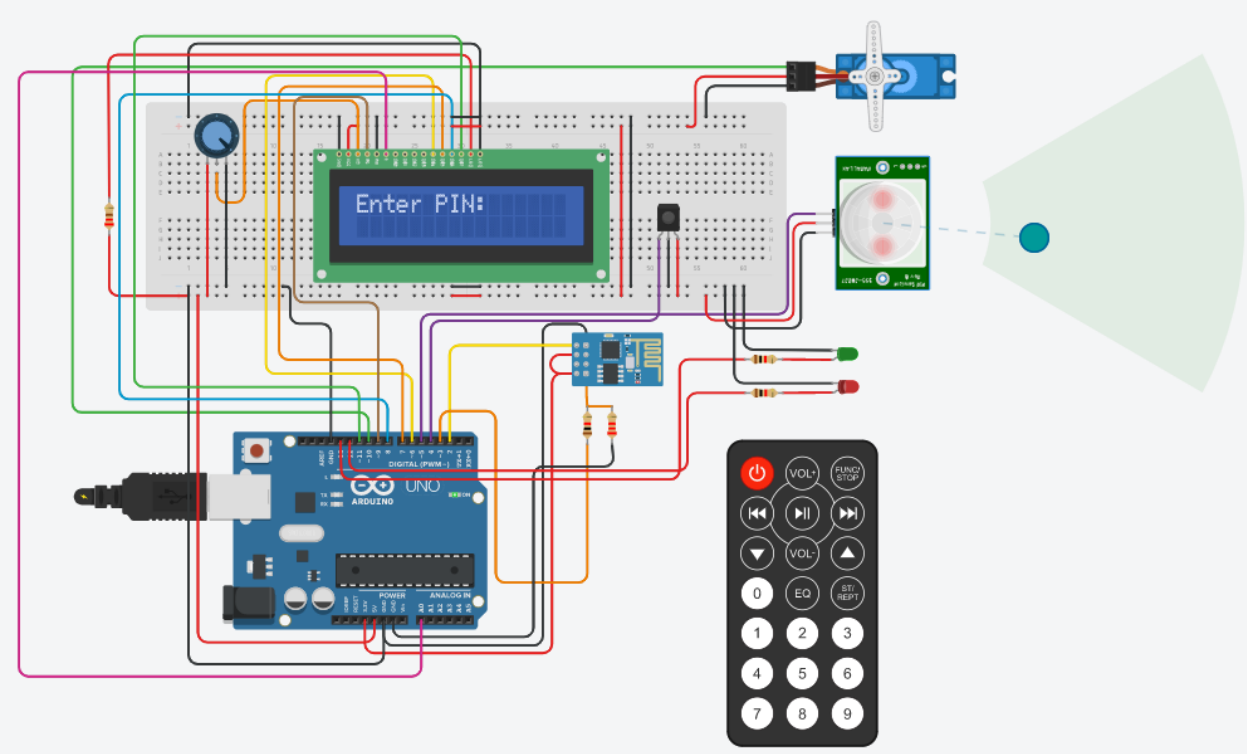

Fig. 9.2 Test Case 2

Test Case 3:

Door is **locked** and motion **is not** detected. PIR sensor is **enabled.** Password entered is **incorrect.**

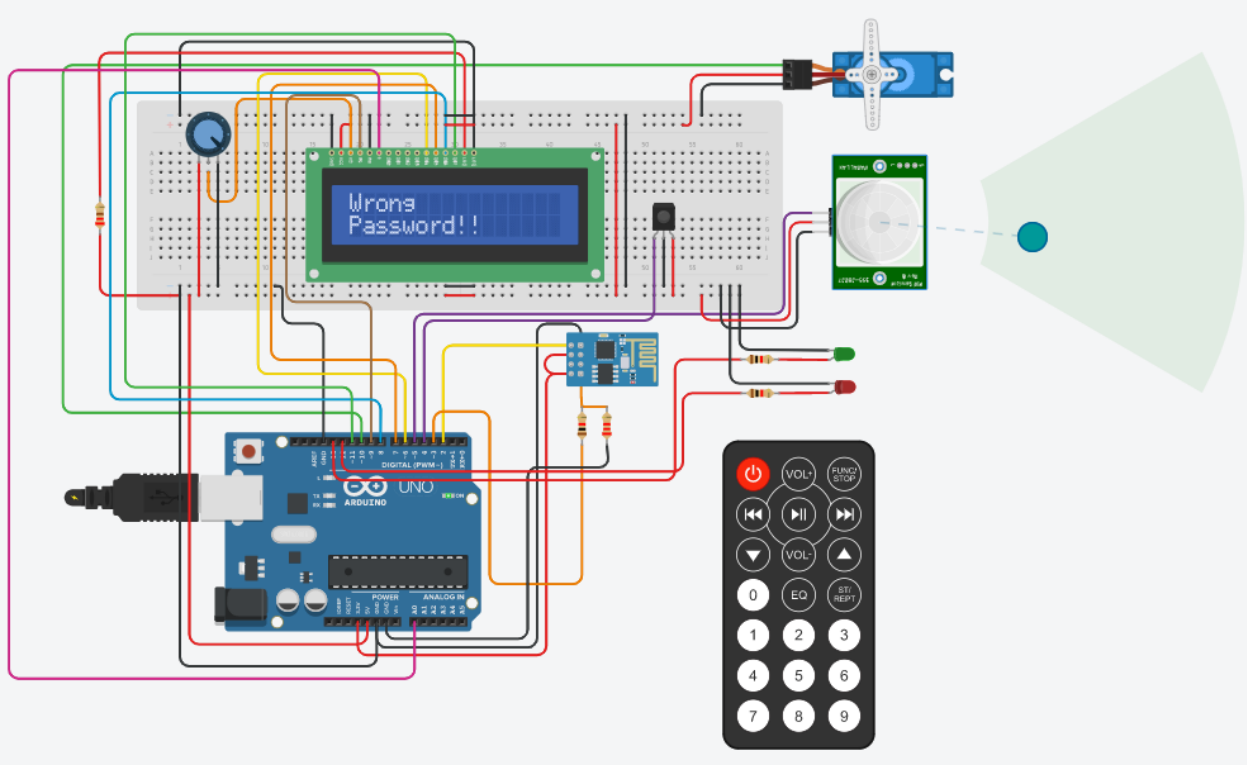

Fig. 9.3 Test Case 3

Test Case 4:

Door is **locked** and motion **is** detected. PIR sensor is manually **disabled.**

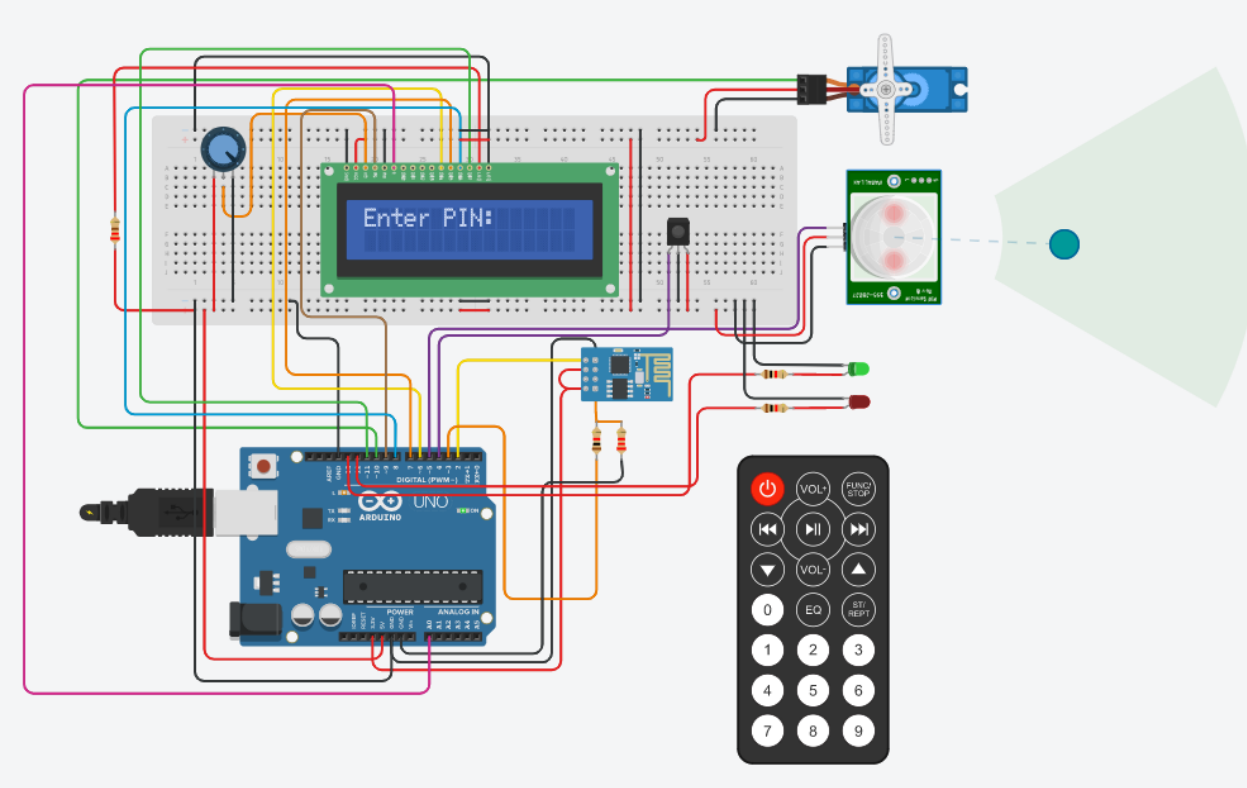

Fig. 9.4 Test Case 4

Test Case 5:

Password entered is **correct.** Door is **unlocked** and motion is **not** detected. PIR sensor is **disabled.**

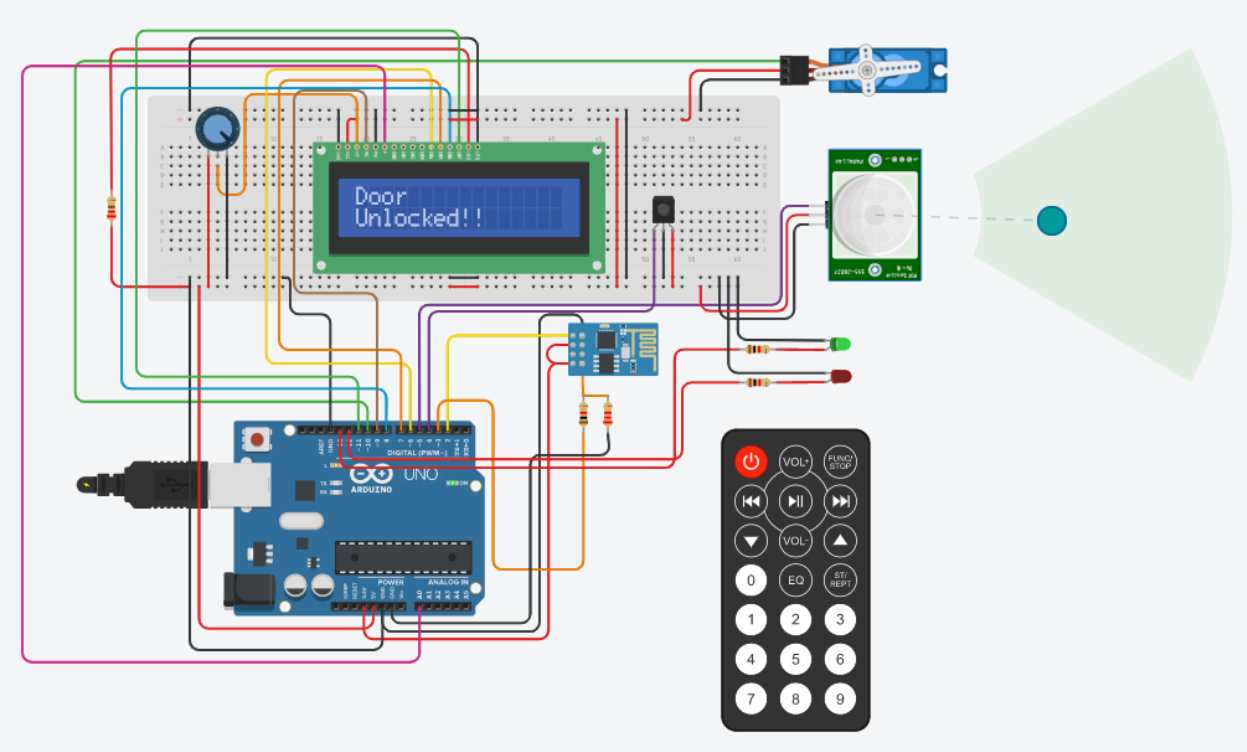

Fig. 9.5 Test Case 5

Test Case 6:

Door was **unlocked.** Power button **is** pressed.

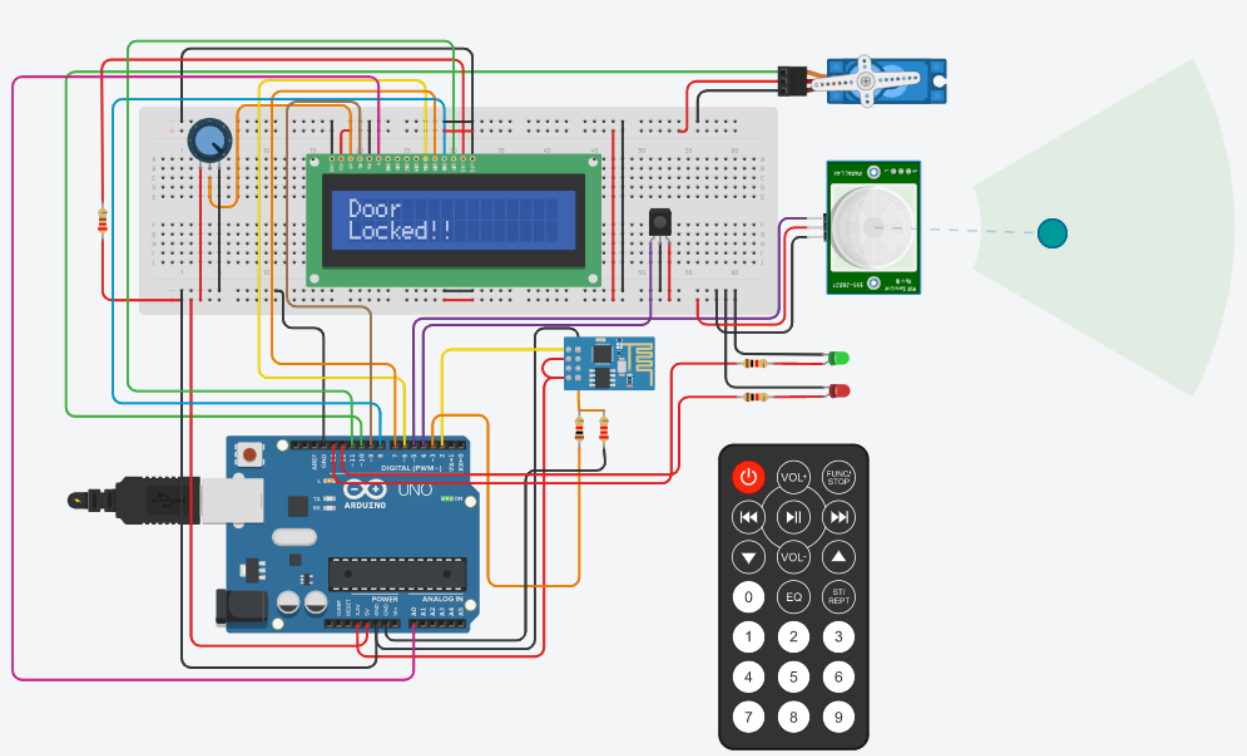

Fig. 9.6 Test Case 6

CHAPTER 10: RESULTS

1. In test case 1, the outcome will be the LCD staying at the “Enter PIN:” message. No motion is detected so the Red LED will remain OFF.

2. In test case 2, the door is locked so the LCD will stay on the “Enter PIN:” message. Motion is detected, so the Red LED will blink as long as the motion is being detected by the PIR sensor.

3. In test case 3, the password entered is incorrect. Thus a “Wrong Password!!” message is displayed on the LCD. The user cannot bypass the lock without entering the correct password. The PIR sensor is enabled so the movements will be still detected and notified.

4. In test case 4, the PIR sensor is manually disabled by the user. This is done via pressing the POWER button on the remote. After doing so, the Green LED will light up, thus indicating that the PIR sensor will not alert the owner even if the motion is detected. The Red LED will not blink either in case of motion detection.

5. In test case 5, the user enters the correct password. The password is accepted and the Solenoid Lock (Servo Motor in Simulation) will unlock. The Green LED will also light up as long as the door is unlocked, which indicates that the PIR sensor will stop working as long as the door is unlocked.

6. In test case 6, the door was already unlocked. The user presses the POWER button, doing so locks the door again. The PIR sensor is reactivated. Door is in a locked state again, which means the PIR sensor will start detecting and reporting the motions again.

CHAPTER 11: CONCLUSION AND FUTURE SCOPE

Conclusion:

Security issues are becoming more important and developed day by day. Dedicated technology is being made by hackers and intruders to overcome the various digital locking mechanisms. Thus, an attempt at creating an enhanced door lock system using IoT and wireless networking is made. An extra layer of security is also added in the form of motion detection with the help of PIR sensor. The entire control of the apparatus can be wirelessly done with the help of a remote by the owner. The owner is also made aware of the intruders via ThingSpeak platform with the help of ESP8266 Wi-Fi shield. Various scenarios and test cases of intrusion activities are taken into consideration and accordingly actions corresponding to those events are designed and implemented in the project. The main reason behind this implementation is to provide a secure and enhanced form of security accessible to everyone.

Future Scope:

Due to the nature of the project, it is possible to add various modules. Various other wireless sensors can be included in the project. Notable among those are GSM and GPS modules. In this project, a GSM module can be installed. The module can enable one to connect to any mobile network and send / receive SMS and other communications. If a GSM module is used in this project, then the owner can be notified about intrusions via SMS as well. This eliminates the need of a constant Wi-Fi connection which is required by the ESP8266 module. The other components which can be used as an alternative can be buzzers and speakers. Whenever an intrusion is detected, the speakers can sound alarms and notify the surrounding guards about any intrusions.

REFERENCES

[1] Author Name, “Paper/Website Link”, published/website.

[2] Shivam Kumar, “Wireless Sensor Network (WSN) - GeeksforGeeks”, website.

[3] Anonymous, “https://www.electronicshub.org/wireless-sensor-networks-wsn”,website.

[4] Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy, “Smart Door Locking System using IoT”, published.

[5] Jeong-ile Jeong, “A Study on the IoT Based Smart Door Lock System”, published.

[6] Dae Gyu Seo et al, “ Design and Implementation of Digital Door Lock by IoT”, published.

[7] Sanjana Prasad, P. Mahalakshmi, A.John Clement Sunder, R Swathi, “Smart Surveillance Monitoring System using Raspberry Pi and PIR sensor”, published.

[8] Trio Adiono et al, “IoT-Enabled Door Lock System ”, published.

[9] Firza Fadlullah Asman, Endi Permata, Mohammad Fatkhurrokhman, “A Prototype of Smart Lock Based on Internet of Things (IoT) with ESP8266”, published.

[10] Dr Abbas M. Al. Bakry, Rajaa D. Resan, ”Smart Phone - Arduino based of Smart Door Lock/unlock using RC4 stream Cipher Implemented in Smart Home”, published.

[11] Anonymous, “https://www.arduino.cc/en/Main/arduinoBoardUno>”, website.

[12] Syed Zain Nasir, “Introduction to Arduino IDE - The Engineering Projects”, website.

[13] Krishna,”What is C Programming Language? Basics, Introduction, History (guru99.com)”,website.