SMART LOCK

Design & developed by

I.Venkata Hari Paniindra	2111CS050106
D.Nithish Reddy	2111CS050100
M.Shivraj	2111CS050079
CH.Abhiram	2111CS050098

GUIDED BY

Mr V Vijaykumar Dasari

Department of Computer Science & Engineering (Internet of Things)

IIYR-IISEM

Malla Reddy University, Hyderabad

2021-2025

MALLA REDDY UNIVERSITY
(Telangana State Private Universities Act No.13 of 2020 and G.O.Ms.No.14, Higher Education (UE) Department)

CERTIFICATE

This is to certify that this is the bonafide record of the application development entitled "**SMARTLOCK"**, submitted by **I.Venkata Hari Paniindra (2111CS050106), D.Nithish Reddy (2111CS050100),M.Shivraj (2111CS050079), Ch.Abhiram (2111CS050098)** B. Tech II year II semester, Department of CSE (IOT) during the year 2022-23. The results embodied in this report have not been submitted to any other university or institute for the award of any degree or diploma.

Internal Guide
Mr V Vijaykumar Dasari
(Associate Professor)

Head of the department
Dr. G Anand Kumar
Internet of Things

External Examiner

ACKNOWLEDGEMENT

We would like to express our gratitude to all those who extended their support and suggestions to come up with this software. Special Thanks to our mentor **Mr.V Vijaykumar Dasari** whose help and stimulating suggestions and encouragement helped us all time in the due course project development.

We sincerely thank our Head of the Department **Dr.G Anand Kumar** for his constant support and motivation all the time. A special acknowledgement goes to a friend who enthused us from the backstage. Last but not the least our sincere appreciation goes to our family who has been tolerant, understanding our moods and extending timely support.

ABSTRACT

The emergence of smart technologies has revolutionized various aspects of our daily lives,including home security. One prominent innovation in this domain is the smart lock.A technologically advanced device that replaces traditional mechanical with intelligent and connected systems.Smart incorporate a combination of hardware and software components to enchance the security and convenience of access control. These locks utilise wireless connectivity, through Wifi or Bluetooth, to connect to a central control system, such as smartphone or home automation hub.Through this connection user can remotely manage and monitor access to their home, granting or revoking access permissions as needed.

INDEX

CHAPTER - 1

INTRODUCTION

1.1 Introduction

The emergence of smart technologies has revolutionized various aspects of our daily lives,including home security. One prominent innovation in this domain is the smart lock.A technologically advanced device that replaces traditional mechanical with intelligent and connected systems.Smart incorporate a combination of hardware and software components to enchance the security and convenience of access control. These locks utilise wireless connectivity, through Wifi or B luetooth, to connect to a central control system, such as smartphone or home automation hub.Through this connection user can remotely manage and monitor access to their home, granting or revoking access permissions as needed.

In recent years the importance of security have incresed widely with thefts becoming more easier and stalkers getting more confident it is important to advance the level of technology in security as well. By innovationg the use of latest technology I.O.T we can improve the safety of ourselves and our loved ones.

To develop this security tool we used the connection of an electric lock with a microcontrollers to automate the process of notifyimg us when there is a visitor in front of our door.

1.2 Purpose

To help the user of the lock to be confidetn and tense free about the safety of their belongings and their loved ones .To prevetn the stalking activites of people and be a certain of what's happening at our home/office. To provide a sense of threat to people with bad intentions to create a fear of being watched and being liable to their thoughts and possible actions .

To Utilize the benefits of the internet and connecting with our inter ecosystem to provide data on our security and improve the quality with the help of the evolvong technologies.

1.3 Problem Statement

Security is always concern with the rapidly evolving society and technolgy .It becomes huge matter of concern when there is an stranger in front of our door and and the fear of unknown. We're trying to create a sense of security and make the way of living stress free and easier through the automation of monitoring and believing that the security data can be utilzed in strong way by analyzing it thoroughly.

CHAPTER - 2
LITERATURE REVIEW

The history of smart lock technology can be traced back to the late 20th century when advancements in electronics and digital systems began to revolutionize the traditional lock and key mechanisms. While the concept of keyless entry systems had existed for some time, it was during the early 2000s that the term "smart lock" started to gain prominence.

In the early stages, smart locks primarily focused on improving convenience by replacing physical keys with alternative means of access control. One of the earliest examples of this technology was the introduction of keyless entry systems in automobiles, allowing drivers to unlock their cars using remote key fobs or proximity sensors.

The application of smart lock technology to residential and commercial properties began to gain traction in the mid-2000s. Companies like Kwikset, Yale, and Schlage introduced electronic locks that utilized keypads or touchscreens for code-based entry. These early smart locks were typically standalone devices and required manual code input to grant access.

As wireless connectivity technologies such as Bluetooth and Wi-Fi became more widespread, smart locks evolved to offer increased functionality and remote control capabilities. The integration of wireless protocols allowed smart locks to communicate with smartphones, enabling users to remotely lock and unlock doors, receive notifications, and manage access permissions.

Around 2013, the emergence of the Internet of Things (IoT) further accelerated the development of smart lock technology. Smart locks began to integrate with broader smart home ecosystems, enabling seamless communication with other connected devices such as security cameras, thermostats, and voice assistants.

Biometric authentication, including fingerprint scanning, facial recognition, and voice recognition, also became a prominent feature in smart locks. These advanced authentication methods added an extra layer of security and convenience, as users could gain access to their properties using their unique biological traits.

In recent years, advancements in artificial intelligence and machine learning have allowed for more sophisticated algorithms in smart lock systems. These algorithms can analyze user behavior patterns, detect anomalies, and provide personalized access control. Additionally, smart lock manufacturers have focused on improving the physical security aspects, such as tamper resistance and resistance to forced entry.

As the smart home industry continues to grow, smart locks have become an integral part of home automation systems, offering seamless integration with voice assistants like Amazon Alexa and Google Assistant. They can be controlled using voice commands and can be programmed to work in tandem with other connected devices, creating a comprehensive smart home experience.

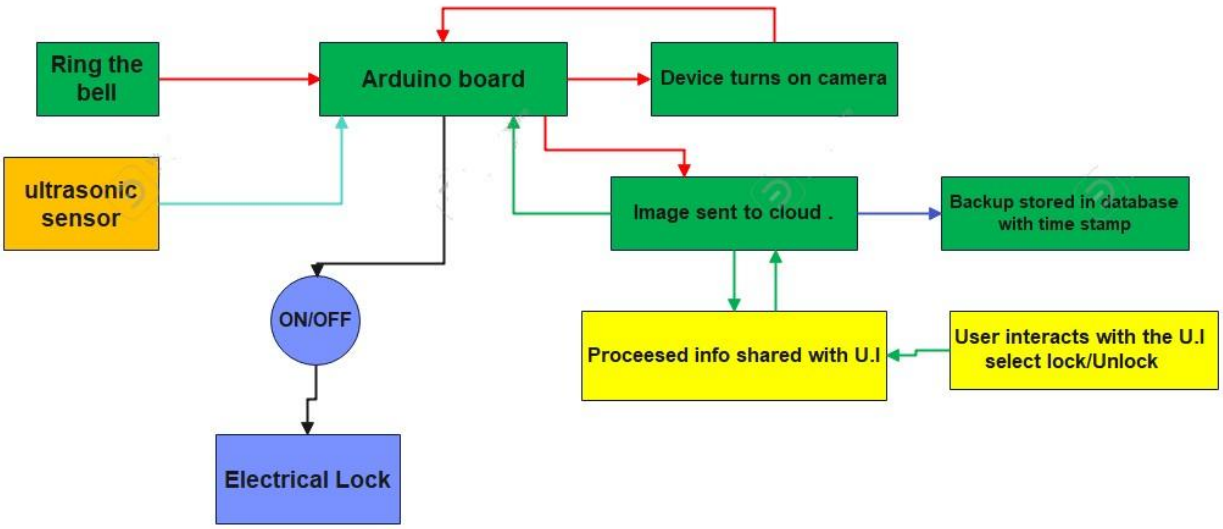
Looking ahead, the future of smart lock technology holds the potential for even more advanced features, including advanced biometrics, gesture recognition, and improved connectivity. Standardization efforts and addressing privacy and security concerns will likely play a crucial role in ensuring the widespread adoption of smart locks in residential and commercial settings.

CHAPTER - 3

PROJECT DESCRIPTION

3.1 Methodology

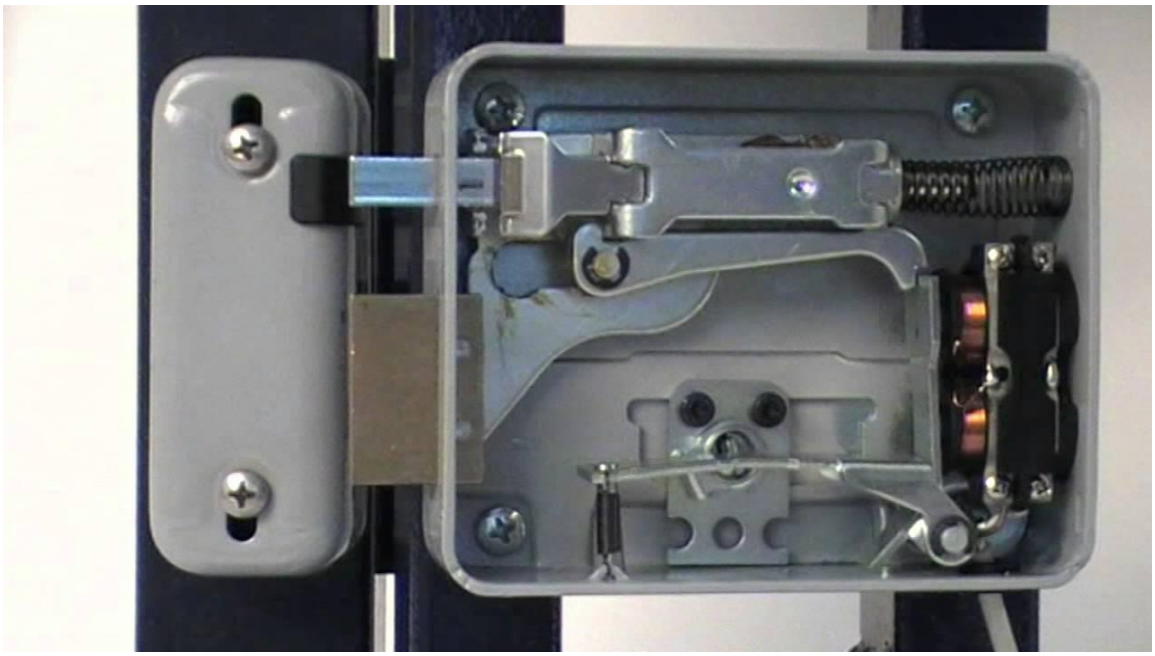
The project deals with SmartLock using arduino board which takes input from ultrasonic sensor and switch button to initiallize to collect data.



The arduino board transfers the data signals from analog to digital or digital to analog the device can make an efficient use of the pherperal devices connected to it. The device can establish a connection to the cloud and store the data into it by sharing the data wirelessly and uses the battery supply efficiently turns the camera off when not in used and awakens when the bell is pressed or the ultrasonic detects an obstacle.

3.2 Working of an Electric Lock

Electric locks are equipped with a power supply to work on its electric working mechanism .The control mechanism of the lock receives input signal being sent from the arduino board after being processed .The input signal is verified by it's signal processing .Once the input signal is verified the control mechanism sends a trigger to lock or unlock the door. This can involve triggering a solenoid or motor which controls the physical bit of the lock.



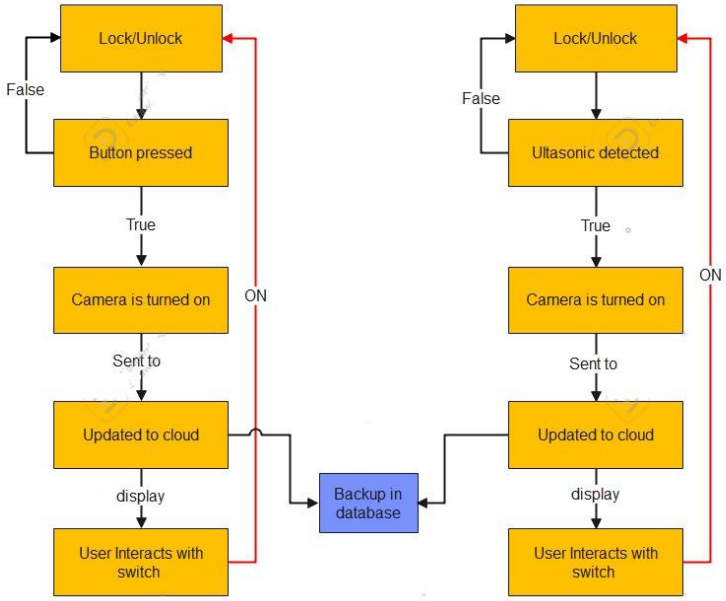
.

3.3 Working of the switch and camera

The smart lock uses a microcontroller board which is connected to all the peripheral devices and uses the connection to collect the data and process the input into output. When the bell is pressed it generates a digital output .This output is collected as input by the controller and is processed as and sends an input to the camera module as an input resulting in the camera turning ON and transferring the data to the cloud inn form of bytes.

3.4 Working of Ultrasonic sensor

An ultrasonic sensor has two main components a transmitter and a receiver. The transmitter generates a signal of above 20,000 Hz. The mechanical waves generated from vibrating are transformed into ultrasonic sounds this waves travel distances until it comes contacts to an opaque object when it comes to contact the waves travel back and reach the receiver. The ultrasonic sensor make notes of the time taken to travel to the object by using the formulae d = speed of sound * time (0.0343*t) the distance of the object is calculated .There is a default limit of distance (Ex : Between two opposite door half the distance between them is the range.) when the distance value becomes less than the range the board sends signal similar to the switch which turns ON the camera.



3.5 Working of the cloud

There is a boom in the use of cloud technology along with the IOT as they are so compatiable with each other the cloud acts as the platform which can perform the computational task of the big data generated by the I.O.T devices in day-day life.The microcontroller sends the to the cloud and the cloud stores it in the database by using API the cloud interacts with microcontroller by sending data the cloud can be used as an interface to control the lock.

3.6 Hardware requirments

- Microcontroller
- Electric clock
- ArduCam
- switch
- Ultrasonic sensor

3.7 Software requiremets

- Oracle
- C language
- Blynk

CHAPTER-4

IMPLEMENTATION AND ANALYSIS

4.1 CODE

```
#include <WiFi.h>

#include <AsyncTCP.h>

#include <ESPAsyncWebServer.h>

#include <ArduCAM.h>

#include <Wire.h>

#include <BlynkSimpleEsp32.h>

//#include<SD.h>

#include<SPI.h>

#include<SD.h>

const char* ssid = "YourWiFiSSID";

const char* password = "YourWiFiPassword";

const char* auth = "YourBlynkAuthToken";


// ArduCAM pin connections

#define OV2640 6

const int CS_PIN = 5;

const int RESET_PIN = 15;

const int SDA_PIN = 21;

const int SCL_PIN = 22;

int Switch_Pin = 9;
```

```
int Lock_Pin = 12;
const int TRIGGER_PIN = 27;
const int ECHO_PIN = 26;

BlynkTimer timer;
ArduCAM arduCam(OV2640, CS_PIN);

bool lockStatus = false; // Initially locked

void setup() {
  Serial.begin(115200);
  pinMode(Lock_Pin,OUTPUT);
  digitalWrite(Lock_Pin,LOW);
  pinMode(Switch_Pin, INPUT);

  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
  }
  Serial.println("Connected to WiFi");

  Blynk.begin(auth, ssid, password);

  arduCam.InitCAM();
```

```
  arduCam.set_format(JPEG);
  arduCam.InitCAM();
  arduCam.OV2640_set_JPEG_size(OV2640_320x240);

  timer.setInterval(1000L, checkLockStatus);

  // Virtual pin for lock control switch in Blynk app
  Blynk.virtualWrite(V1, lockStatus);

  setupServer();
}

void loop() {
  Blynk.run();
  timer.run();
}
void doorBell(){
  if(digitalRead(Switch_Pin) == HIGH){
    captureImage();
    checkLockStatus();
  }
  else{
    doorBell();
  }
}
```

```
void checkPersonDetection() {
  bool newPersonDetected = detectPerson();
  bool personDetected = false;

  if (newPersonDetected && !personDetected) {
    personDetected = true;
    captureImage();
  } else if (!newPersonDetected && personDetected) {
    personDetected = false;
  }
}

bool detectPerson() {
  // Generate ultrasonic pulse
  digitalWrite(TRIGGER_PIN, LOW);
  delayMicroseconds(2);
  digitalWrite(TRIGGER_PIN, HIGH);
  delayMicroseconds(10);
  digitalWrite(TRIGGER_PIN, LOW);

  // Measure the duration of the echo pulse
  unsigned long duration = pulseIn(ECHO_PIN, HIGH);

  // Calculate the distance based on the speed of sound
  float distance = duration * 0.034 / 2;
```

```
  // If a person is within a certain range, return true
  if (distance < 100) {
    Serial.println("Person detected");
    return true;
  } else {
    Serial.println("No person detected");
    return false;
  }
}

void checkLockStatus() {
  if (lockStatus) {
    // Lock the door
    lockDoor();
  } else {
    // Unlock the door
    unlockDoor();
  }
}

void lockDoor() {
  // Code to lock the door using the smart lock
  Serial.println("Locking the door...");
  digitalWrite(Lock_Pin, HIGH);  // Activate lock mechanism
```

```
  Blynk.virtualWrite(V2, 255);
  // Add your lock control code here
}

void unlockDoor() {
  // Code to unlock the door using the smart lock
  Serial.println("Unlocking the door...");
  // Add your unlock control code here
  digitalWrite(Lock_Pin, LOW);  // Activate lock mechanism
  Blynk.virtualWrite(V2, 0);
}
void viewLockStatus()
{
  int lockStatus = digitalRead(Lock_Pin);
  Blynk.virtualWrite(V2, lockStatus * 255);  // Update lock status on Blynk app (LED widget)
}
void setupServer() {
  AsyncWebServer server(80);

  server.on("/capture", HTTP_GET, [](AsyncWebServerRequest *request) {
    captureImage();
    request->send(200, "text/plain", "Image captured");
  });

  server.begin();
```

```
}

void captureImage() {
  char filename[13];
  sprintf(filename, "/image-%lu.jpg", millis());

  arduCam.clear_fifo_flag();
  arduCam.start_capture();

  while (!arduCam.get_bit(ARDUCHIP_TRIG, CAP_DONE_MASK))
    delay(1);

  int total_bytes = arduCam.read_fifo_length();
  int buf_len = total_bytes;
  byte *image_buffer = new byte[buf_len];

  arduCam.CS_LOW();
  arduCam.set_fifo_burst();

  for (int i = 0; i < total_bytes; i++) {
    image_buffer[i] = SPI.transfer(0x00);
  }

  arduCam.CS_HIGH();
```

```
  arduCam.clear_fifo_flag();


  File file = SD.open(filename, FILE_WRITE);
  if (file) {
    file.write(image_buffer, buf_len);
    file.close();
    Serial.println("Image captured and saved: " + String(filename));
  } else {
    Serial.println("Failed to save image.");
  }


  delete[] image_buffer;
}


BLYNK_WRITE(V1) {
  lockStatus = param.asInt();
}
```

4.2 Experimental results & Analysis

Code is compiled by installing the required libraries.

When the switch (trigger pin) is pressed the camera module turns ON.

When the Ultrasonic sensor detects a person the camera is turned ON.

When the UI switch is turned ON the LOCK is turned OFF.

CHAPTER -5

RESULTS & CONCLUSION

5.1 Conclusion:

We have created a smart lock which can be connected to the Wifi which can share data to the cloud and access can be shared with the user who can control through the U.I of the blynk. The main use of this smart lock application is to share the video and time database and can be checked later time and stay updated with activites in day-day life in their absence .

5.2 Future scope:

- By using machine learning algorithm we can try face detection for members of the family.
- We can try to share live video footage in place of static photo
- By Integrating with our smart home we can set the smart lock to have a record and alert feature during night times.