BANK VAULT SECURITY SYSTEM

Prof. Swetha V
Associate Professor
Computer Science & Engineering
RGIT

Mohammed Zayaan PS
Computer Science & Engineering
RGIT

Mohammed Maqsood Hussain
Computer Science & Engineering
RGIT

Bismitha
Computer Science & Engineering
RGIT

Elena Prasanna
Computer Science & Engineering
RGIT

Abstract - People are always searching for safe places to keep their money and belongings. People who are more mature think that banks are the most reliable location to store their belongings. Since items housed in bank vaults are frequently the target of thieves, bank security has been a crucial component in ensuring that visitors feel comfortable about their belongings. In the past, banks have used biometric identification, keypad cinches, burglar warnings, and enhanced security. By automating bank security, this scheme also sets up a trap for any potential offenders. Our design will use two doors for the bank vault instead of the typical single door style. Face recognition technology will be used at the initial entry. If someone is permitted there, they are also permitted at the secondary entry. This camera can identify whether a person is a real person by looking at their face. Although a communication or data transfer will take place through the BLYNK iot garçon, this door will be protected by the security system to allow access to the backup door in the next stage, or coming DOOR2, if permission is granted. A message will also be sent through the security station, and if the goal cannot be reached, an alarm or temptress will sound. The alternative door is coupled to a speech recognition system for access to the vault door. As a result, it will also be decided whether to provide a registered stoner access to the vault or not. Consequently, the provided outcome will support in raising bank vault security.

Keywords—IOT, Security, Arduino uno, raspberry pi, Biometrics, finger print, face recognition, sensor, PI camera, dc motor

I.   INTRODUCTION

People have taken good care of their valuables from the beginning of time. The concept of a bank developed over time. A bank is the safest place for people to store their belongings. The number of people keeping their possessions in banks has grown recently, which has boosted the quantity of money moving through banks. The bank stores its possessions, money, and any gains in a safe location called the bank vault. The increasing cash flow has piqued bank robbers' curiosity. Due to the current pace of technological advancement, even burglars are able to access bank vaults and take their contents. Bank vaults are hence particularly susceptible to these kinds of crimes. While bank robbers once used advanced technology, it is now essential to stop them employing cunning technologies.

This strategy aims to successfully thwart burglars who use cutting-edge technology. This technique uses two doors in place of the conventional one used for bank vaults. The first door will have a camera-equipped admission system. The biometric lock on the second door will be replaced with a voice playback module that operates on 0s and 1s. The recommended approach will successfully repel robbers by utilising cutting-edge technology. All around the Bank, strict security criteria are assumed. Every single person carries out everyday banking operations. Because of the high level of protection they offer, we utilize bank lockers to keep our possessions, such cash, jewelry, and important papers, safe.

It has so developed into a part that is necessary for every common person. If the banking industry is to continue to thrive in the current environment, it must be able to handle exceptionally large increases in security. We are all aware that when new branches open, they consider the needs of the surrounding area.

Therefore, every business has to have more security. Progress has allowed the current system and services to enjoy a higher level of autonomy, and financial services are not far behind. Numerous studies have found that the security system's components and technology are flawed.

The project's overarching goals revolve around enhancing security and streamlining access to bank vaults. Only a select few people are allowed access to the system. A Bank employee and four more people are the only ones who have access to the vault. There are two security alternatives in

this situation.

At the first checkpoint, the entrance to the bank vault room, we installed a progressive security system:
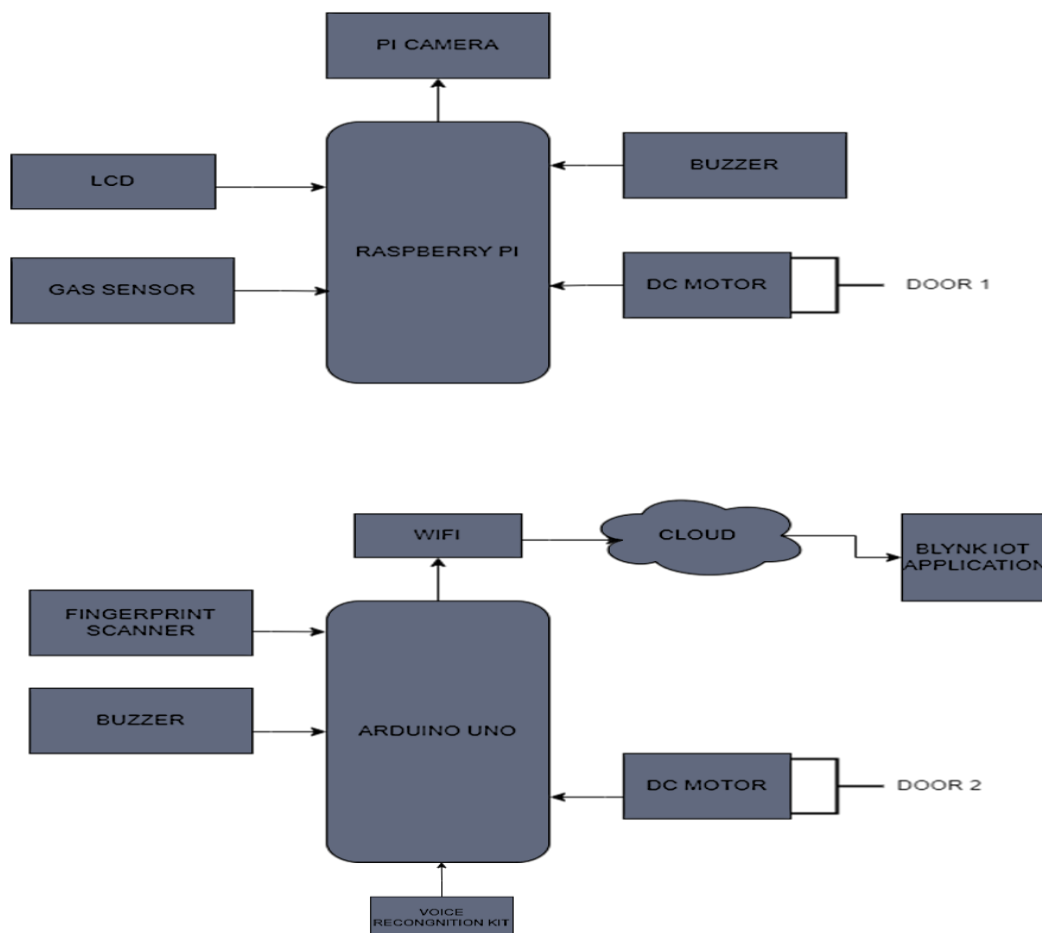
a. Face recognition

b. voice playback

c. Finger print

The second door is interfaced with a voice recognition system using 0s and 1s to enable entry to the vault door. The registered user will thus either be granted access to the vault or denied it if his voice is recognized.

The bank system will prohibit thieves from entering the vault if they violate the first door's security, and it will also capture them.

Block diagram of the bank vault security system

II.   MODULES INOLVED
HARDWARE COMPONENTS:
DOOR1:
1.   Raspberry Pi
2.   Pi camera
3.   Buzzer
4.   Gas sensor
5.   DC motor
6.   LCD

DOOR2:
1.   Arduino UNO
2.   Fingerprint Scanner
3.   Buzzer
4.   DC motor
5.   Voice recognition kit

SOFTWARE COMPONENTS
1.   Raspberry Pi OS
2.   Arduino IDE Software
3.   Embedded C programming/Arduino C
4.   Python
5.   OpenCV
6.   Android APP(BLYNK IOT)

RASPBERRY PI

The Raspberry Pi is a small single-board computer that is about the size of a credit card.

Open-source tools including web-based communication, multimedia, and the usage of microcontrollers are all included in the Raspberry Pi. Mobile devices' portability is the issue.

RASPBERRY PI SPECIFICATIONS:

Memory: Version B of the Raspberry Pi, which is the most recent version, contains 512 Mb of SDRAM, over two times as much as edition A's 256 Mb. In the grand scheme of things, it is a little computer. Even if the RAM utilized in these types of apps is more than 256 Mb or 512 Mb, a common computer's memory space is measured in gigabytes.

CPU: The capability of the Raspberry Pi (CPU). It is responsible for implementing logical and mathematical processes to carry out computer orders. The well-known brand Raspberry Pi is powered on an ARM11 series CPU. It now belongs to the Samsung Galaxy smartphone family.

GPU: The Raspberry Pi uses a special CPU named the graphics processing unit. (GPU). It aims to speed up and simplify manipulating visual calculations. OpenGL is compatible with the Broadcom video core IV included inside the Raspberry Pi.

Ethernet Port: The Ethernet connection onboard the Raspberry Pi serves as the main interface for interfacing with external electronics. To access the internet, plug your home router via the Ethernet connection on the Raspberry Pi.

GPIO Pins: The Raspberry Pi's universal inputs and outputs are used to connect it to other circuit boards. A configured Raspberry Pi may transmit and receive instructions to GPIO pins. The Raspberry Pi is equipped with digital GPIO pins.

Other electronic components are linked to these pins. You might, for instance, attach it to the temperature sensor that sends digital data.

XBee Socket: The raspberry pi has two XBee connections for wireless communication. Connectors for an Electrical Source: On the side of this shield is a little switch that may be used to activate a power source via an external source.

UART: A UART is a sequential input and output interface. This allows it to exchange text-based serial data and adjust the debugging code.

ARDUINO UNO

An 8-bit ATmega328P microprocessor serves as the core of the Arduino Uno microcontroller board. A crystal oscillator, a voltage regulator, and serial connectivity are additional parts for the ATmega328P CPU. The Arduino Uno has 14 digital I/O ports, including six that may be utilized for PWM output, 6 analog input pins, a USB the interface, and 6 digital I/O ports.

Arduino Uno Pinout

Arduino Uno Specifications

Microcontroller	ATmega38P – 8 bit AVR family microcontroller
Operating Voltage	5V
Recommended Input Voltage	7-12V
Input Voltage Limits	6-20V
Analog Input Pins	6 (A0-A5)
Digital I/O Pins	14 (Out of which 6 provide PWM output)
DC Current on I/O Pins	40mA
DC Current on 3.3V Pin	50mA
Flash Memory	32 KB (0.5 KB is used for Bootloader)
SRAM	2kB
EEPROM	1kB
Frequency (Clock Speed)	16MHz

PI CAMERA

The Raspberry Pi Cam is used to do this kind of internet streaming. The innermost circle is streamed online by the Raspberry Pi CPU and may be accessed by any web server by providing the host's IP address. By enabling you to see what's going on in the inner circle whenever you want and from any location as long as you have internet connection, you can secure your security. The Raspberry Pi camera module is also capable of recording HD video in addition to still photos.

PI CAMERA FEATURES:

8MP camera
Wider picture, 2592x1944 stills, and 1080p30 video are all supported by CSI.
25 x 20 x 9 mm in size

Camera Details:

Raspberry Pi, which is mounted on a tiny circuit board with dimensions of 25mm by 20mm by 9mm, is connected to the camera through the Camera Serial Interface (CSI) bus. The camera's image sensor, which has a fixed focus lens, has a native resolution of five megapixels. The camera's software is capable of taking full-quality still pictures up to 2592x1944 and movies at 1080p30, 720p60, and 640x480p60/90 resolutions. Before installing the ribbon cable, the Raspberry Pi board's CSI port has to be attached. Even though it might be a little challenging, if you adhere to the instructions in the videos, you shouldn't have any issues. A small camera board and wire are also included when purchasing the camera.

You'll need to devise a method to sustain the camera in order to use it. Raspberry Pi enclosures and camera supports are now easily available. You can rig a straightforward gadget yourself if you want to. I attached mine to a case using a little piece made of plastic and dual-sided adhesive.

BUZZER

A beeper or buzzer, for example, might be formed of mechanical, piezoelectric, or electromagnetic components, but the signal's main purpose is to convert

audio to sound. Computers, printers, computers, timers, alarm clocks, and other electronic gadgets regularly utilize and power it. Depending on the different designs, it may emit a broad range of noises, including alarm, melody, bell, and siren. The beeper has both positive as well as negative pins

SPECIFICATIONS OF BUZZER:

These are some of the buzzer's specifications.

• Operating temperatures range from -20 to +60 degrees Celsius.
• Operating voltages vary from 3 to 24 volts DC.
• The color is black.
• The supply current is less than 15 mA, or 85 dBA, in terms of sound pressure level.

GAS SENSOR

The 400 different smell receptor types in a typical human nose can detect over 1 trillion distinct odours. But many of us still don't know what sort or how much fuel is present in our environment. Sensors are useful in this situation. A gas sensor comes in handy in situations when it's important to monitor variations in the number of dangerous gases for the purpose to preserve system security and forewarn/avoid any unexpected risks. To identify amongst chemicals like oxygen, carbon dioxide, nitrogen, and methane, among others, there are several types of gas sensors available. They are widely utilized in a variety of other devices as well, such as those that evaluate the air quality in commercial buildings and look for harmful gas leaks.

GAS SENSOR FEATURES

• Can measure or detect LPG, alcohol, propane, hydrogen, carbon monoxide, and even methane;
• Operating voltage is +5V;
• 0V to 5V for analogue output; 0V or 5V for digital output (TTL Logic)
• Can be used as a digital or analogue sensor; 20-second preheating time.

DC MOTOR

A DC motor is an electrical device that uses electricity to create mechanical energy. The operational principle of the DC motor states that when a current carrying conductor comes into touch with the electromagnetic field, it feels a mechanical force.
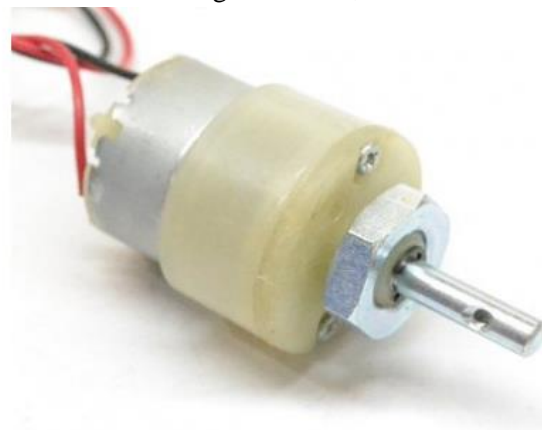
POWER SUPPLY

A power supply is an electrical circuit that changes the voltage from alternating current (AC) to direct current (DC). Transformer, rectifier, filter, and regulator circuits make up the majority of its components. In specifically, a power supply transforms alternate high voltage current (AC) to direct current (DC) and controls the DC output voltage to the precise tolerances needed for contemporary computing components. The task of turning the energy from the outlet into power that can be utilized by various components of an electrical device belongs to the power supply unit. The two types of power supplies that are available are DC power

supplies and AC power supplies.

VOICE RECOGNITION MODULE

It is a compact spoken recognition board that is easy to use. This speaker-reliant module has room for as many as 80 voice commands. Any sound may be made to function as an order. Before a module can comprehend any spoken command, users must train it. Like a library, all spoken orders are gathered into one sizable collection. Recognizer might import any of the seven spoken commands from the library. It indicates that seven instructions are active at once.

This board may be controlled via either the general input pins or the full-function serial port. (part of function). When an oral instruction is recognized, generic output pins on the board might produce a variety of waves.

SPECIFICATIONS OF VOICE RECOGNITION MODULE

- Voltage: 4.5-5.5V
- Current: 40mA
- Digital: 5V TTL level UART interface
- Analog: 3.5mm mono-channel microphone connection
- Recognition Accuracy: 99%. (under ideal environment)
- Up to 80 voice commands may be supported and seven voice commands may be active at once.
- UART/GPIO and user-control general pin output are two straightforward control techniques.

LCD

A flat display technology known as "Liquid Crystal Display," or LCD, is frequently used in computer displays, instrument panels, smartphones, digital cameras, TVs, laptops, tablets, and calculators. It is a small monitor with excellent image quality and support for high resolutions.

LCDs Work

The fundamental principle behind LCDs is that liquid crystals are employed in LCD screens to turn pixels on and off to reveal a certain color. Additionally, the liquid crystal molecule has a propensity to untwist when an electrical current is applied. Both the angle of the top polarizing filter and the angle at which light—light that is passing through the polarized glass molecule—is changed as a result.

As a result, a little amount of light is made available to the polarized glass with the help of a particular region of the LCD. As a result, this specific area will get darker than surrounding regions. Instead of emitting light, LCDs work on the principle that light should be blocked. A reflecting mirror was mounted on the back of the LCDs during construction. An electrode plane composed of indium-tin-oxide is kept on top of the apparatus.

Additionally, the bottom of the smartphone is covered with a polarized glass with a polarizing film. Liquid crystal material must be positioned above the single electrode that is used to contain the LCD as a whole.

Then, a second rectangle-shaped piece of glass with an electrode is attached to the bottom and a second polarizing film is put to the top. But make sure that both components are positioned at the right angles. When there is no current, light enters the LCD's front and, after reflecting with the help of a mirror, goes back. A red, green, and blue pixelated screen is placed in front of the light. A filter can be activated or deactivated by the liquid crystals to either make a given color visible or keep that pixel dark. This explains why LCD devices like monitors and TVs consume a lot less energy than equivalent CRT devices.

FINGERPRINT SCANNER

There are many various types of fingerprint scanners, which are devices used to detect individuals by scanning their fingerprints. Humans all have ridges on our fingertips, and each one of those ridges presents a distinct pattern, which a fingerprint scanner scans to recognize us. Here are a few illustrations:

• Optical reflexive
• Capacitive
• Mechanical
• Thermal
• Dynamic output

HOW DO FINGERPRINT SCANNERS WORK

A light-penetrating a microcontroller that could consist of a charge-coupled device, CMOS image sensor, CCD, or both, is included within the sensor. As a consequence, a digital picture is produced. The fingerprint is mechanically separated from the image by the CPU, which then uses specialized pattern-identical

software to encrypt the data.

There are more modes of operation for scanners besides this one. Different types of scanners, such as capacitive ones, may scan the areas between our ridges. When an individual places their palm on an object, the ridges make contact with the object's surface. To categories these ridges, the distances between the gaps are measured. The pattern might then be recorded as a consequence. In other words, it requires calculating the separation between two ridges that were never in contact.

TECHNOLOGY USED

1.IOT(Internet of Things)
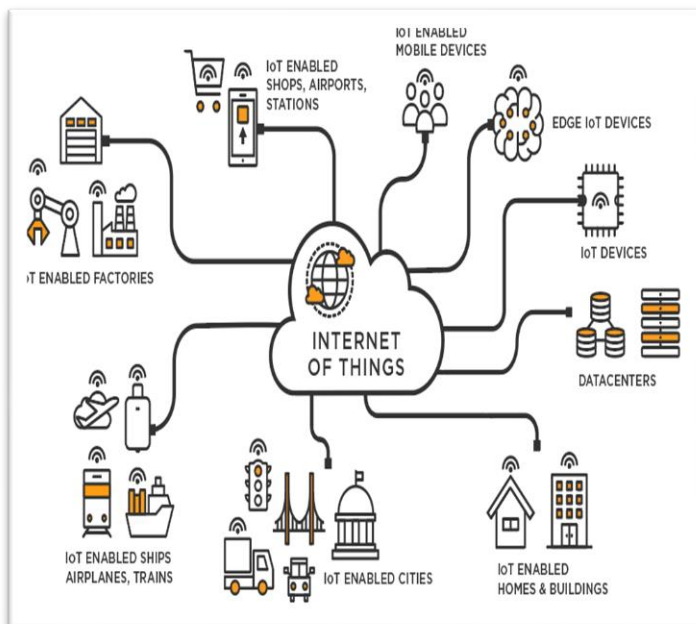
The internet of things, or IoT, is a network of electromechanical and digital gadgets, living creatures, inanimate objects, people, and computers that can communicate with each other and with each other remotely.

The Internet of Things (IoT) ecosystem is made up of web-enabled smart devices that employ embedded technology, such as processors, sensors, and tools for communication, to collect, communicate, and act on the data they receive from their environment.

IoT devices can communicate the sensor data they gather to another edge device or an IoT bridge, which either analyses the data internally or transmits it to the cloud for analysis. These devices will at times communicate with other similar devices.

2.Machine learning :
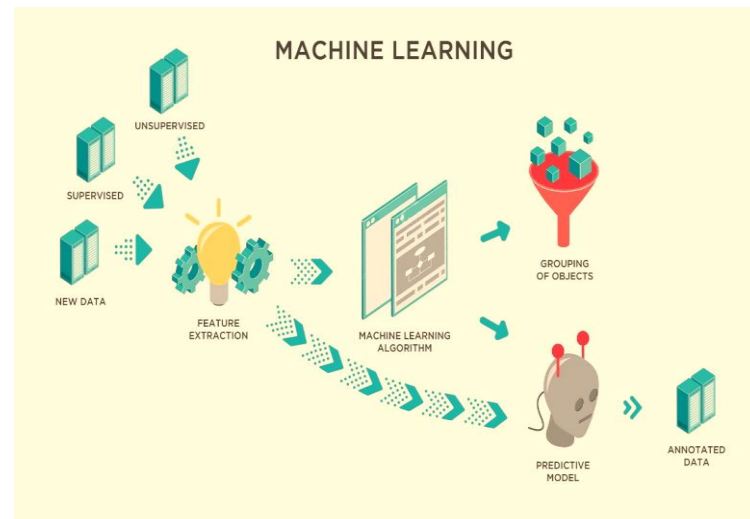
In the real world, we are surrounded by individuals who can learn from what they have learned, as well as robots that we can programming to carry out our requests. Some claim that the main objective of machine learning, which is a subfield of AI, is to develop algorithms that let a computer learn on its own using data and information from the past. Without explicit programming, machine learning algorithms build a mathematical model from past data samples, or "training data," to provide forecasts or judgements. Machine learning and statistics are used to create prediction models. Machine learning either uses pre-existing algorithms or develops its own. The performance will improve as more information is provided.

A machine learning algorithm predicts the result using forecasting algorithms that it created using historical data. Larger data sets make it simpler to create models that predict outcomes with more accuracy, but the overall quantity of data employed influences how well the output can be anticipated.

Let's imagine that we find ourselves in a challenging situation that calls for making certain forecasts. We could simply feed the data into general computations, which would then produce the logic that corresponds to the data and are expecting the consequences, rather than creating custom code.

As a result of machine learning, our knowledge of the problem has changed. The block diagram below shows how information is shared across machine learning algorithms.

Despite the fact that people may interact with the devices to set them up, provide instructions, or get data, the devices mostly operate without human interaction. The specific currently recognized IoT applications have a considerable impact on the communication, networking, and connectivity protocols used by these web-enabled devices.

To assist modernize and streamline data gathering procedures, IoT may also make use of machine learning and AI. (AI).

People may live more shrewdly, work more efficiently, and have total control over their life by employing the internet of things. The Internet of Things is crucial to business and provides innovative tools for smart home automation. With the help of the Internet of Things, businesses can gain insights on anything from machinery efficiency to logistics and supply chain operations, enabling them to see how their systems actually operate in real time.

IoT enables organizations to automate procedures and reduce employee costs. Additionally, it enhances service delivery, lowers the cost of producing and transporting items, and provides transparency into customer interactions.

Through the Internet of Things, companies are given the resources they need to enhance their business plans, which compels them to reconsider how they manage their operations.

Some firms are currently going through a digital transformation, even though it has also found uses for organizations in the infrastructure, home automation, and agricultural sectors. Typically, the industrial, transportation, and utility sectors are home to IoT businesses that make use of sensors and other IoT devices.

IoT in agriculture might help farmers by simplifying their work. Sensors can gather information on the soil's chemistry, temperature, humidity, rainfall, and other elements that will aid in automating agricultural practices.
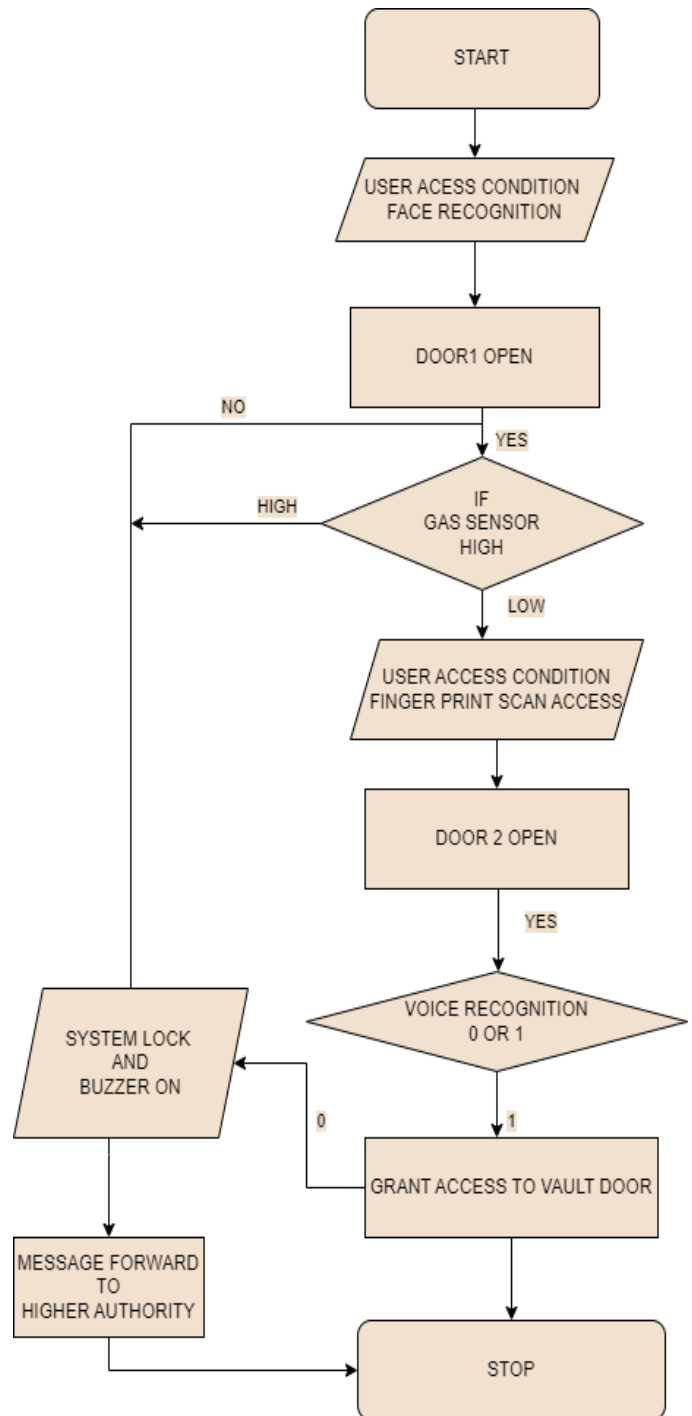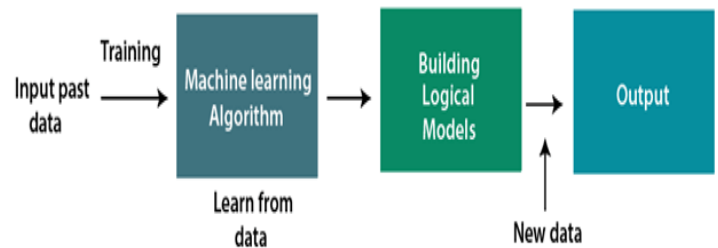

F*ig. 3. Flowchart of bank vault security system*

Verifying, monitoring, and controlling the bank security locker rooms as well as providing high-proof protection to highly protected zones like bank locker rooms are significant goals of a bank vault security system.

In order to deter burglars from entering the bank vault, a buzzer or siren is utilized in the "Bank vault security" system that is being developed. It also guards and keeps the bank vault safe by attempting to jail any intruders who try to enter it. In contrast to the usual one door used for vault security, the suggested approach uses two doors. The one who has been granted access to the first door will have access to the second door. The initial door will be unlocked using a facial recognition technology. The Raspberry Pi System will have a camera module that can only be accessed by registered users or a specific person.

As a result, if the user qualifies using face recognition, he will be permitted to enter DOOR1; otherwise, the access will be denied, preventing the burglar from entering the second door. Thus, the LCD monitor of the security system will display the access data.

Unauthorized entry into the second door will lock the thief at the first door itself if it is attempted. As a result, the suggested method will not only stop thieves from breaking into the vault but will also catch them if they are able to get past the protection at the first door.

The subsequent stage, or the subsequent DOOR2, will involve connecting all the parts to an Arduino UNO microcontroller, which provides fingerprint access as its primary feature. This microcontroller will recognize the fingerprint of the registered user and, if access is granted, transmit a message or piece of data through the BLYNK IoT server, which will be monitored by the security system for entry to the second door. The security station will also send a message, and if the fingerprint is not available, an alert or siren will sound. It is possible to open the vault door using 0s and 1s by interfacing a voice recognition system with the second door. The registered user will thus either be granted access to the vault or refused if his voice is recognized. Identify the faces in the block diagram. When a burglar tries to use gas-flaming equipment, a gas sensor is activated, an alarm or buzzer flashes, information is shown on an LCD screen, and the security station is informed

A Raspberry Pi camera and a gas sensor are both attached to the first door in order to detect registered faces. If access is allowed, a warning will be shown on the LCD and a component DC motor will turn on and begin the door's opening mechanism.

A buzzer, buzzer motor, and fingerprint reader are

connected to an Arduino in a manner similar to this. At the security station, data is watched using an IOT application. If someone can unlock the first door and their fingerprint is accepted, they will also be able to open the second door. If not, the monitoring station will receive the alarm via an IoT application, the bell will ring, the door access request will be refused, and the bell will ring.

III.   OUTCOMES OF THE PROJECT

The contemporary world is causing new systemic upheavals. The prevention of all forms of protection is necessary to halt robberies in bank lockers. IOT can therefore be used to prevent bank fraud, as well as the use of alarms, buzzers, LCDs, and voice recognition kits to verify registered users' voices, produce alert messages, and send data to bank security stations in the event of any misleading actions or to obtain safety from unauthorized individuals. Enlarging our mechanism to stop bank theft might make banks more secure.

IV.   FUTURE WORK

The camera itself and hardware connected to it that offers many layers of security, such as utilizing PIR sensor and RFID system, warning message, and facial recognition that identifies the user's face, as well as by employing dual keys, will be used to detect motion in order to boost security. There is a very secure biometric fingerprint identification technology that is infrequently used. IOT will send an email alert to a GSM module or provide a real-time update.

V.   CONCLUSION

The "Bank Vault Security system" is validated using a gas sensor at the main door and facial recognition using a Raspberry Pi to find registered faces. If the burglar tries to use gas flame instruments, the sensor will activate, and an LCD screen will display an alarm or buzzer that will light up and inform the security station to the attempt. If access is permitted, a component DC motor will activate, opening the door, and an LCD message indicating approval will be shown. Similar connections exist between the buzzer, DC motor, and fingerprint reader for the first door and the Arduino for the second door.

An IOT application is used by a security station to monitor the data. If a person has fingerprint access, he or she will be allowed to open the first door as well as the second one The first door and the second door can both be opened by someone with fingerprint access. If not, an IoT application will send a notification to the security station, the buzzer will ring, and the door access granted will be denied.

The Bank Security System for Bank Vault comes with

safe, automated, and remote monitoring capabilities. The current technology for defending vault rooms worked well because it combined biometric sensors and image processing. It is possible to draw the conclusion that the recommended system has succeeded in achieving its main goals and objectives. By employing numerous sensors and other security technology in the near future, the number of security layers may be enhanced. This suggested strategy can be used in places that need stricter protection, such military installations.

VII. REFERENCES

[1] "Design of a Bank Vault Security System with Password, Thermal & Physical Interrupt Alarm," International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013, ISSN 2229-5518. November 2012 issue of the International Journal of Computer Applications (0975 - 8887), volume 57, no 18.

[2] "GSM Based Bank Vault Security System," International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 2, February 2016. Ripan Kumar Ray, Muhammad AfsarUddin, and Syed Foysol Islam.

[3] "OTP (One Time Password) Based Locker System," International Journal of Engineering Research and Development (IJERD), ISSN: 2278-067X. Meha Brahmbhatt and Vishva Pandya Recent developments in electrical and electronic engineering, pages 78–80 [RTEECE] April 8th–9th, 2016

[4] R.Ramani, S.Valarmathy, S. Selvaraju, P.Niranjan,"Bank Locker Security System based on RFID and GSM Technology," International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012.

IJRASET Volume 4 Issue IV, April 2016, Ch. Sumalatha, A. Viyayamanasa, K. Ramasrujana, I. Meghamala, K. Lakshmi Prasanna, and K. Hema Rani, "Bank Locker Security System Using RFID and GSM Technology."

[6] "Self-Powered and Reusable Biocomputing Security Keypad Lock System Based on Biofuel Cells," Chempubsoc Europe Volume16, Issue26, July 12, 2010, by Ming Zhou, Xiliang Zheng, Jin Wang, and Shaojun Dong.

[7] "RFID based security and access control system using arduino with gsm module," IJEEE, Vol. 2, Issue 2, April, 2015. Grewal Kaushal, Rishabh Mishra, Neelam Chaurasiya, and Paramdeep Singh.

[8] RFID-based School Bus Tracking and Security System by Shraddha Shah and Bharti Singh, IEEE, April 2016.

[9] RFID-based Kindergarten Intelligence security system by Zhiyuan Fang, Li Wei, and Li Wei was published in IEEE September 2012.

[10] Sundus K. E. and AL Mamare S. H., "Using Digital Image Processing to Create an Intelligent Gate," International Journal of Advanced Computer Science and Applications, Vol. 5, No. 5, 2014