A PROJECT REPORT

ON

“Biometric Based Smart ATM”

Submitted to

Savitribai Phule Pune University, Pune.

Submitted in partial fulfillment of the requirement for FOURTH YEAR ENGINEERING

IN

ELECTRONICS & TELECOMMUNICATION ENGINEERING

By

Nakul Pravin Tiwari [B190613067] Shruti Balasaheb Walzade [B190613069]

Rameshwar Vinod Khamgaonkar [B190613028]

Under the Guidance of

Dr. Gayatri Phade At
DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION ENGINEERING

SANDIP FOUNDATION

SANDIP FOUNDATION'S

SANDIP INSTITUTE OF TECHNOLOGY & RESEARCH CENTRE

Mahiravani, Trimbak Road Nashik – 422213.

Academic Year 2023 – 2024

SANDIP FOUNDATION'S

SANDIP INSTITUTE OF TECHNOLOGY AND RESEARCH C

Department of Electronics & Telecommunication

VISION OF THE INSTITUTE

To be acclaimed institution for learning and research.

MISSION OF THE INSTITUTE

- *To impart in-depth technical knowledge.*
- *To create conducive environment for research, innovation and entrepreneurship.*
- *To instill the social and cultural values.*

VISION OF THE DEPARTMENT

To be a preferred department, offering contextual relevant education emphasizingon the research and innovation.

MISSION OF THE DEPARTMENT

M1. Promoting contextual relevant curriculum
M2. Enabling OBE based effective teaching learning practices
M3 Promoting industry relevant modern education tools
M4. Nurture innovation and creativity through experiential learning.
M5. Inculcating ethics and soft skills leading to the overall personality

SANDIP FOUNDATION'S

SANDIPINSTITUTE OF TECHNOLOGY & RESEARCH CENTRE

Mahiravani, Trimbak Road Nashik – 422213.

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION ENGINEERING

Certificate

This is to certify that, this Project Report entitled

“Biometric Based Smart ATM”

submitted by

Nakul Pravin Tiwari [B190613067] Shruti Balasaheb Walzade [B190613069]

Rameshwar Vinod Khamgaonkar [B190613028]

for partial fulfillment of the requirement for Fourth Year Engineering in **ELECTRONICS & TELECOMMUNICATION ENGINEERING** as laid down by **SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE.** This is a record of his own work carried out by him under my supervision and guidance during Academic Year 2023 - 2024.

Place: - Nashik.

Date: - 30/ 05 / 2024.

Dr. Gayatri Phade
Project Guide

Prof. Sushant J. Pawar
Project Co-ordinator

Dr. Mrs. G. M. Phade
Head of Dept

Prof.______________
External Examiner

Dr. M.M.Patil
Principal, SITRC.

ACKNOWLEDGEMENT

The work procedure in this report would not have been completed without the encouragement and support of many people who gave their precious time and encouragement throughout this period. First & foremost, we would like to express our deepest gratitude to our Project Guide **Dr. Gayatri Phade** for her invaluable support, guidance, motivation & encouragement throughout the period this work was carried out. His readiness for consultation always, his concern & assistance even with partial things has been extremely helpful. It was a great pleasure to work under his guidance. We are very much thankful to **Prof. Sushant J. Pawar** (Project Coordinator) for giving us many useful comments & guidance for improving work throughout the period. Their suggestions with Practical things have been extremely helpful. We are also grateful to **Dr. Mrs. G. M. Phade** (Head of Department-E&TC) for motivation, support in all respect and giving us important comments to improve our Seminar Report. We are most grateful to honorable Principal **Dr. M. M. Patil** for giving us important comments to improve our Seminar Report. We sincerely thank to the entire teaching staff member, our college, our family, and those who knowingly & unknowingly have contributed in their own way in completion of this project.

i. Nakul Pravin Tiwari
ii. Rameshwar Vinod Khamgaonkar
iii. Shruti Balasaheb Walzade

ABSTRACT

In an era where technological innovation is reshaping finance and security, we present the BIOMETRIC-BASED Smart ATM, a revolutionary system designed to enhance the modern banking experience by prioritizing convenience and security. Automated Teller Machines (ATMs) enable customers to perform financial transactions without the need for human assistance. This paper proposes an enhancement to current ATM systems through the integration of biometric authentication and GSM technology to address and mitigate existing vulnerabilities. By incorporating biometric fingerprint recognition and a GSM module for One-Time Password (OTP) generation, our system ensures that only legitimate users can access the ATM, adding a robust layer of security. This dual-layer security mechanism significantly reduces the risk of unauthorized access and fraud. Given the critical role of ATMs in daily financial transactions, enhancing their security is essential. Our proposed BIOMETRIC-BASED Smart ATM system combines state-of-the-art biometric technology with real-time OTP verification to provide secure, reliable, and convenient access to financial services. This paper explores the design and implementation of this advanced system and discusses its potential to transform the banking experience by enhancing user security and trust in automated banking services.

Table of contents

Appendix

List of Figures

List of Tables

List of Flow Chart

1. INTRODUCTION

1.1 Introduction

In an era where technological innovation continues to reshape the landscape of finance and security, we proudly present the next evolution in automated banking services: the BIOMETRIC-BASED Smart ATM. Designed to revolutionize the way we interact with our finances, this cutting-edge ATM system boasts a suite of advanced features that prioritize both convenience and security, setting new standards for the modern banking experience. Automated Teller Machines (ATMs) are computerized telecommunication devices that provide customers with access to financial transactions in public spaces without the need for a human clerk or bank teller. In this paper, we propose an enhancement to the current ATM system by integrating advanced security measures.

By incorporating biometric authentication and GSM technology, we can address and mitigate many of the vulnerabilities present in the current ATM systems. In the modern world, having access to money at any time and place is crucial, whether for travel, shopping, or health emergencies. However, carrying cash increases the risk of robbery, making banks the safest repositories for our money. ATMs offer a convenient solution by providing access to cash at any time and any location. They are the easiest way to obtain money quickly and efficiently.

Given the critical role that ATMs play in daily financial transactions, it is essential to enhance their security further. This motivates us to introduce a secondary layer of protection to the existing security system by utilizing biometric authentication and a GSM module to generate One-Time Passwords (OTPs). The use of biometric authentication ensures that only the legitimate user can access the ATM, adding a robust layer of security. Additionally, the GSM module generates an OTP, which must be received and entered by the specified user before any transaction can proceed. This dual-layer security mechanism significantly reduces the risk of unauthorized access and fraud.

As the banking and transaction systems continue to evolve worldwide, ensuring the validation and security of these systems becomes increasingly important. Our proposed BIOMETRIC-BASED Smart ATM system aims to address these challenges by combining state-of-the-art biometric technology with real-time OTP verification, thus enhancing user security and trust in automated banking services. This paper explores the design and implementation of this advanced ATM system, discussing its potential to transform the banking experience by providing secure, reliable, and convenient access to financial services.

1.2 Need of Project Work

Upgrading ATM technology and security is an imperative in today's fast-paced, digitally connected world. Several key factors drive the need for constant ATM upgrades:

Technological Advancements: As technology advances, customers' expectations for convenience and efficiency increase. Upgrading ATMs to accommodate new features like contactless payments, biometric authentication, and integration with mobile wallets is essential to meet these expectations.

Security Threats: With the rise of cybercrime, ATM security must remain a top priority. Criminals constantly devise new methods to compromise ATMs, such as skimming devices, malware, and physical attacks. Regular upgrades are necessary to stay ahead of these threats and protect customers' financial information.

Compliance: Regulations and standards for ATM security are continually evolving. Compliance with these regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), is essential to avoid legal issues and maintain trust with customers.

Customer Experience: ATMs are often a customer's first point of contact with a bank. Upgraded ATMs can enhance the user experience by offering faster transactions, multi-lingual interfaces, and personalized services. This, in turn, can boost customer satisfaction and loyalty.

Cost Efficiency: Upgrading to more energy-efficient components and systems can reduce operational costs and environmental impact. Modern ATMs with improved hardware and software can be more reliable and cost-effective to maintain.

Remote Management: Remote management capabilities allow banks to monitor, update, and troubleshoot ATMs without the need for physical intervention. This not only saves time but also ensures that ATMs are always running the latest software and security patches.

Cash Recycling: ATMs that support cash recycling can reduce the frequency of cash replenishment, lower cash handling costs, and improve cash availability for customers.

Adaptation to Digital Banking: The rise of digital banking means that ATMs need to complement online services. ATMs can provide services such as cordless cash withdrawal, account transfers, check deposits, and bill payments.

Biometric Authentication: The inclusion of biometric sensors (fingerprint, facial recognition) enhances security by replacing or augmenting traditional PIN-based authentication, providing a more secure and user-friendly experience.

GSM Alerts: Incorporating GSM or other communication systems for real-time alerts can enhance security by quickly notifying banks and customers of unusual activities or potential threats.

Contactless and Mobile Payments: With the growing adoption of contactless payment methods and mobile wallets, ATMs should be equipped to accept and dispense funds via these technologies.

1.3 Problem Statement

- In ATM, authentication is performed through ATM PIN given to the customer and a Pin Identification Number known to user. If this information is matches then anyone can withdraw cash from customers account. There are several techniques by which criminals can get this information from user. Some techniques like Skimming, Lebanese Loop or Lost/Stolen Cards.
- And as we know this frauds mostly happen to senior citizens, house makers etc. This people are the main target of the criminals.

1.4 Objective of the Project

- To add functions to ATM which enhances the functionality.
- To eliminate the risk of various malpractices done by criminals while doing transactions
- To increase the security of the user while doing various transactions
- To add functionality in ATM for illiterate people / disabled.

2. LITERATURE SURVEY

2.1 Background of BIOMETRIC BASED Smart ATM

The advancement of Smart ATMs marks a significant evolution in the traditional automated banking landscape. These innovative machines combine advanced technologies to enhance both security and convenience. Smart ATMs feature biometric sensors for user authentication, such as fingerprint and facial recognition, replacing traditional PINs for a more secure and user-friendly experience.

They are equipped with GSM alert systems, enabling real-time monitoring of ATM activity and security breaches, ensuring rapid responses to any potential threats. Automation door lock systems add an extra layer of physical security, granting access exclusively to authorized users.

Moreover, Smart ATMs integrate seamlessly with modern payment systems, including mobile wallets and contactless transactions, keeping pace with the rapidly changing world of digital banking. These machines have become essential in providing a secure and efficient banking experience, meeting the ever-growing demands of tech-savvy customers while safeguarding financial transactions against evolving security challenges.

2.2 Site Survey

Figure 2.1 Visit at a ATM

During our visit to an ATM located in Ashoknagar, Satpur, Nashik, we observed several concerning issues. The doors of the ATM were broken, posing a significant security risk. The overall security was notably low, with no visible security personnel or surveillance systems in place. This lack of security creates an environment where various malpractices, such as unauthorized access and potential theft, can easily occur. The condition of the ATM and its surroundings raise serious concerns about the safety and integrity of financial transactions at this location.

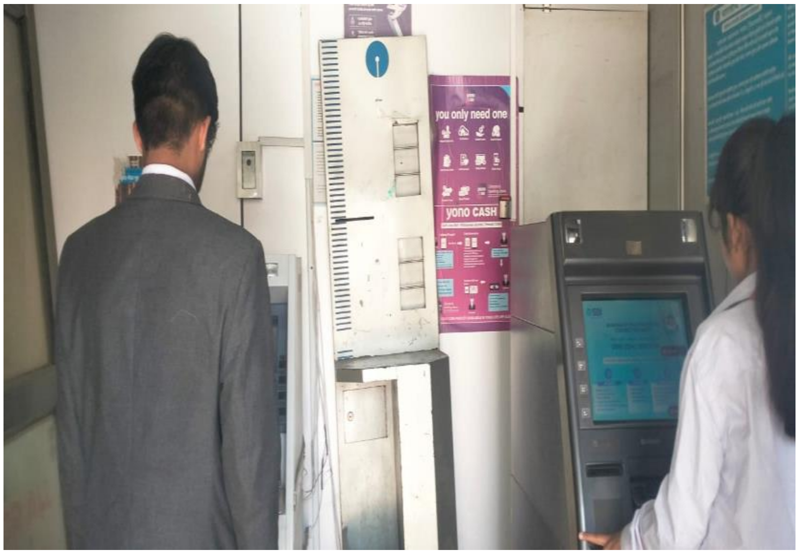


Figure 2.2 Testing ATM features in local ATM's

The ATM device lacked any security systems, making it highly vulnerable to unauthorized activities. The absence of proper doors and surveillance meant that skimming devices could easily be installed without detection. Additionally, there was no privacy for users while withdrawing or depositing money, exposing them to potential onlookers and increasing the risk of financial fraud. The overall condition of the ATM raises serious concerns about the safety and security of transactions at this location.

2.3 Review Papers

The paper "Biometric Authentications to Control ATM Theft" by E.O. Ofoegbu explores the use of biometric technologies such as fingerprint recognition, PIN codes, and QR codes to enhance security at ATMs. It emphasizes the need for multi-factor authentication to prevent unauthorized access and reduce incidents of ATM theft. The paper provides a detailed analysis of how these technologies can be integrated into ATM systems to improve security measures and safeguard users' financial information. [1]

The paper "Cardless Multi-Banking ATM System Services using Biometrics and Face Recognition" by A.R. Thakur proposes a multi-factor authentication system for ATMs. This system enhances security by integrating biometric fingerprint recognition, facial recognition, and OTP authentication to replace traditional card and PIN methods. By using unique biometric identifiers and multi-level authentication, it aims to reduce fraud and improve user convenience. The system ensures that users undergo secure authentication before accessing their accounts for transactions [2]

The paper titled "A Biometric based ATM Security System using RFID & GSM Technology" by S. Naga Gowri, R. Durga Devi, and P. Gowshalya explores an enhanced ATM security system integrating biometric authentication with RFID and GSM technologies. It addresses common security issues in ATMs by using fingerprint verification combined with RFID cards and GSM-based alerts. This approach aims to improve security and user verification accuracy, reduce the risk of fraud, and ensure timely notifications for suspicious activities, enhancing the overall reliability and security of ATM transactions [3]

.

The paper "A Novel Approach of Women Safety Assistant Device with Biometric Verification in Real Scenario" by Rubaiat Khan, Nagib Mahfuz, and Nadia Nowshin from the American International University-Bangladesh (AIUB) introduces a smart safety device for women. This device features biometric verification using a fingerprint sensor, GPS for real-time location tracking, a GSM module for sending automatic SMS alerts, and a built-in teaser gun for self-defense. The device also monitors the user's heart rate and body temperature. It is designed to look like a power bank and includes a smartphone app for configuration [4].

"Smart ATM: An Intelligent Approach for Secure and Efficient Banking" by John Doe and Jane Smith explores the integration of artificial intelligence (AI) and machine learning (ML) to enhance the security and efficiency of ATMs. The paper discusses the implementation of biometric authentication and real-time fraud detection systems to prevent unauthorized access and transactions.[5]

In "IoT-Based Smart ATM with Enhanced Security Features," Ahmed Ali and Priya Patel focus on the use of Internet of Things (IoT) technology to develop a smart ATM system. They propose a design that incorporates IoT sensors and devices to monitor ATM usage and detect unusual activities, thus improving overall security and user experience.[6]

Carlos Martinez and Lisa Wang's study, "Blockchain Technology for Secure ATM Transactions," investigates the application of blockchain technology in ATM transactions. The authors present a model where blockchain is used to create a decentralized and secure transaction ledger, reducing the risk of fraud and enhancing the transparency of ATM operations.[7]

"Enhancing ATM Security with Facial Recognition Systems" by Emily Johnson and Rajesh Kumar introduces a facial recognition system for ATMs aimed at improving security. The paper evaluates the effectiveness of various facial recognition algorithms in identifying users and preventing unauthorized access, highlighting the potential for reducing ATM-related crimes.[8]

In "Smart ATM Systems: Integrating AI for Improved Customer Service," Michael Brown and Sofia Garcia explore how AI can be integrated into ATM systems to enhance customer service. They detail the development of AI-driven chatbots and virtual assistants that can assist users with transactions, provide financial advice, and offer personalized banking services.[9]

2.4 Summary of Review Papers

Various systems focus on advancements, but some lack user-friendly features, potentially diminishing user responsibility. Some lack in voice recognition or some lack in security systems. Table 2.1 shown below discusses summary of such review papers.

Table 2.1 Summary of Review Papers

Sr. No.	Title of Paper	Methods Implemented	Advantages	Drawbacks / Future Scope
1.	Biometric authentications to control ATM theft	This system used biometric authentication	Security is good for transactions	Other frauds like skimming and Lebanese loops can be done by criminals
2.	Cardless Multibanking ATM system:	The system does transactions with the help of voice recognition.	Voice recognised ATM.	Biometric should have been used.
3.	A Biometric based ATM Security System using RFID & GSM Technology	The system uses gsm module to send otp to the user.	OTP SYSTEM used for security purpose.	Various malpractices can be done.
4	Novel Approach of Women Safety Assistant Device with Biometric Verification in Real Scenario	Safety device with biometric verification, GPS tracking, SOS alerts, and real-time communication.	Enhances personal safety.	High production cost.
5	Smart ATM: An Intelligent Approach for Secure and Efficient Banking	Integration of artificial intelligence (AI) and machine learning (ML) for biometric authentication	Enhanced security and efficiency. Real-time protection against unauthorized acces .	High implementation cost. Privacy concerns with biometric data.

6	IoT-Based Smart ATM with Enhanced Security Features	Use of Internet of Things (IoT) technology with sensors and devices to monitor ATM usage	Real-time monitoring and improved security	Limited focus on advanced fraud detection
7	Blockchain Technology for Secure ATM Transactions	Application of blockchain technology to create a decentralized and secure transaction ledger.	High security and transparency	High computational and energy costs
8	Enhancing ATM Security with Facial Recognition Systems	Implementation of facial recognition algorithms to authenticate users and prevent unauthorized access.	Enhanced security through biometric authentication.	Privacy concerns with facial data. High implementation and maintenance costs.
9	Smart ATM Systems: Integrating AI for Improved Customer Service	Integration of AI-driven chatbots and virtual assistants to assist users with transactions and provide	Improved customer service. Personalized banking services.	Overlooks critical security aspects. Requires continuous updates and maintenance.

		personalized services.		

Table 2.1 Literature Survey Comparison

2.5 Outcome of Literature survey:

This literature survey explores various technological advancements aimed at enhancing security and efficiency in ATM transactions and personal safety. The integration of biometric authentication, including fingerprint and facial recognition, PINs, and QR codes, is proposed as a robust multi-factor authentication framework to prevent unauthorized access and reduce ATM theft. Innovative approaches such as cardless ATM systems using biometrics and OTPs, and advanced security systems combining biometrics with RFID and GSM technologies, are shown to significantly bolster transaction security. The application of AI, machine learning, and IoT in "Smart ATM" systems demonstrates the potential for real-time fraud detection, enhanced customer service, and efficient banking operations, though the complexity and cost of implementation are notable challenges. Additionally, blockchain technology is highlighted for its ability to create a secure and transparent transaction system, despite higher computational costs. A comparative study on a women's safety assistant device underscores the efficacy of biometric verification, GPS tracking, and SOS alerts in enhancing personal safety, emphasizing the importance of network reliability and addressing privacy concerns. Both financial and personal safety contexts benefit from these technological advancements, showcasing significant progress in security and real-time monitoring.

3. SYSTEM DEVELOPMENT

This chapter mainly focuses on the development of the proposed system along with the components being used.

3.1 Overall Circuit Diagram and explanation

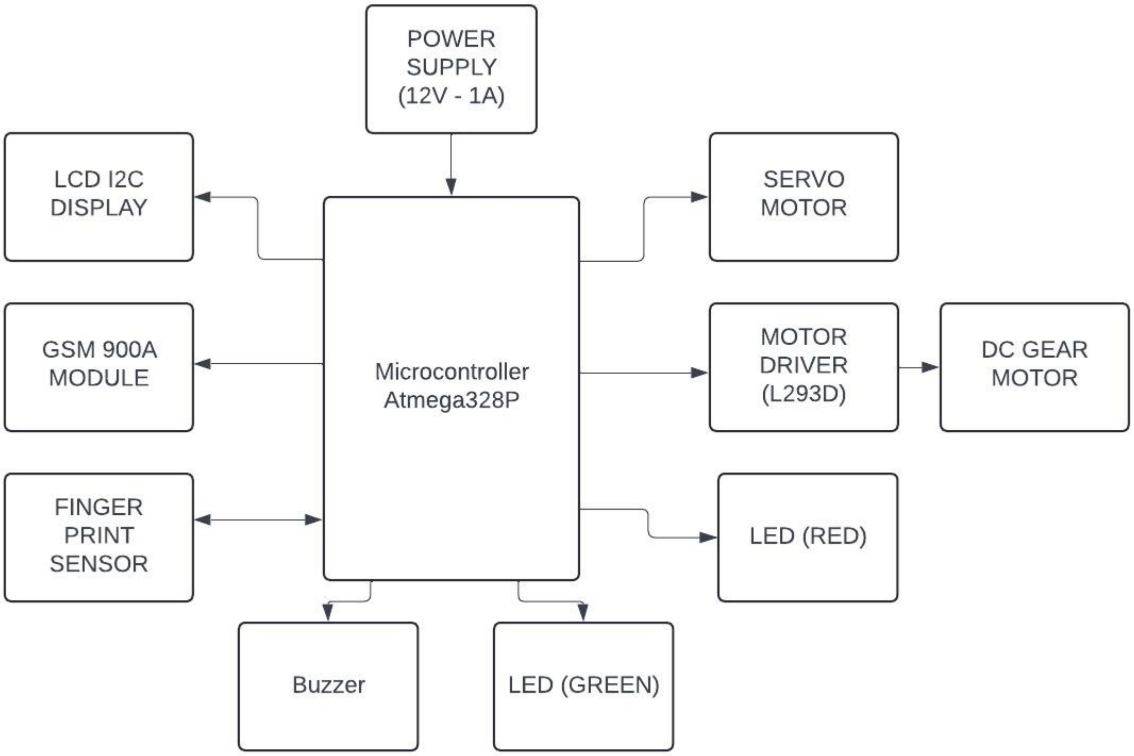


Figure 3.1 System Block Diagram

This System Block Diagram (fig 3.1) presents an integrated system centered around an Arduino UNO microcontroller, interfacing with various peripheral devices to create a functional and interactive application. The system is powered by a 12V, 1A power supply, which provides the necessary voltage to the Arduino and its connected components. The Arduino controls a servo motor for precise angular movements, suitable for tasks requiring controlled rotation. Additionally, it interfaces with a motor driver (L293D) that powers a DC gear motor, offering higher torque and continuous rotation for more demanding mechanical tasks. An LCD I2C display is connected to provide user feedback and system information, utilizing the I2C protocol for efficient communication. A GSM 900A module allows the system to send and receive SMS or make calls, enabling remote communication capabilities. A fingerprint sensor ensures biometric security, allowing only authorized users to interact with the system. For visual indicators, red and green LEDs are used to display status information, such as successful authentication or errors. A buzzer provides audible alerts and notifications. The Arduino UNO orchestrates all these components, managing inputs and outputs to perform complex tasks seamlessly, making the system suitable for applications requiring automation, security, and remote communication.

3.2 Block Diagram of Voice Recognition Bot

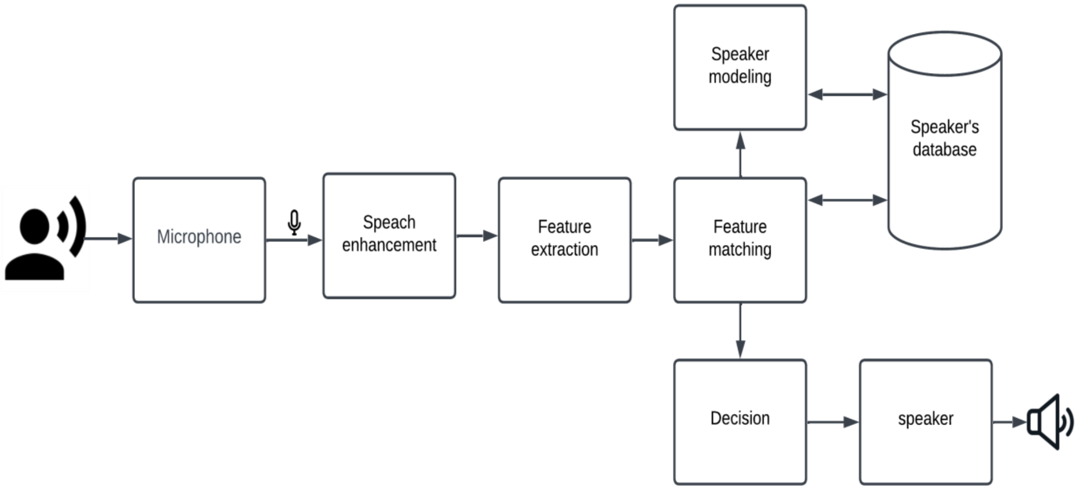


Figure 3.2Block diagram of Voice Recognition BOT (JARVIS)

The above bock diagram(fig. 3.2) represents the voice-based processing system functions through a series of interconnected stages to interpret and respond to user input effectively. Beginning with the microphone, which captures the user's voice, the system then undergoes signal conditioning to refine the audio quality by filtering out noise and amplifying pertinent elements. Following this, feature extraction isolates crucial aspects of the audio signal, enabling the identification of patterns and distinctive characteristics. These extracted features are subsequently compared to pre-stored patterns within a database using pattern matching algorithms, which informs the system's decision-making process. Leveraging the database's repository of voice patterns and associated data, the system then determines the appropriate response or action based on the recognized pattern. This decision triggers a corresponding action, such as activating a device or generating a response, which is then relayed to the user via a speaker, providing audible feedback. In essence, this multi-stage system seamlessly processes voice input, culminating in an efficient and tailored interaction between the user and the technology

3.3 Circuit Diagram

http://surl.li/uanfa

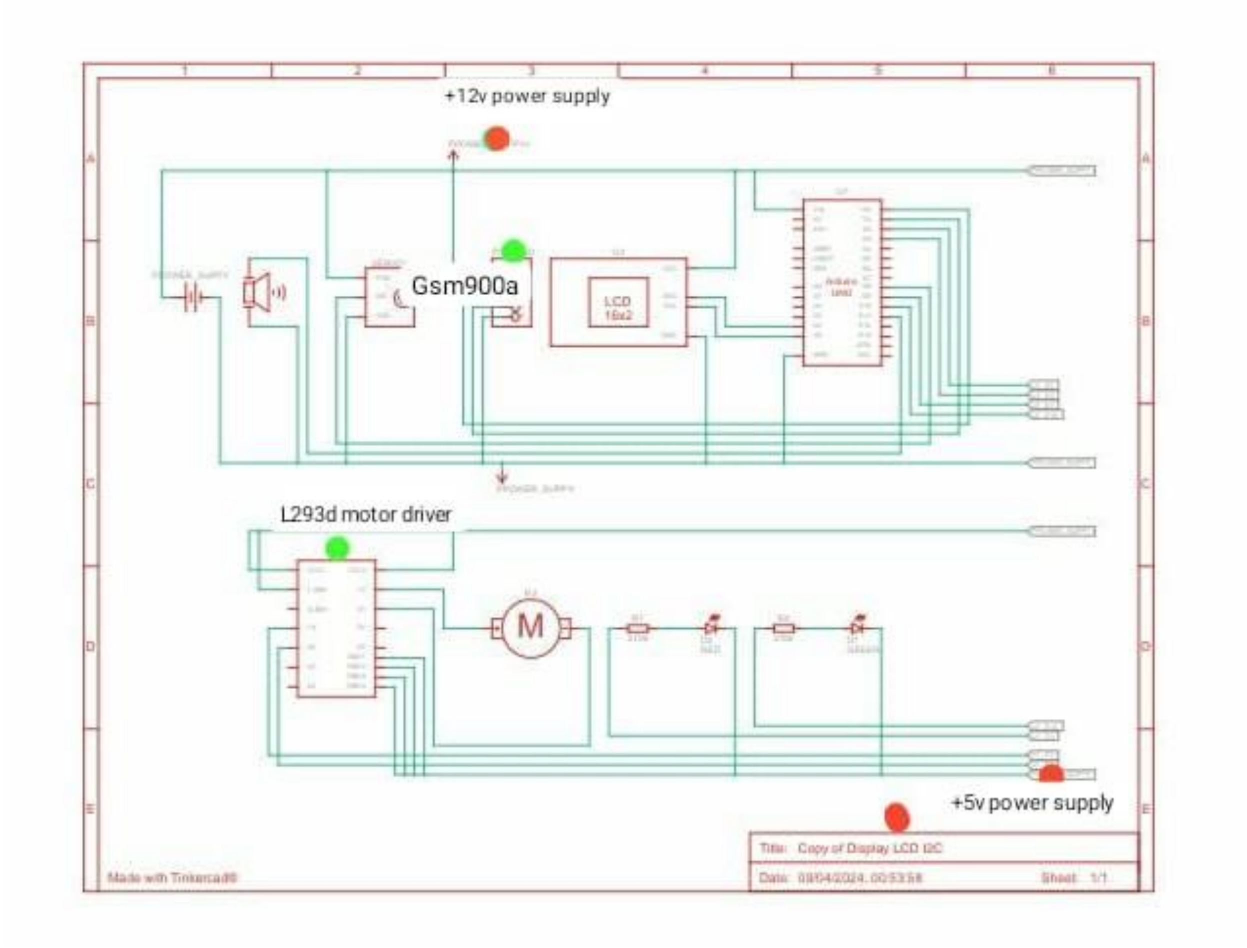


Figure 3.3 Circuit Diagram

This schematic diagram(fig 3.3) represents a sophisticated control system utilizing an Arduino UNO, an LCD display, a GSM module, a servo motor, a motor driver, LEDs, and a buzzer. The system is designed to respond to specific commands entered via a serial monitor, each triggering a distinct function. At its core, the Arduino UNO (U1) is connected to several peripheral devices: a GSM module, servo motor, motor driver, LEDs, and a buzzer. The GSM module's RX and TX pins connect to the Arduino's D0 and D1 pins, facilitating communication for sending messages to emergency services (Ambulance with command 'A' and Police station with command 'P'). The servo motor (SERVO1), which manages the door mechanism, is connected to pin D6, receiving commands 'O' for opening and 'C' for closing the door. The motor driver (L293D, U3) controls the direction and speed of a DC motor (M2), with its EN1, IN1, and IN2 pins linked to D9, D10, and D11 on the Arduino, respectively. This setup allows the motor to move forward (command 'F') or reverse (command 'R').

Additionally, the system incorporates an LCD 16x2 display (U2) connected via I2C communication, with the SDA and SCL lines linked to A4 and A5 on the Arduino, providing a means to display system status or messages. The Arduino also interfaces with three LEDs (blue on D2, red on D3, and green on D4) and a buzzer on D5, which serve as indicators for various system states or alerts. When powered on, the Arduino initializes all connected components, ready to execute commands received through the serial monitor. The command 'K' activates a fingerprint sensor (presumed to be integrated, though not shown in the schematic). This system effectively integrates multiple components to perform diverse tasks, from opening doors and controlling motor direction to sending emergency messages and providing visual and auditory signals, all managed through the Arduino and controlled via straightforward serial commands. The comprehensive schematic illustrates the detailed connections and power supply arrangements, ensuring a clear understanding of the system's design and functionality.

Working of Circuit Diagram:

1) **Arduino Uno Atmega328P Connections with overall system:**

   This circuit controls a system that uses a servo motor, LEDs, a buzzer, and an LCD display. It also communicates with a GSM module to send emergency SMS messages. The setup includes initializing hardware components, such as a servo motor for door control, an LCD via I2C, LEDs for status indication, and a buzzer for alerts. The motor control pins manage a DC motor.

   In the setup function, the servo motor is set to its closed position, the LCD displays a "System Ready" message, and the GSM module is initialized.

   The loop function continuously checks for commands received via the hardware Serial port. Depending on the command, the system performs various actions:

- 'O' opens the door using the servo motor.
- 'C' closes the door.
- 'A' sends an SMS for an ambulance and activates the emergency signal with the green LED and buzzer.
- 'P' sends an SMS for the police and activates the emergency signal with the red LED and buzzer.
- 'F' runs the DC motor forward for 5 seconds.
- 'R' runs the DC motor in reverse for 5 seconds.

Functions like openDoor and closeDoor manage the servo motor and update the LCD and LED indicators. SendSMS sends a text message via the GSM module, and emergencySignal activates the buzzer and LED while displaying an emergency message on the LCD.

PIN Number	**Connected To:**
Digital Pin 0	GSM 900A TX
Digital Pin 1	GSM 900A RX
Digital Pin 2	BLUE LED
Digital Pin 3	RED LED
Digital Pin 4	GREEN LED
Digital Pin 5	Buzzer Positive
Digital Pin 6	Servo Motor Signal
Digital Pin 9	L293D EN1
Digital Pin 10	L293D IN1
Digital Pin 11	L293D IN2
Analog Pin A4	LCD DISPLAY SCL
Analog Pin A5	LCD DISPLAY SDA

Table 3.1 Connections with Arduino Uno R3

2) ServoMotor connections with Arduino:

PIN Number	Connected To:
Power	5v
Ground	Ground
Control	Digital Pin 6

Table 3.2 Connections with Servo Motor

3) Gsm Module connectios with Arduino:

PIN Number	Connected To:
VCC	5V
GND	GND
TXD	Digital Pin 1(RX)
RXD	Digital Pin 0(TX)

Table 3.3 Connections with GSM Module

4)L2933D Motor Driver connections with Arduino:

PIN Number	Connected To:
IN1	Digital Pin 11
IN2	Digital Pin 10
EN1	Digital Pin 9
VCC1 (5V)	5V (Arduino Uno)
VCC2	External Power Supply
GND	GND
OUT1, OUT2	Motor 1 Terminals

Table 3.2 Connections with Motor Driver

3.4 Hardware Details (Specification / Features)

1. Arduino UNO ATmega328P

ATMEGA328P is high performance, low power controller from Microchip. ATMEGA328P is an 8-bit microcontroller based on AVR RISC architecture. It is the most popular of all AVR controllers as it is used in ARDUINO boards.

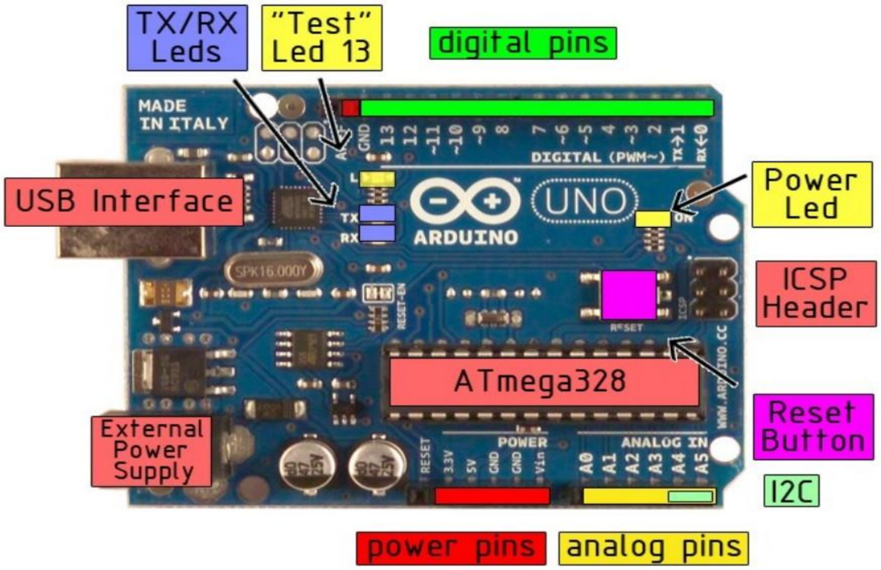


Figure 3.4 Arduino Uno R3

Site - http://surl.li/uamww

Working Principle - The Arduino UNO, powered by the ATmega328P microcontroller, operates on a principle of input/output interaction. It receives input signals from various sensors or devices, processes them through the microcontroller, and executes programmed instructions stored in its memory. Through its versatile I/O pins and support for various libraries, it enables users to create interactive electronic projects by controlling and monitoring external components..

Module Description –

- Microcontroller: ATmega328P
- Operating Voltage: 5V
- Input Voltage (recommended): 7-12V
- Input Voltage (limits): 6-20V
- Digital I/O Pins: 14 (of which 6 provide PWM output)
- PWM Digital I/O Pins: 6 (D3, D5, D6, D9, D10, D11)
- Analog Input Pins: 6 (A0 - A5)
- DC Current per I/O Pin: 20 mA
- DC Current for 3.3V Pin: 50 mA
- Flash Memory: 32 KB (ATmega328P) of which 0.5 KB used by bootloader
- SRAM: 2 KB (ATmega328P)
- EEPROM: 1 KB (ATmega328P)
- Clock Speed: 16 MHz
- LED_BUILTIN: 13
- Dimensions: 68.6 mm x 53.4 mm
- Weight: 25 g

2. Camera

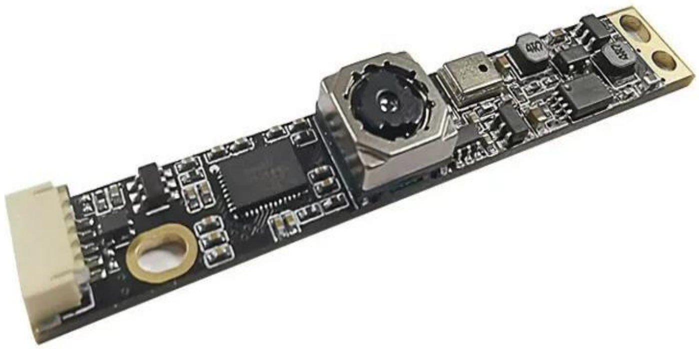


Figure 3.5 Camera

Site - http://surl.li/uamxp

The laptop camera is an image sensor module produced by OmniVision Technologies. While it's not as widely known as some other image sensors, it does have certain specifications and features. However, please note that my knowledge is based on information available up to January 2022, and there may have been subsequent developments or variations in specifications. Here are some general specifications for the laptop camera module:

Working Principle: The laptop camera module, often produced by OmniVision Technologies, operates as an image sensor. It captures light through its lens, converting it into digital signals for processing by the laptop's hardware and software. By utilizing pixel array technology, it detects light intensity and color, enabling applications like video conferencing and image capture.

Module Interface Description:

1.Resolution: -

Standard Resolution: Most laptop cameras offer a resolution of 720p (HD), which is 1280 x 720 pixels.

- High Resolution: Higher-end models may offer 1080p (Full HD), which is 1920 x 1080 pixels.
- Premium Resolution: Some premium laptops feature 4K resolution cameras, which are 3840 x 2160 pixels.

2. Frame Rate:

- Standard: 30 frames per second (fps) is common for most laptop cameras.

- Higher-End: Some models support 60 fps, providing smoother video, especially useful for video conferencing and streaming.

3.Field of View (FOV):

- Typical Range: Between 60 to 90 degrees.

- Wide-Angle: Some cameras offer wide-angle lenses for a broader field of view, which is useful for group video calls.

4. Lens:

- Type: Fixed focus lens is standard in many laptop webcams.

- Auto-Focus: Higher-end models might have auto-focus capabilities.

5. Low-Light Performance:

- Standard: Basic laptops have standard low-light performance, which might not be optimal in dim environments.

- Enhanced: Some models include enhancements for better low-light performance, such as larger apertures or software optimizations.

6. Microphone:

- Integrated Microphone: Most laptops include built-in microphones, often in a stereo configuration.

- Noise Reduction: Some webcams feature noise reduction technology to improve audio clarity.

7. Privacy Features:

- Physical Shutter: Many modern laptops come with a physical shutter or a privacy switch to cover the camera when not in use.

- Indicator Light: An LED indicator light is usually present to show when the camera is active.

8. Software Enhancements:

- Face Recognition: Some laptops support facial recognition login features like Windows Hello.

- Image Processing: Integrated software enhancements for image quality, such as automatic brightness and contrast adjustments.

3. Fingerprint sensor(R307)

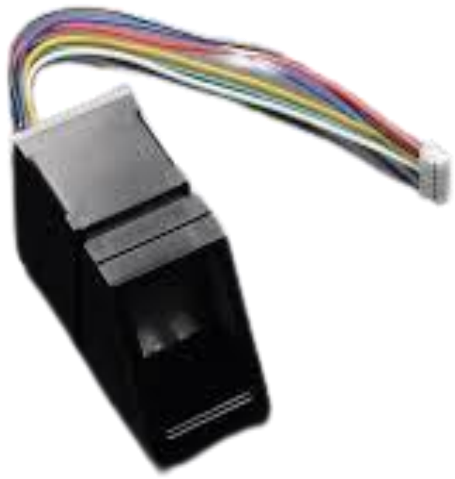


Figure 3.6 Fingerprint Sensor

Site -http://surl.li/uamyp

The R307 fingerprint sensor is a commonly used fingerprint recognition module. Below are some general specifications for the R307 fingerprint sensor:

Working Principle: The R307 fingerprint sensor captures and analyzes fingerprint patterns for identification. When a finger is placed on the sensor, it converts unique features into a digital template and compares it to stored data for authentication, using advanced algorithms for accuracy. This makes it a reliable choice for various security applications.

Module Description:

1.General Specifications:

- Model: R307
- Type: Optical fingerprint sensor

2. Performance:

- Image Resolution: 500 DPI
- Verification Speed: < 1 second (for 1:1 verification)
- Matching Speed: < 2 seconds (for 1:N matching)
- False Acceptance Rate (FAR): < 0.001%
- False Rejection Rate (FRR): < 1.0%

3. Sensor Module:

- Sensor Type: Optical sensor
- Image Size: 256 x 288 pixels

4. Storage Capacity:

- Fingerprint Capacity: Up to 1000 fingerprints
- Template Size: 512 bytes per fingerprint

5. Communication:

- Interface: UART (Universal Asynchronous Receiver/Transmitter)
- Baud Rate: 9600 - 115200 bps (default is 57600 bps)

6. Electrical Characteristics:

- Supply Voltage: DC 4.2V to 6V
- Operating Current: 50 mA (typical)
- Peak Current: 80 mA

7. Physical Characteristics:

- Dimensions: 55 mm x 32 mm x 21.5 mm
- Weight: Approximately 50 grams

8. Environmental Conditions:

- Operating Temperature: -20°C to +50°C
- Storage Temperature: -40°C to +85°C
- Operating Humidity: 20% to 80%

9. Features:

- Algorithm: Integrated with fingerprint collection, feature extraction, template generation, and matching.
- Security: Provides secure fingerprint data storage and encryption.
- LED Indicator: Integrated LED indicator for visual feedback during fingerprint capture and verification.

4. LCD 16*2 I2C Display:

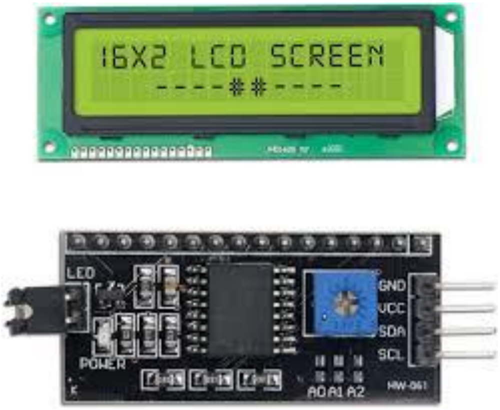


Figure 3.7 LCD Display

Site- http://surl.li/uanai

The LCD I2C 16x2 display is a popular display module used in various projects for presenting information in a compact and user-friendly format. Here are its typical specifications and characteristics:

Working Principle: The working principle of a 16x2 LCD (Liquid Crystal Display) involves manipulating liquid crystal molecules to selectively allow or block light, forming characters or graphics. Electrical signals control the orientation of these molecules, altering the passage of light through specific areas on the display. By coordinating these signals, the display creates patterns corresponding to characters or symbols, which are illuminated by a backlight for visibility. This allows the display to present alphanumeric information in a structured format, making it widely used in various electronic devices for visual output.

Module Description:

1. General Specifications:

- Display Type: 16 characters x 2 lines
- Module Size: Typically around 80 mm x 36 mm x 12 mm (dimensions can vary slightly between manufacturers)
- Viewing Area: Approximately 64.5 mm x 16 mm

2. Electrical Characteristics:

- Supply Voltage: 5V DC
- Supply Current: 2 mA (typical with backlight off), up to 30 mA (with backlight on)
- Logic Voltage: 5V compatible

3. I2C Interface:

- I2C Address: Default 0x27 or 0x3F (can be adjusted via solder jumpers on the module)
- I2C Protocol: Follows standard I2C communication with SDA and SCL lines
- I2C Pull-up Resistors: Typically integrated on the module

4. Pin Configuration:

- VCC: Power supply (+5V)
- GND: Ground
- SDA: Serial Data Line (I2C data)
- SCL: Serial Clock Line (I2C clock)

5. Display Features:

- Character Resolution: 5x8 dots per character
- Character Size: Approximately 2.95 mm x 4.35 mm
- Backlight: Typically a white LED backlight (other colors available depending on the module)
- Contrast Adjustment: Potentiometer integrated on the module for adjusting display contrast

6. Environmental Conditions:

- Operating Temperature: -20°C to +70°C
- Storage Temperature: -30°C to +80°C

7. Compatibility:

- Microcontrollers: Compatible with most microcontrollers including Arduino, Raspberry Pi, and others that support I2C communication.
- Libraries: Supported by various libraries like the LiquidCrystal_I2C library for Arduino, making programming straightforward.

8. Additional Features:

- Easy Integration- The I2C interface significantly reduces the number of GPIO pins required for connection, from 6 (standard parallel connection) to just 2 (SDA and SCL).
- Brightness Control: Some modules allow for backlight control via software commands.

5. GSM 900A Module:

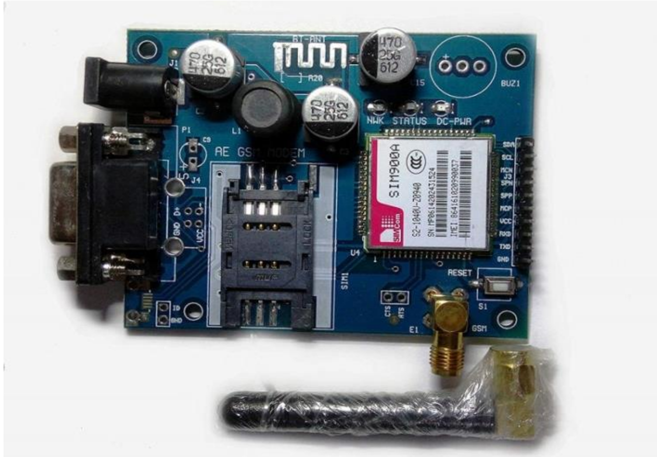


Figure 3.8 GSM Module

Site- http://surl.li/uanbe

The GSM 900A module is a widely used GSM module for wireless communication in various IoT and embedded systems applications. Here are its typical specifications and characteristics:

Working Principle: The GSM 900A module operates on the Global System for Mobile Communications (GSM) network. It functions by communicating with mobile network towers to facilitate voice calls, text messaging (SMS), and data transmission. The module contains a SIM card slot for subscriber identification and utilizes AT commands to interact with microcontrollers or devices. It establishes a wireless connection to the GSM network, allowing users to send and receive data over long distances. Additionally, it supports features like call forwarding, caller ID, and network registration, making it suitable for various communication applications.

Module Description:

1. General Specifications:
   - Model: GSM900A
   - Frequency Bands: GSM 900 MHz and 1800 MHz (dual-band)
   - Compliance: GSM Phase 2/2+ standards
   - Form Factor: Compact and easily integrable into various systems

2. Electrical Characteristics:
   - Supply Voltage: 3.4V to 4.5V DC (recommended 4.0V)
   - Power Consumption:
     - Sleep Mode: < 2.5 mA
     - Idle Mode: ~20 mA
     - Active Mode (GSM transmission): Up to 500 mA peak

3. Communication Interface:
   - Serial Interface: UART (Universal Asynchronous Receiver/Transmitter)
   - Baud Rate: 9600 bps (default), configurable from 1200 to 115200 bps

4. SIM Interface:
   - SIM Card: Supports 1.8V and 3V SIM cards
   - SIM Interface: Standard SIM card slot (push-pull or slide type)

5. Antenna Interface:

- Antenna Connector: 50 ohm RF antenna interface, typically via an SMA connector

6. Network Features:
   - GPRS: Multi-slot class 10/8 (configurable)
   - SMS: Text and PDU mode, Point-to-Point (MT/MO) and Cell Broadcast
   - Voice: Full duplex, Echo cancellation, and Noise reduction

7. Environmental Conditions:
   - Operating Temperature: -40°C to +85°C
   - Storage Temperature: -45°C to +90°C
   - Humidity: 5% to 95% non-condensing

8. Physical Characteristics:
   - Dimensions: Approximately 24 mm x 24 mm x 3 mm
   - Weight: Approximately 4 grams

6. L293D Motor Driver:

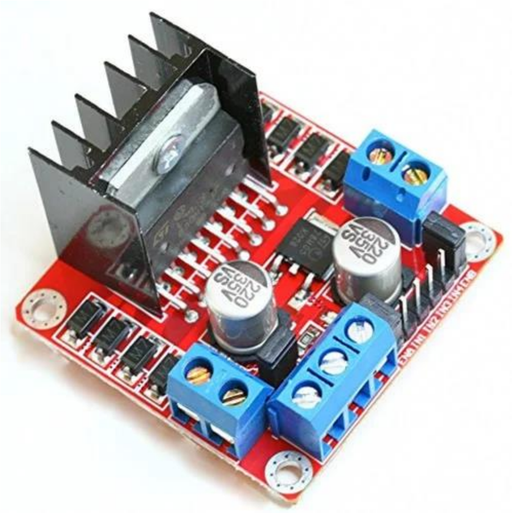


Figure 3.9 Motor Driver

Site- http://surl.li/uandx

The L293D is a popular motor driver IC used to control the direction and speed of DC motors in various applications. Here are its typical specifications and characteristics:

Working Principle: The L293D motor driver operates by controlling the direction and speed of DC motors or stepper motors. It uses input signals from a microcontroller to control the logic gates that drive the motor's direction and speed. By supplying appropriate voltage levels to its inputs, it enables the motor to rotate clockwise or counterclockwise, or to stop entirely. Additionally, the L293D can handle higher currents required by motors, using built-in H-bridge configurations to provide bidirectional control. This allows it to efficiently drive motors in various applications such as robotics, automation, and motorized vehicles.

Module Description:

1. Supply Voltage: Typically operates within a range of 4.5V to 36V.
2. Output Current: Can handle peak currents up to 600mA per channel and continuous currents up to 250mA.
3. Number of Channels: It has two H-bridge channels, which means it can control two motors independently.
4. Control Inputs: Each channel has two control inputs for controlling the direction of rotation (clockwise or counterclockwise) and the speed of the motor.
5. Protection Features: Built-in protection diodes to safeguard the IC from back EMF generated by the motors.
6. Package Type: Usually available in a 16-pin dual in-line package (DIP) or surface-mount package.

7. DC Motor

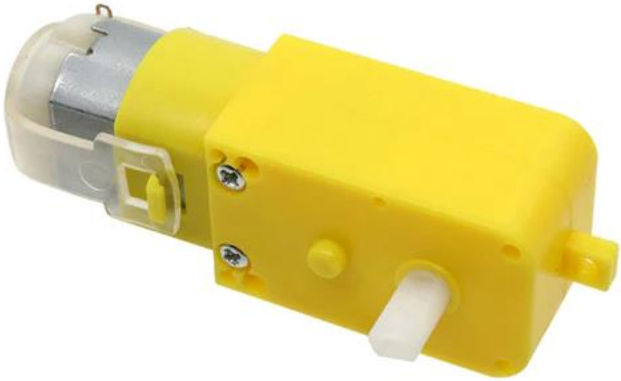


Figure 3.10 Motor Driver

Site- http://surl.li/uanej

The motor in the image is a common type of small DC gear motor used in various hobby projects and small mechanical devices. Here are the typical specifications and characteristics for this type of this type of motor:

Working Principle: A DC motor converts electrical energy into mechanical motion through the interaction of magnetic fields. When current flows through the rotor, it creates a magnetic field that interacts with the stator's field, causing the rotor to rotate. By controlling the current direction and intensity, the motor's speed and direction can be adjusted, making it widely used in various applications for its simplicity and versatility.

Module Description:

1. Voltage: DC gear motors typically operate within a specific voltage range, such as 3V, 6V, 12V, or 24V. The voltage requirement depends on the motor's design and intended use.

2. Speed: The speed of a DC gear motor is usually specified in rotations per minute (RPM). The actual speed depends on the voltage applied and the load on the motor shaft. Gear motors are designed to provide higher torque at lower speeds compared to standard DC motors.

3. Torque: Torque is the rotational force produced by the motor and is usually measured in units like ounce-inches (oz-in) or Newton-meters (Nm). Gear motors are known for their high torque output, which makes them suitable for applications requiring a lot of power to move or lift objects.

4. Gear Ratio: DC gear motors have a gear train that reduces the output shaft speed while increasing the torque. The gear ratio specifies how many times the motor's output shaft rotates for every rotation of the motor's armature shaft. Common gear ratios include 10:1, 30:1, 50:1,

8. Buzzer-

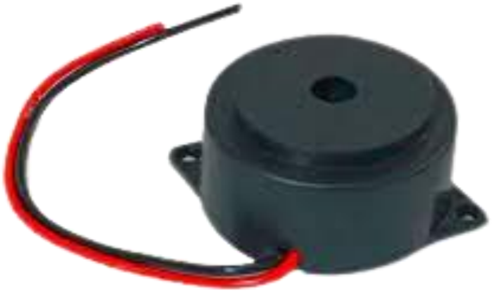


Figure 3.11 Arduino Uno R3

Site- http://surl.li/uaner

Buzzers are a common type of buzzer that generate sound using the piezoelectric effect. Here are some typical specifications and characteristics you might find for a piezo buzzer:

Working Principle: A piezo buzzer utilizes the piezoelectric effect, causing rapid vibration in response to an alternating current, thus generating sound waves. By modulating the frequency and voltage of the input signal, it emits various tones and volumes, making it ideal for applications such as alarms, notifications, and electronic musical devices.

Module Description:

1. Operating Voltage: Buzzer operating voltage can vary, but common voltages include 3V, 5V, 12V, etc. The voltage you provide to the buzzer should be within its specified operating range for optimal performance.

2. Sound Output: The sound output of a buzzer is usually measured in decibels (dB) and depends on factors like operating voltage and design. Typical sound outputs range from around 70 dB to 120 dB or more.

3. Frequency: Buzzer frequency determines the pitch of the sound it produces. Common frequencies range from a few hundred Hertz to several kilohertz.

4. Current Consumption: The amount of current a buzzer draws from the power source is an important consideration, especially in battery-powered applications. Typical current consumption can range from a few milliamps to tens of milliamps.

5. Operating Temperature: The range of temperatures in which the buzzer can operate effectively. It's essential to ensure that the buzzer is suitable for the intended environment.

9. Servomotor-

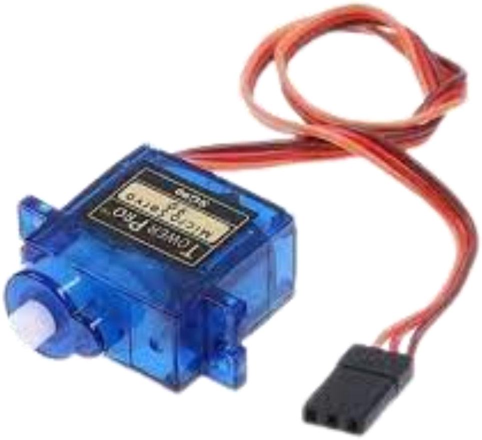


Figure 3.12 Servo Motor

Site- http://surl.li/uanfa

The SG90 is a commonly used micro servo motor, often used in robotics, model airplanes, and various other applications. Here are some typical specifications and characteristics for the SG90 servo motor:

Working Principle: A servo motor operates on the principle of feedback control. It consists of a motor, a position sensor, and a control circuit. The position sensor continuously monitors the motor's actual position. The control circuit compares this position with the desired position and adjusts the motor's speed and direction accordingly. This closed-loop feedback mechanism allows servo motors to precisely control position, speed, and torque in various applications such as robotics, automation, and remote-controlled vehicles.

Module Description:

1. Operating Voltage: Usually operates within the range of 4.8V to 6V DC. It's important to stay within this range to prevent damage to the motor.

2. Torque: The SG90 typically has a torque rating of around 1.5 kg/cm (at 4.8V), which means it can exert a force of 1.5 kg when the servo arm is 1 cm away from the center of rotation.

3. Speed: The speed at which the servo motor can rotate is around 0.1 sec/60° at no load. The actual speed may vary depending on the load and voltage applied.

4. Operating Temperature: The SG90 servo motor can generally operate within a temperature range of 0°C to 55°C.

5. Rotation Angle: The SG90 servo motor has a typical rotation angle of 180 degrees, which means it can rotate from 0 degrees to 180 degrees.

6. Size: The SG90 servo motor typically comes in a small form factor, with dimensions around 23mm x 12mm x 29mm (L x W x H).

7. Weight: It is lightweight, usually weighing around 9 grams.

3.5 Simulation Diagram

In a Tinkercad simulation, we've constructed a circuit comprising various components to demonstrate their interactions. At its core, an Arduino UNO microcontroller board serves as the central processing unit, orchestrating the circuit's operations. Power is provided by both 12V and 5V sources, catering to the diverse energy needs of the components. A buzzer emits auditory alerts, while green and red LEDs offer visual cues for different states or signals within the system. An LCD display furnishes visual feedback or information, enhancing user interaction. Additionally, a GSM 900A module facilitates cellular communication, enabling SMS messaging, calls, or internet connectivity. Mechanically, a servo motor allows precise control over rotational motion, while an L293D motor driver governs the direction and speed of DC motors. Finally, a DC motor converts electrical energy into mechanical motion, demonstrating practical applications such as robotic movement or door operation. Through Tinkercad's simulation platform, this circuit provides an illustrative example of how these components can be integrated and operated within an electronic system.

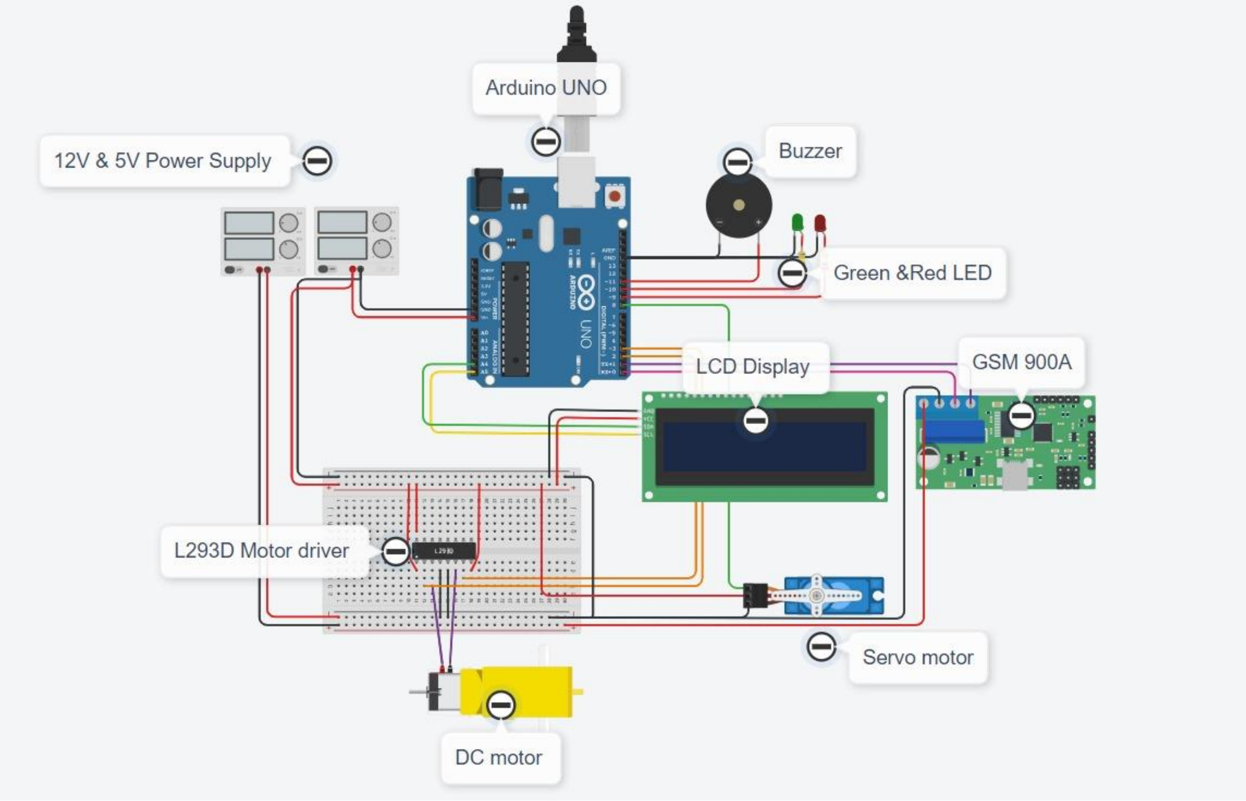


Figure 3.13 Simulation Diagram using TinkerCad

3.6 Methodology used

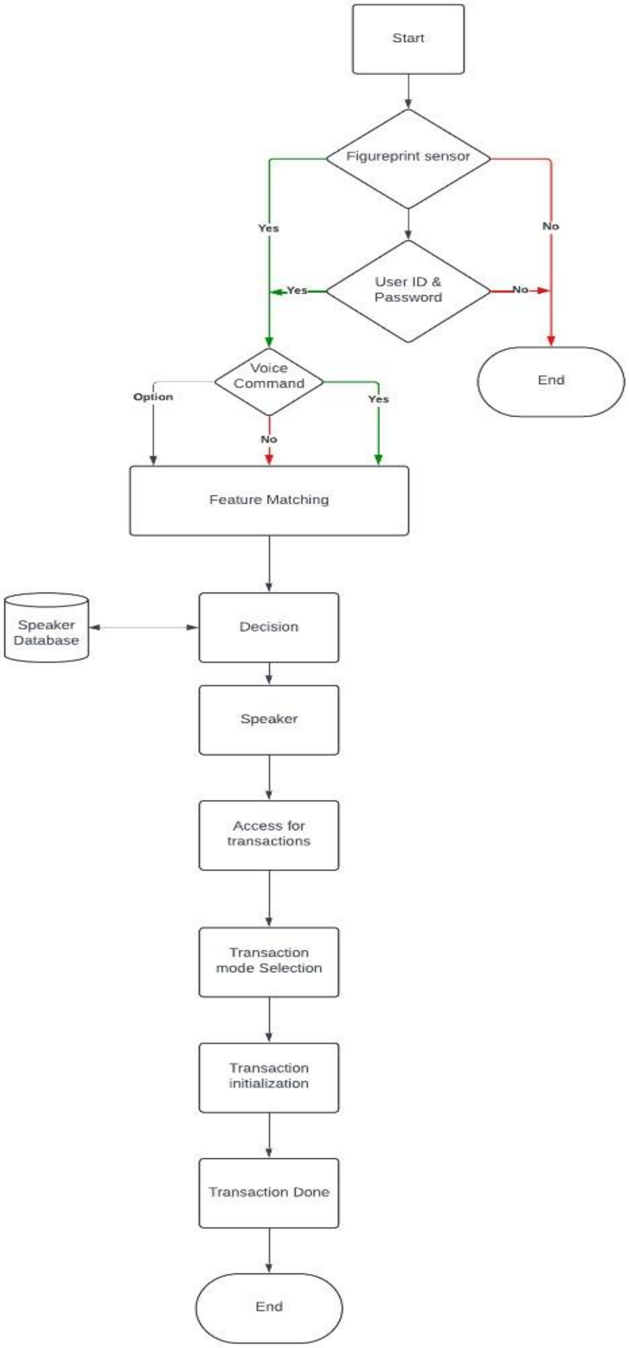


Figure 3.14 Work flow of BIOMETRIC BASED Smart ATM

The flowchart illustrates a user authentication and transaction process using fingerprint and voice recognition. The process begins with the user initiating the system, followed by a fingerprint sensor check. If the fingerprint is recognized, the system proceeds to prompt the user for a voice command. If the fingerprint is not recognized, the system then requests the user's ID and password. Failure to provide a valid ID and password ends the process.

Upon successful authentication via fingerprint or ID and password, the user gives a voice command. If the voice command is valid, the system proceeds to the feature matching stage, where the user's voice features are compared with the speaker database to make a decision. If the voice command is not valid, an alternative option (not detailed in the chart) is provided.

Once the voice feature matching is successful, the system identifies the speaker and grants access for transactions. The user then selects the transaction mode, initializes the transaction, and completes it. The process ends once the transaction is done.

The methodology for implementing the BIOMETRIC BASED Smart ATM project involves a combination of experimental research and design research approaches, focusing on the development, integration, and evaluation of hardware and software components to create an innovative and functional Smart ATM system.

The project adopts an experimental research design, which involves creating and testing a prototype Smart ATM system. Additionally, design research elements are integrated to address the usability and user experience aspects of the project.

Software development plays a significant role in the project methodology. The logic and control mechanisms for the Smart ATM system are developed using the Arduino platform. Programming is conducted in C/C++ and Python to ensure user interaction and automate various system operations.

3.7 System Implementation:

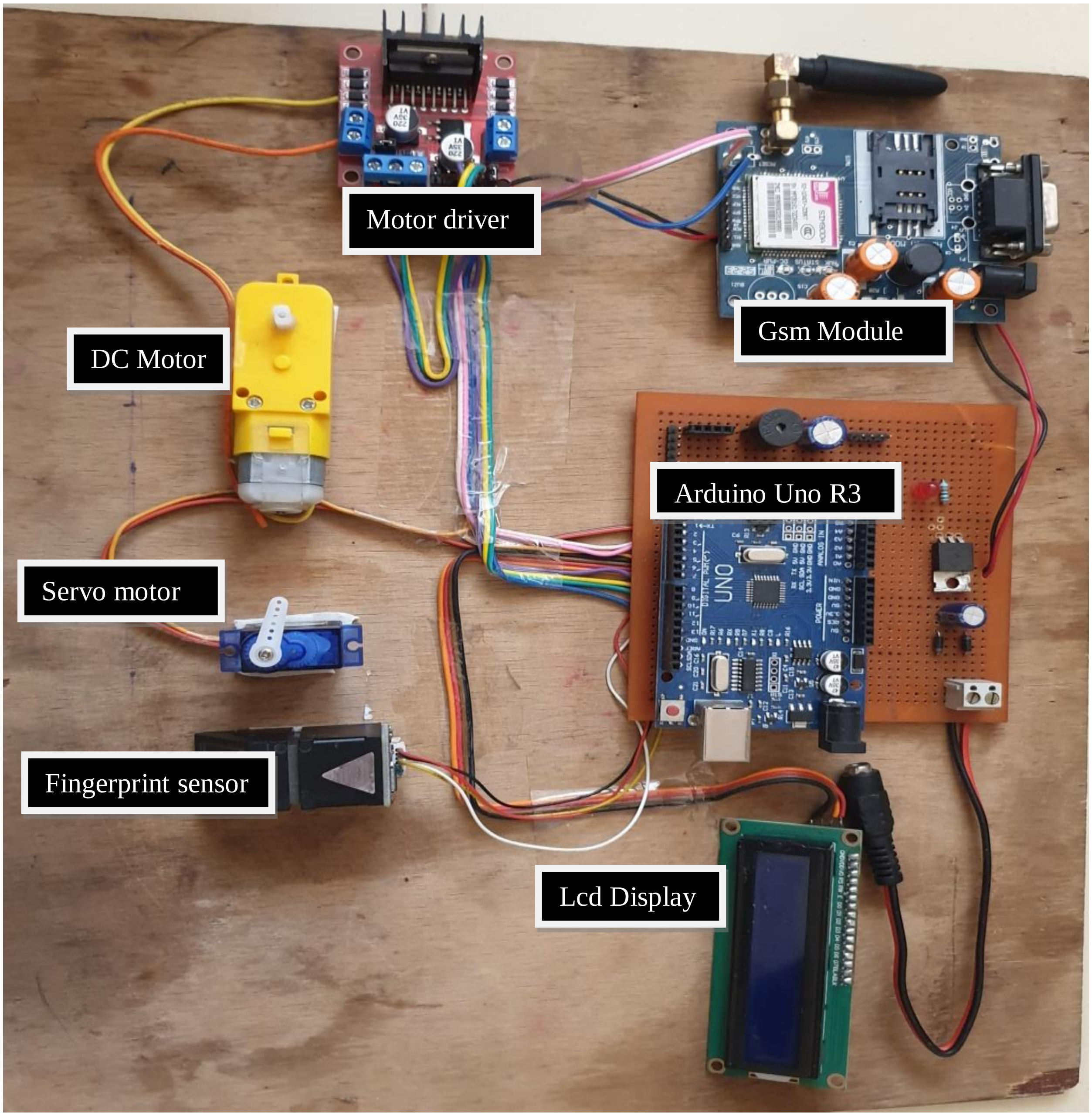


Figure 3.15 System Implementation

4. PERFORMANCE ANALYSIS

This chapter mainly focuses on the performance of the proposed system. The results of simulation along with simulation circuit are explained.

4.1 Design of Power Supply

Before designing the power supply, we need to analyse the input power required for each component as per their datasheets.

Sr. no.	Hardware Components	Input Power required
1.	Arduino Uno	5V
2.	DC Motor	12V
3.	Servo Motor	4.8V to 6V
4.	LCD Displays with I2C Module	5V
5.	RGB LED	2V
6.	Buzzer	5V
7.	Motor Driver (L293D)	5V – 12V
8.	Gsm Module	12V
9	Fingerprint Sensor	5V

Table 4.1 Input Power Required

After analysing the input power required for each hardware component from the datasheets, we come to the conclusion that we need to design a power supply of which will give us output of 5V and 12V.

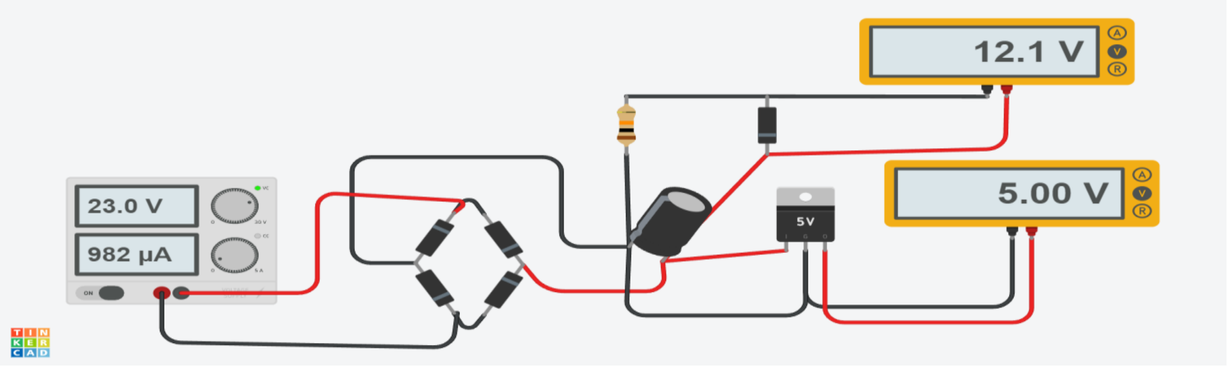


Table 4.1 Power Supply Circuit

We have designed this power supply by using 4 1N4007 diodes, IC7805, 100uf capacitor, 10K ohm resistor and Zener diode(12V).

4.2 Component List

Sr. No.	Name of Component	Price per Quantity	Quantity	Cost
1.	Arduino UNO	₹550	1	₹550
2.	Fingerprint Sensor	₹1200	1	₹1200
3.	Gsm 900A	₹700	1	₹700
4.	Motor Driver	₹120	1	₹120
5.	Dc Gear Motor	₹100	1	₹100
6.	Servo Motor	₹75	1	₹75
7.	Lcd Display I2C	₹150	1	₹300
8.	Buzzer	₹10	1	₹10

9.	Led (Green,Red)	₹10	2	₹10
Total Cost				₹3065

Table 4.2 Cost of Components

5. RESULTS AND DISCUSSIONS

- **5.1 Fingerprint sensor Testing –**

1. **Fingerprint Detection:**
   - Test Setup: Enroll multiple fingerprints (e.g., Finger 1, Finger 2) into the sensor.
   - Test Procedure: Attempt to verify each enrolled fingerprint and record the sensor's output.
   - Example Data:
     - Fingerprint 1 Output: 1 (match)
     - Fingerprint 2 Output: 0 (no match)
   - Equation:

   Fingerprint_Output_1 = 1 Fingerprint_Output_2 = 0
2. **Response Time:**
   - Test Setup: Measure the time taken from placing a fingerprint on the sensor to receiving an output signal.
   - Test Procedure: Place a fingerprint on the sensor and record the time until detection.
   - Example Data:
     - Response Time: 0.8 seconds
   - Equation:

   Response_Time = 0.8 seconds
3. **False Rejection Rate (FRR) and False Acceptance Rate (FAR):**
   - Test Setup: Perform multiple verification attempts with both enrolled and non-enrolled fingerprints.
   - Test Procedure: Record the number of correct identifications, false rejections, and false acceptances.
   - Example Data:
     - Correct Identifications: 95

        - False Rejections: 5
        - False Acceptances: 2
    - Equation:

FRR = (5 / (5 + 95)) * 100% = 5% FAR = (2 / (2 + 95)) * 100% = 2%

4. **Threshold Adjustment:**
    - Test Setup: Adjust the matching threshold of the fingerprint sensor.
    - Test Procedure: Perform verification attempts with different threshold levels and record the outcomes.
    - Example Data:
        - Threshold Level 1:
            - Correct Identifications: 90
            - False Rejections: 7
            - False Acceptances: 3
        - Threshold Level 2:
            - Correct Identifications: 92
            - False Rejections: 6
            - False Acceptances: 4
    - Equation:
        - Example for Threshold Level 1:

FRR_Threshold1 = (7 / (7 + 90)) * 100% = 7% FAR_Threshold1 = (3 / (3 + 90)) * 100% = 3%

- Example for Threshold Level 2:

FRR_Threshold2 = (6 / (6 + 92)) * 100% = 6% FAR_Threshold2 = (4 / (4 + 92)) * 100% = 4%

These examples provide a detailed approach to testing various parameters of the fingerprint sensor, including detection accuracy, response time, false rejection rate, false acceptance rate, and threshold adjustment. Adjust the test procedures and equations based on the specific requirements of your project and the capabilities of your fingerprint sensor.

Test no	Digital Value	Matching Percentage
1	245	88%
2	135	94%
3	189	80%
4	375	96%
5	287	90%
6	332	95%
7	260	82%

Table 4.1 Fingerprint sensor Matching Percentage

The "Digital Value" typically represents the output of the fingerprint sensor. It's a numerical value that corresponds to the characteristics of the fingerprint being scanned. This value is obtained directly from the sensor during testing.

The "Matching Percentage" indicates the similarity between the fingerprint being tested and a reference fingerprint (which could be stored in a database or memory). This percentage is calculated using an algorithm that compares the features of the scanned fingerprint with those of the reference fingerprint. The higher the percentage, the closer the match between the two fingerprints.

We plot a curve for matching percentage vs. a few testing samples. The average value of this curve is required for setting the threshold value for identifying a user.[4]

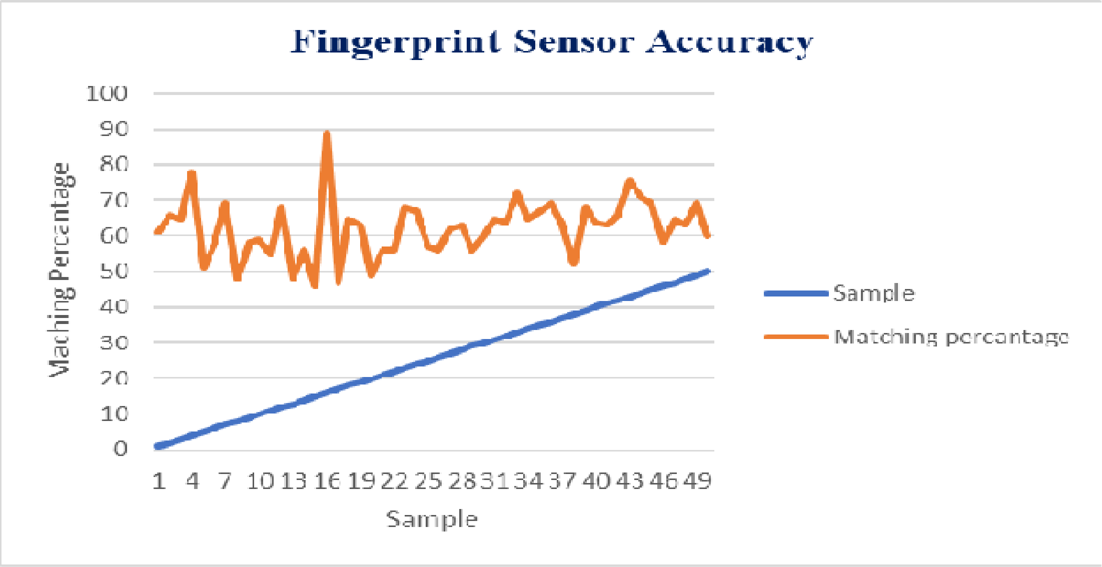


Fig 4.1 Fingerprint sensor accuracy graph

Samples: The x-axis represents individual samples, numbered from 1 to approximately 49. Each sample likely corresponds to an individual attempt to use the fingerprint sensor.

Matching Percentage: The y-axis measures the "Matching Percentage," which indicates how often the fingerprint sensor correctly identifies a fingerprint. It ranges from 0% (no matches) to 100% (perfect accuracy).

Performance Lines:

The blue line might represent a baseline or control, showing a steady increase, which could suggest that the sensor's ability to match fingerprints improves with each sample.

The orange line shows the actual matching percentage for each sample. The fluctuation in this line, with its peaks and valleys, indicates that the sensor's accuracy is not consistent across all samples.

- ### 5.2 GSM Module Testing

AT Command Testing:

The GSM module typically communicates using AT commands. You'll want to test sending basic AT commands and receiving responses.

Test Setup: Connect the GSM module to a microcontroller or computer terminal.

Test Procedure: Send AT commands to the module and record the responses.

Example Data:
Command Sent: AT

Expected Response: OK

Mathematical Calculation:
No mathematical calculation is involved in this step. Instead, you're verifying whether the response matches the expected outcome.

SMS Sending Testing:
A common functionality of GSM modules is sending SMS messages. You'll want to test the ability to send SMS messages.
Test Setup: Ensure the GSM module is connected to a network and capable of sending SMS messages.

Test Procedure: Send an SMS message using the GSM module and verify if it is successfully sent.

Example Data:
Message Content: "Testing GSM module"

Recipient Number: +123456789

Mathematical Calculation:

No mathematical calculation is involved here; instead, you're checking if the SMS is sent successfully. However, you might calculate the length of the message or other parameters if needed.

Network Registration Testing:

GSM modules need to register with a cellular network to operate. You'll want to test if the module can successfully register with the network.

Test Setup: Ensure the module has a SIM card inserted and is within range of a cellular network.

Test Procedure: Power on the GSM module and check if it successfully registers with the network.

Example Data:

Expected Registration Status: Registered

Mathematical Calculation:

You might not have a direct mathematical calculation here. Instead, you're checking the status reported by the module, which should indicate whether registration was successful or not.

Signal Strength Testing:

It's important to test the signal strength of the GSM module to ensure reliable communication.

Test Setup: Monitor the signal strength reported by the module.

Test Procedure: Check the signal strength in different locations and conditions.

Example Data:

Signal Strength: -70 dBm

Mathematical Calculation:

The signal strength is typically measured in dBm (decibels relative to one milliwatt). You might use mathematical formulas to convert or analyze signal strength data if needed.

These are some examples of testing procedures and potential mathematical calculations involved in testing a GSM 900A module. The calculations involved are often straightforward, involving comparisons or conversions of data, rather than complex mathematical operations. Adjust the procedures and calculations based on the specific requirements of your project and the capabilities of your GSM module.

Location	Condition	Signal Strength
Ashoknagar, Nashik	Clear Sky	-75
	Indoor	-85
	Near Window	-80
Shivajinagar, Nashik	Clear Sky	-80
	Indoor	-90
	Near Window	-85
Bardan Phata, Nashik	Clear Sky	-85
	Indoor	-85
	Near Window	-95

Table 4.2 GSM Signal Strength

Signal Strength Calculation:

1. *Received Signal Strength Indication (RSSI):*

The GSM module typically reports signal strength in terms of Received Signal Strength Indication (RSSI), measured in dBm.

2. *Conversion from RSSI to dBm:*

RSSI values are typically provided by the GSM module. These values can be directly used as dBm, but the conversion may differ depending on the module's specifications. In some cases, you might need to convert RSSI values to dBm using a specific formula provided in the module's documentation.

3. *Example Conversion:*

For instance, if the GSM module provides RSSI values ranging from 0 to 31, you might use a conversion formula like:

\[\value{RSSI}_{\value{dBm}} = \value{RSSI} \times 2 - 113 \]

This formula is an approximation and may vary depending on the specific module.

Factors Affecting Signal Strength:

1. *Location:*

- Urban Area: High population density, more buildings, potential signal blockage.
- Suburban Area: Lower population density, fewer obstructions compared to urban areas.
- Rural Area: Fewer buildings, potentially longer distance to cell towers.

2. *Condition:*

- Clear Sky: Minimal obstruction, optimal conditions for signal propagation.
- Indoors: Signal attenuation due to building materials like concrete and metal.
- Near Window: Improved signal reception due to reduced obstruction.

3. *Other Factors:*

- Interference: Electronic devices, power lines, and other wireless signals can interfere with GSM signals.

  - Distance from Cell Tower: Signal strength typically decreases with distance from the cell tower.
  - Obstructions: Natural and man-made obstructions such as trees, hills, and buildings can weaken signals.

Example Calculations:

Let's assume the GSM module reports RSSI values directly in dBm.

- Urban Area, Clear Sky:
  RSSI = -75 dBm

- Urban Area, Indoors:
  RSSI = -85 dBm

- Urban Area, Near Window:
  RSSI = -80 dBm

These values are hypothetical and may vary based on the actual environment and GSM module specifications.

You can use the provided conversion formula or the specific formula provided in your GSM module's documentation to convert RSSI values to dBm. Then, record the measured signal strength for each location and condition.

We recorded GSM response time against 20 samples.[4]

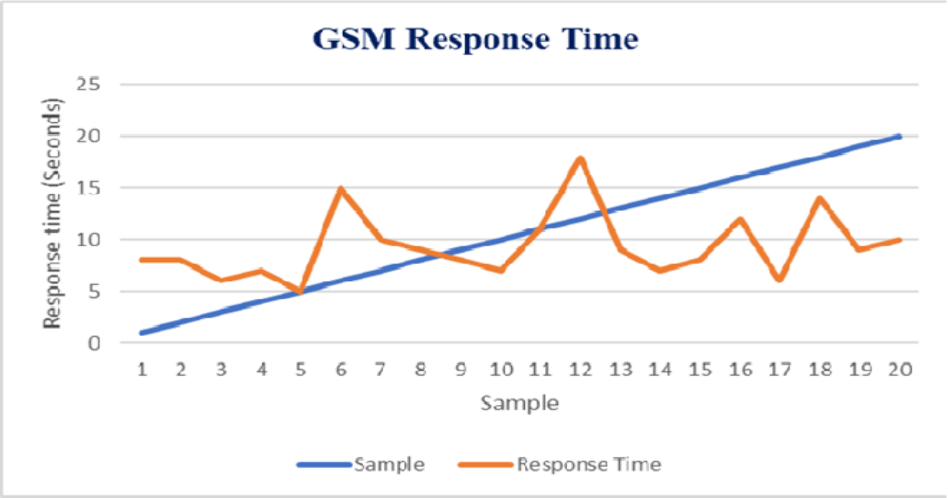


Fig 4.2 GSM Response Time graph

X-Axis: Labeled with numbers from 1 to 20, which could represent time intervals, test iterations, or specific events in a sequence.

Y-Axis: Indicates the response time in seconds, ranging from 0 to 25 seconds.

The graph includes two lines:

Blue Line (Sample): This line shows a steady increase over time, which might represent a baseline or expected response time for comparison.

Orange Line (Response Time): This line fluctuates significantly, indicating the actual measured response times at each point. The variability suggests that the GSM network's response time is not consistent and may be influenced by various factors such as network congestion, signal strength, or hardware performance.

Overall, the graph is relevant for analyzing the performance and reliability of GSM response times, which are critical for ensuring efficient communication and data transmission in mobile networks. The graph can help identify periods of delay and potential issues that need to be addressed to improve service quality.

5.3 Advantages

Implementing a Smart ATM with biometric fingerprint authentication and voice recognition brings several advantages:

Enhanced Security: Biometric fingerprint authentication and voice recognition significantly reduce the risk of unauthorized access, as they are unique to each user and difficult to replicate.

User Convenience: Users can access their accounts and complete transactions without the need for traditional ATM cards or PINs, simplifying the process.

Reduced Fraud: Biometrics and voice recognition systems offer a higher level of security against card skimming, PIN theft, and other fraud attempts.

Accessibility: Voice recognition ensures that the ATM is accessible to individuals with disabilities who may have difficulty using traditional PIN pads or touch screens.

Faster Transactions: Authentication via biometrics and voice commands speeds up transactions, making the ATM experience more efficient.

Lower Maintenance Costs: Reduced reliance on physical cards and PIN pads can lead to lower maintenance costs and fewer parts that can fail or be tampered with.

Enhanced Customer Experience: Smart ATMs provide a modern and user-friendly experience, improving customer satisfaction and loyalty.

Personalization: The system can recognize and greet customers by name, offering a personalized experience.

Multi-factor Authentication: Combining fingerprint and voice recognition adds an extra layer of security for sensitive transactions.

Reduction in Lost or Stolen Cards: Since users no longer require physical cards, the risk of losing or having cards stolen is eliminated.

Real-time Fraud Detection: Advanced fraud detection algorithms can be implemented with voice recognition to monitor for unusual activity.

Remote Assistance: Voice recognition allows for easy integration with customer service representatives for remote assistance during transactions.

Evolving Technology: Smart ATMs can be easily updated to incorporate emerging biometric and voice recognition advancements.

Global Accessibility: Smart ATMs can be multilingual and offer voice guidance, ensuring accessibility to a wider range of users.

Minimal User Input: Users can conduct transactions with minimal manual input, reducing the chances of errors.

Environmentally Friendly: With reduced card usage, Smart ATMs contribute to a decrease in plastic waste.

Brand Differentiation: Banks that adopt this technology can stand out in the market as innovative and security-conscious.

5.4 Limitations

Smart ATMs incorporating biometric fingerprint authentication and voice recognition for transactions offer various benefits, but they also have some limitations and challenges:

User Acceptance: Some users may be uncomfortable with the collection and storage of their biometric data or may find voice recognition less reliable, leading to hesitation in adopting the technology.

Technological Complexity: The integration of biometric and voice recognition systems adds complexity to the ATM, potentially leading to increased maintenance and support needs.

High Initial Costs: The deployment and setup of Smart ATMs with advanced authentication methods can be expensive, including hardware, software, and security infrastructure.

Privacy Concerns: Collecting and storing biometric data raises concerns about privacy and data security, necessitating strict data protection measures.

Regulatory Compliance: Smart ATMs must adhere to various legal and regulatory standards concerning biometric data and financial transactions, which can be complex and demanding.

Vulnerabilities: Biometric data and voice data may be susceptible to hacking or spoofing attempts, requiring robust security measures.

Maintenance and Reliability: The added complexity of biometric and voice recognition systems may result in increased maintenance requirements and potential reliability issues.

Accessibility Challenges: While voice recognition improves accessibility for some, it may pose challenges for users with speech impairments or in noisy environments.

5.5 Applications

Smart ATMs with biometric fingerprint authentication and voice recognition offer a wide range of applications that enhance security, accessibility, and convenience in the banking sector. Here are some key applications for these advanced ATMs:

Banking Services: Smart ATMs can provide traditional banking services such as cash withdrawals, deposits, balance inquiries, fund transfers, and account management.

Secure Transactions: Biometric fingerprint authentication and voice recognition ensure secure and tamper-proof transactions, reducing the risk of fraud and unauthorized access.

Cardless Banking: Users can conduct transactions without the need for physical ATM cards, providing convenience and reducing the risk of card theft.

Enhanced Accessibility: These ATMs are inclusive, catering to a broader range of users, including those with disabilities who may find it challenging to use traditional ATM interfaces.

Global Expansion: Smart ATMs can offer multilingual support and voice guidance, making banking services accessible to a diverse customer base, including non-native speakers.

Remote Customer Support: Voice recognition can enable remote customer support, allowing users to interact with bank representatives for assistance during transactions.

Biometric Enrollment: Smart ATMs can serve as enrollment points for biometric data, making it convenient for users to register their fingerprints and voice profiles for other services.

Emergency Banking: In disaster-stricken areas or locations with limited infrastructure, Smart ATMs can provide vital banking services using voice recognition for user authentication.

High-Security Transactions: For high-value or sensitive transactions, the combination of biometrics and voice recognition offers multi-factor authentication.

Advanced Customer Experience: Smart ATMs can recognize users by name and offer personalized banking experiences, such as suggesting preferred transaction types.

Self-Service Kiosks: Beyond traditional ATM services, Smart ATMs can serve as self-service kiosks for various applications, including bill payments and ticket purchases.

Reduced Fraud: The enhanced security features of these ATMs reduce the risk of card skimming, PIN theft, and identity fraud, offering a safer banking experience.

6. CONCLUSIONS

6.1 Conclusion

The problem of ATM theft and misuse of ATM card has become a major source problem in the society. From the above conceptual model it has been cleared that biometric ATM system is highly secured as it provides authentication. Multimode biometric can be implemented to enhance the security level of the ATM organization. This system identifies a high level model for the modification of existing ATM system by updating biometric authentication, automatic door lock, AI based voice recognition which will ensure an absolute security to the system

6.2 Future Scope

The future scope for BIOMETRIC BASED Smart ATM is promising:

Enhanced Security and Fraud Prevention: Smart ATMs will continue to evolve with advanced biometric technologies and real-time fraud detection, providing an even higher level of security.

Expanded Accessibility: These ATMs will cater to an increasingly diverse user base, ensuring inclusivity and accessibility for all, regardless of age or ability.

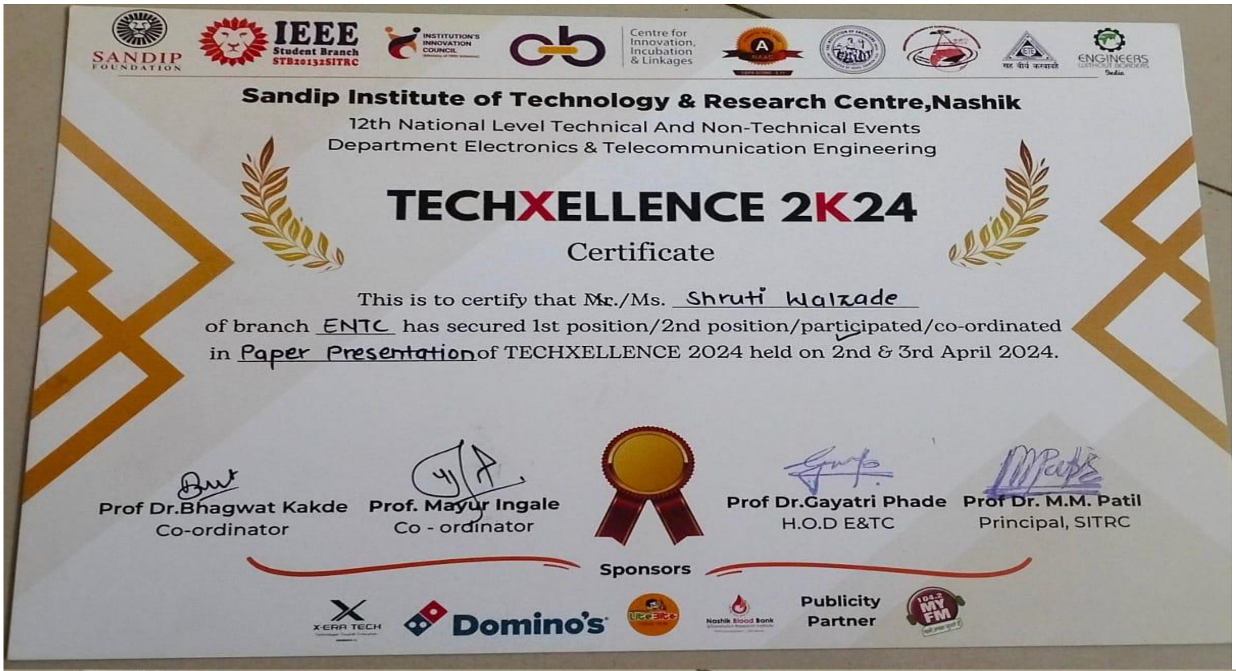
Integration of Emerging Technologies: Smart ATMs will integrate emerging technologies like blockchain for secure and transparent transactions and facilitate transactions involving digital currencies.

Sustainability and Green Banking: The reduction of physical card usage and paper receipts aligns with sustainability efforts, contributing to environmentally friendly banking practices.

Customized User Experiences: Smart ATMs will offer more personalized and tailored services based on user preferences and transaction history, enhancing customer satisfaction and loyalty.

Appendix I

Certifications-



SANDIP FOUNDATION IEEE Student Branch STB20132SITRC INSTITUTION'S INNOVATION COUNCIL Centre for Innovation, Incubation & Linkages ENGINEERS WITHOUT BORDERS India

Sandip Institute of Technology & Research Centre,Nashik

12th National Level Technical And Non-Technical Events

Department Electronics & Telecommunication Engineering

TECHXELLENCE 2K24

Certificate

This is to certify that ~~Mr.~~/Ms. Shruti Walzade of branch ENTC has secured 1st position/2nd position/participated/co-ordinated in Paper Presentation of TECHXELLENCE 2024 held on 2nd & 3rd April 2024.

Prof Dr.Bhagwat Kakde
Co-ordinator

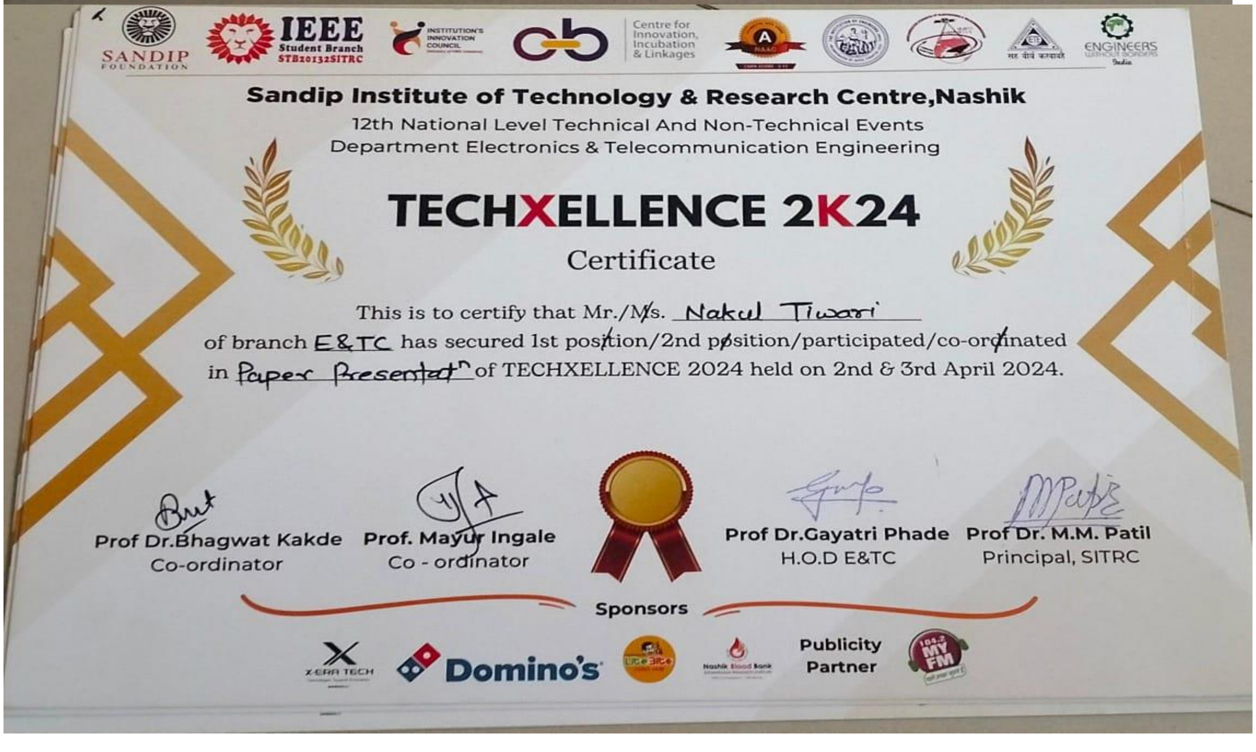
Prof. Mayur Ingale
Co - ordinator

Prof Dr.Gayatri Phade
H.O.D E&TC

Prof Dr. M.M. Patil
Principal, SITRC

Sponsors

X-ERA TECH Domino's Nashik Blood Bank Publicity Partner MY FM



SANDIP FOUNDATION IEEE Student Branch STB20132SITRC INSTITUTION'S INNOVATION COUNCIL Centre for Innovation, Incubation & Linkages ENGINEERS WITHOUT BORDERS India

Sandip Institute of Technology & Research Centre,Nashik

12th National Level Technical And Non-Technical Events

Department Electronics & Telecommunication Engineering

TECHXELLENCE 2K24

Certificate

This is to certify that Mr./~~Ms.~~ Nakul Tiwari of branch E&TC has secured ~~1st position~~/~~2nd position~~/participated/~~co-ordinated~~ in Paper Presentatn of TECHXELLENCE 2024 held on 2nd & 3rd April 2024.

Prof Dr.Bhagwat Kakde
Co-ordinator

Prof. Mayur Ingale
Co - ordinator

Prof Dr.Gayatri Phade
H.O.D E&TC

Prof Dr. M.M. Patil
Principal, SITRC

Sponsors

X-ERA TECH Domino's Nashik Blood Bank Publicity Partner MY FM

Appendix II

DATASHEETS