IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

# AI-Enhanced Fingerprint Authentication for Exam Hall Security

**Dinesh.R[1], Logeeshwara.PA[2], Rishi S Chandran[3], Sowresh.S[4], Srinivas.R[5]**

Assistant Professor, Mechanical department, SNS College of Technology, Coimbatore, India.[1]

UG scholar, Mechanical department, SNS College of Technology, Coimbatore, India.[2-5]

**Abstract:** Academic integrity has grown to be a major concern in educational institutions all over the world in recent years. Since technology has advanced, conventional techniques for administering and overseeing exams have shown to be insufficient in discouraging cheating and guaranteeing fairness. This work suggests a unique fingerprint-based biometric method for exam sheet identification in order to address these issues.The suggested method makes use of each student's own fingerprint pattern to reliably identify and authenticate exam sheets. The integration of fingerprint recognition technology into exam administration procedures allows educational institutions to improve security, stop fraud, and maintain student integrity. Compared to traditional methods, this strategy has a number of benefits, including improved accuracy, efficiency, and dependability.The method of using the system involves several steps, the first of which is enrolling students' fingerprints into a centralized database. Students' fingerprints are taken during exam registration and linked to the appropriate exam sheet. Students must use a biometric scanner attached to the exam sheet distribution system to verify their identity on test day by touching their finger on it. After the student authenticates, the system confirms their identification and obtains the relevant exam sheet from a safe deposit box. This removes the chance of confusion or illegal access by guaranteeing that every student receives their assigned exam sheet. In order to prevent cheating and ensure an equitable testing environment, the system continuously scans for any suspicious activity or attempts at malpractice throughout the exam period. Apart from augmenting security and upholding academic integrity, the suggested system provides pragmatic advantages to educators and learners alike. Exam distribution is streamlined to cut down on administrative work and lower the possibility of mistakes that come with handling exam materials by hand. Additionally, the system's real-time monitoring and auditing features let teachers keep tabs on exam progress and quickly spot irregularities. All things considered, the addition of fingerprint-based exam sheet authentication is a major step toward maintaining academic honesty and equity in learning evaluations. Institutions can reduce the likelihood of academic dishonesty, safeguard the validity of academic credentials, and preserve the values of honesty and integrity in education by utilizing biometric technology.

**Keywords:** Authentication, Finger print, security

## INTRODUCTION

In the current educational environment, upholding academic integrity and guaranteeing impartial evaluations are of utmost importance to establishments across the globe. Traditional approaches to exam administration and monitoring have proven ineffective in preventing academic dishonesty due to the development of digital technologies and the increasing sophistication of cheating tactics. The demand for creative solutions that use technology to support the values of justice, honesty, and integrity in education is developing in response to these issues.

This study's main goal is to investigate the viability and efficiency of using fingerprints to identify exam sheets in educational environments. Through an analysis of the possible advantages, difficulties, and consequences of this kind of system, this study hopes to add to the current conversation around assessment security and academic integrity.

The permanent nature and inherent distinctiveness of fingerprints make them a valuable tool for fingerprint-based identity verification. A trustworthy and impenetrable form of authentication is provided by fingerprints, as opposed to ID cards or passwords, which are easily shared, lost, or stolen. Since every person's fingerprint is different, it is quite difficult for someone to pretend to be someone else. Furthermore, a person's fingerprints don't change over time, adding to the identification procedure' dependability and durability.

This study's main goal is to investigate the viability and efficiency of using fingerprints to identify exam sheets in educational environments. Through an analysis of the possible advantages, difficulties, and consequences of this kind of system, this study hopes to add to the current conversation around assessment security and academic integrity.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

To sum up, the incorporation of fingerprint-based exam sheet identification is a viable strategy for improving assessment security and academic integrity in educational settings. Through the utilization of fingerprints' distinct properties, this system provides a strong, dependable, and easy way to confirm student identities and stop exam cheating. This study aims to support the continuous efforts to preserve the values of integrity, justice, and honesty in education through empirical research and real-world application.

POWER SUPPLY

BLOCK DAIGRAM

The ac voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation.

A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.


Figure. 1

WORKING PRINCIPLE TRANSFORMER

The potential transformer will step down the power supply voltage (0-230V) to (0-6V) level. Then the secondary of the potential transformer will be connected to the precision rectifier, which is constructed with the help of op–amp. The advantages of using precision rectifier are it will give peak voltage output as DC, rest of the circuits will give only RMS output.

BRIDGE RECTIFIER

When four diodes are connected as shown in figure, the circuit is called as bridge rectifier. The input to the circuit is applied to the diagonally opposite corners of the network, and the output is taken from the remaining two corners.

Let us assume that the transformer is working properly and there is a positive potential, at point A and a negative potential at point B. the positive potential at point A will forward bias D3 and reverse bias D4.

The negative potential at point B will forward bias D1 and reverse D2. At this time D3 and D1 are forward biased and will allow current flow to pass through them; D4 and D2 are reverse biased and will block current flow.

The path for current flow is from point B through D1, up through RL, through D3, through the secondary of the transformer back to point B. this path is indicated by the solid arrows. Waveforms (1) and (2) can be observed across D1 and D3.

One-half cycle later the polarity across the secondary of the transformer reverse, forward biasing D2 and D4 and reverse biasing D1 and D3. Current flow will now be from point A through D4, up through RL, through D2, through the secondary of T1, and back to point A. This path is indicated by the broken arrows. Waveforms (3) and (4) can be observed across D2 and D4. The current flow through RL is always in the same direction. In flowing through RL this current develops a voltage corresponding to that shown waveform (5). Since current flows through the load (RL) during both half cycles of the applied voltage, this bridge rectifier is a full-wave rectifier.

One advantage of a bridge rectifier over a conventional full-wave rectifier is that with a given transformer the bridge rectifier produces a voltage output that is nearly twice that of the conventional full-wave circuit. This may be shown by assigning values to some of the components shown in views A and B. assume that the same transformer is used in both circuits. The peak voltage developed between points X and y is 1000 volts in both circuits. In the conventional full-wave circuit shown—in view A, the peak voltage from the center tap to either X or Y is 500 volts. Since only one diode can conduct at any instant, the maximum voltage that can be rectified at any instant is 500 volts.

The maximum voltage that appears across the load resistor is nearly-but never exceeds-500 v0lts, as result of the small voltage drop across the diode. In the bridge rectifier shown in view B, the maximum voltage that can be rectified is the

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

full secondary voltage, which is 1000 volts. Therefore, the peak output voltage across the load resistor is nearly 1000 volts. With both circuits using the same transformer, the bridge rectifier circuit produces a higher output voltage than the conventional full-wave rectifier circuit.

IC VOLTAGE REGULATOR

Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustably set voltage. The regulators can be selected for operation with load currents from hundreds of milli amperes to tens of amperes, corresponding to power ratings from milli watts to tens of watts.

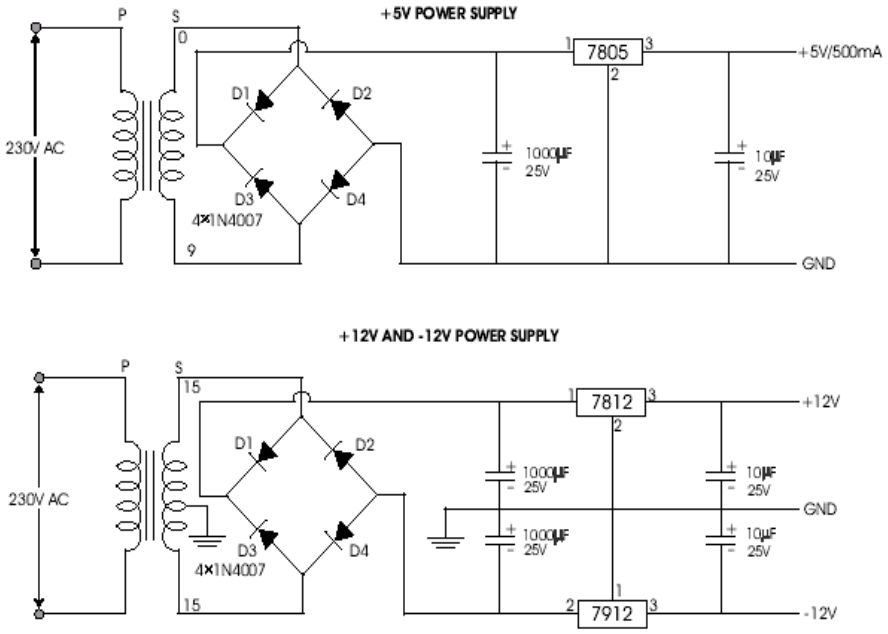



Figure. 2

A fixed three-terminal voltage regulator has an unregulated dc input voltage, Vi, applied to one input terminal, a regulated dc output voltage, Vo, from a second terminal, with the third terminal connected to ground.

The series 78 regulators provide fixed positive regulated voltages from 5 to 24 volts. Similarly, the series 79 regulators provide fixed negative regulated voltages from 5 to 24 volts.

For ICs, microcontroller, LCD --------- 5 volts

For alarm circuit, op-amp, relay circuits ---------- 12 volts

TABLE 19.1 Positive Voltage Regulators in 7800 series

| IC Part | Output Voltage (V) | Minimum Vi (V) |
|---|---|---|
| 7805 | +5 | 7.3 |
| 7806 | +6 | 8.3 |
| 7808 | +8 | 10.5 |
| 7810 | +10 | 12.5 |
| 7812 | +12 | 14.6 |
| 7815 | +15 | 17.7 |
| 7818 | +18 | 21.0 |
| 7824 | +24 | 27.1 |

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

KEY PAD GENERAL EXPLANATION:

A group of keys in a single printed circuit board is call key pad. These key pads are classified into two types.

Key pad
Matrix keypad
In a key pad it has a one or more then one keys are placed in a PCB. And all the keys are commonly grounded. This is the main difference to compared to matrix keypad. This key pads having maximum 8 numbers of keys. more then 8 keys are can not be connected because its not a efficient one. If we need more then 8 kays means, then only we can operate it a matrix keypad.

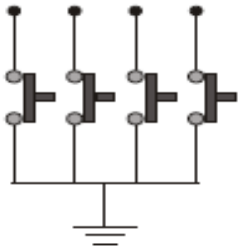


Figure. 3

MATRIX KEYPAD:
Above same keys are connected in a matrix principle it is called as a matrix key pad. This matrix key pad is working with the help of software. Otherwise it can not work. This key pad is normally 3X3, 4X3, 4X4 like that.

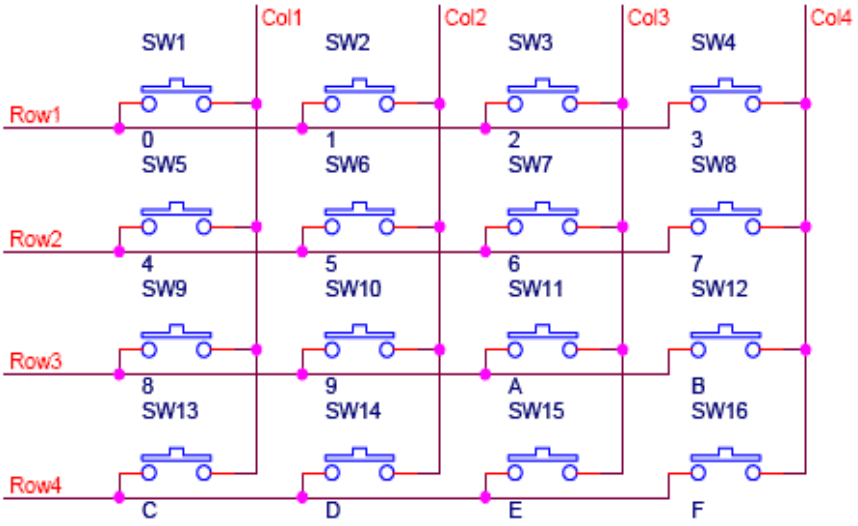



Figure. 4

SCHMATIC EXPLANATION:
There are many methods depending on how you connect your keypad with your controller, but the basic logic is same. We make the columns as i/p and we drive the rows making them o/p, this whole procedure of reading the keyboard is called scanning. In order to detect which key is pressed from the matrix, we make row lines low one by one and read the columns. Lets say we first make Row1 low, then read the columns. If any of the key in row1 is pressed will make the corresponding column as low i.e. if second key is pressed in Row1, then column2 will give low. So we come to know that key 2 of Row1 is pressed.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

This is how scanning is done. So to scan the keypad completely, we need to make rows low one by one and read the columns. If any of the button is pressed in a row, it will take the corresponding column to a low state which tells us that a key is pressed in that row. If button 1 of a row is pressed then Column 1 will become low, if button 2 then column2 and so on…

KEY :

Figure. 5

KEY DIMENSSIONS:

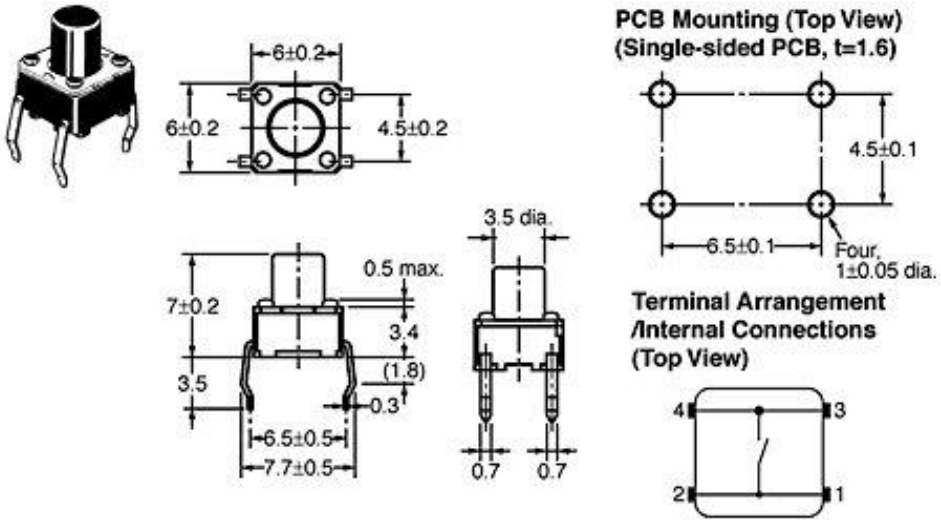
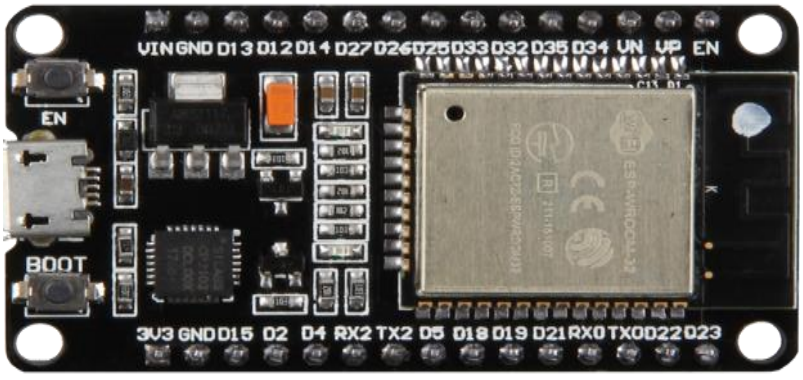



Figure. 6

ESP32 NODEMCU




© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

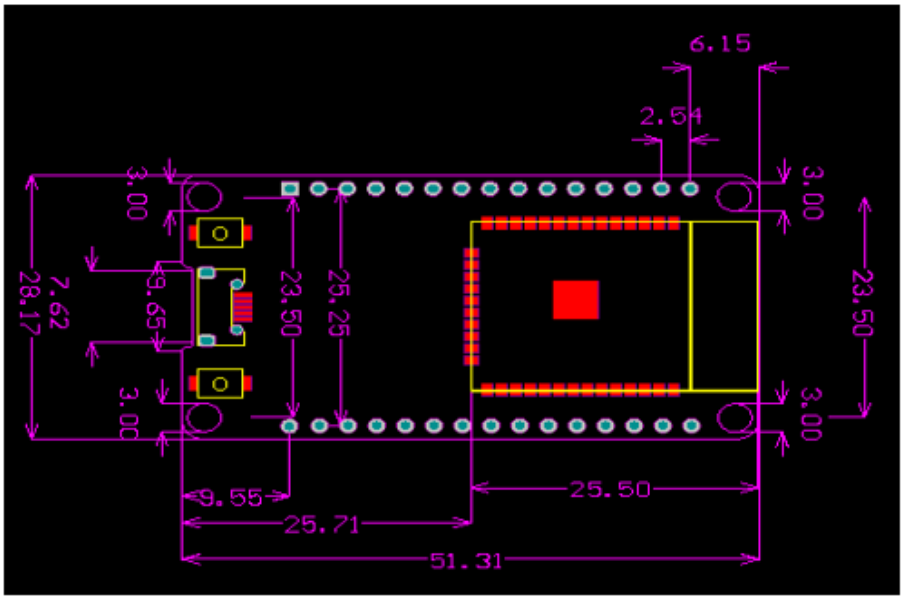



Figure. 7

This is ESP WROOM 32 MCU Module. ESP WROOM 32 is a powerful, generic WiFi-BT-BLE MCU module that targets a wide variety of applications, ranging from low-power sensor networks to the most demanding tasks, such as voice encoding, music streaming, and MP3 decoding.

At the core of this module is the ESP32S chip, which is designed to be scalable and adaptive. There are 2 CPU cores that can be individually controlled or powered, and the clock frequency is adjustable from 80 MHz to 240 MHz. The user may also power off the CPU and make use of the low-power coprocessor to constantly monitor the peripherals for changes or crossing of thresholds.

ESP32S integrates a rich set of peripherals, ranging from capacitive touch sensors, Hall sensors, low-noise sense amplifiers, SD card interface, Ethernet, high-speed SDIO/SPI, UART, and I²C.Using Bluetooth, users can connect to their phone or broadcast low energy beacons for its detection. The use of Wi-Fi enables a large physical range, as well as a direct connection to the internet via a Wi-Fi router. Perfect for wearable electronic or battery-powered applications, the ESP32 chip uses less than 5µA.

In addition, this module can support data rates of up to 150 Mbps and 22 dBm output power at the PA in order to allow for the widest physical range.

Application:

Universal low power IoT sensor hub.
Home automation.
Universal low power IoT recorder.
Mesh network.
Video streaming of the camera.
Industrial wireless control.
OTT TV box / set-top box device.
Baby monitor.
Smart Socket.
Sensor networks.
Wi-Fi toys: Counters, toys, Anti-lost device.
Wearable electronic products.
Wi-Fi speech recognition device.
Wi-Fi location-aware devices.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

Features:
Integrated 520 KB SRAM.
Hybrid Wi-FI & Bluetooth.
High level of integration.
Ultra-low-power management.
4 MB Flash.
On-board PCB antenna.

| | |
|---|---|
| Processor | Two Low-Power Xtensa 32-bit LX6 Microprocessors |
| Operating voltage (v) | 3.0V – 3.6V |
| Operating current (mA) | 80 |
| Clock Frequency (MHz) | 80 ~ 240 |
| Flash memory (MB) | 4 |
| Data Rate (Mbps) | 150 |
| SRAM Memory (KB) | 520 |
| Length (mm) | 28 |
| Width (mm) | 50 |
| Height (mm) | 14 |
| Weight (gm) | 10 |

ESP32 is one such microcontroller that can be used to start learning IOT and making IOT circuits. It is therefore important to learn about its pins layout and also what is the purpose of each pin and how it can be used. In this article, first, the layout of pins available in ESP32 Wroom 30-pin microcontroller is specified.

Then the different types of pins that are available in ESP32 are described. ESP32 is used for a variety of applications including the use of wifi, transmitters, and receiver devices, Serial Peripheral Interfaces, analog and digital devices, and lots of sensors.

ESP32 Pins Types Descriptions

Step 1 − Describe the Power Pins of ESP32.
Step 2 − Describe the GPIO Pins of ESP32.
Step 3 − Describe the Analog Pins of ESP32.
Step 4 − Describe the I2C Pins of ESP32.
Step 5 − Describe the DAC Pins of ESP32.
Step 6 − Describe the Touch Pins of ESP32.
Step 7 − Describe the Transmitter and Receiver Pins of ESP32.
Pin Layout of ESP32

This is how an ESP32 wroom 30 pin microcontroller looks like. ESP32 Wroom 30 pin microcontroller has 30 pins with 15 pins on one side and 15 pins on the other side.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

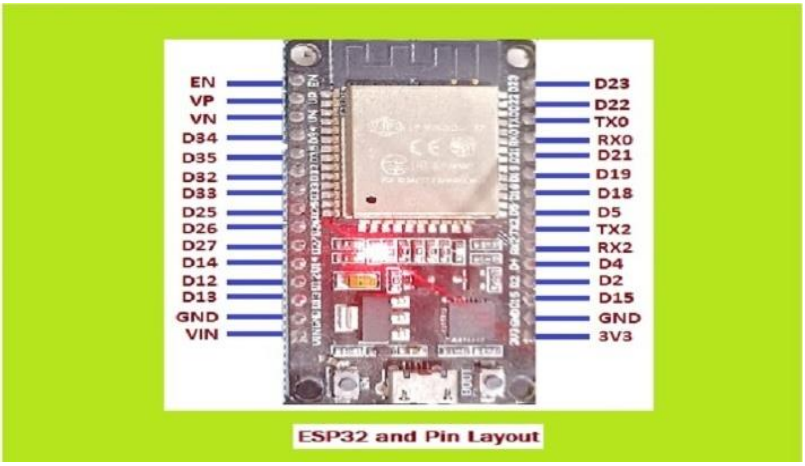



Figure. 8

The Power Pins of ESP32

ESP32 has 2 GND output pins. It has two pins for positive voltages, Vin and 3V3. Vin can be connected to an external voltage source of 5V to 14V. 3V3 is the pin that can output 3.3 volts and powers the ESP32.

General Purpose Input Output (GPIO) Pins of ESP32

There are 25 GPIO pins in ESP32 wroom 30 pin microcontroller. Although these can be used for different functions, there are some unsafe pins and these should be avoided, for example, RX0 and TX0. The safe-to-use pins are underlined here. All the GPIO pins are listed with GPIO numbers in the following table:

| GPIO Pins | ESP32 Pins |
|---|---|
| GPIO 1 | TX0 |
| GPIO 2 | D2 |
| GPIO 3 | RX0 |
| GPIO 4 | D4 |
| GPIO 5 | D5 |
| GPIO 12 | D12 |
| GPIO 13 | D13 |
| GPIO 14 | D14 |
| GPIO 15 | D15 |
| GPIO 16 | RX2 |
| GPIO 17 | TX2 |
| GPIO 18 | D18 |
| GPIO 19 | D19 |
| GPIO 21 | D21 |
| GPIO 22 | D22 |
| GPIO 23 | D23 |
| GPIO 25 | D25 |
| GPIO 26 | D26 |
| GPIO 27 | D27 |
| GPIO 32 | D32 |
| GPIO 33 | D33 |
| GPIO 34 | D34 |
| GPIO 35 | D35 |
| GPIO 36 | VP |
| GPIO 39 | VN |

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

Analog Pins of ESP32:

SP32 has 15 analog-enabled pins called ADC pins. The Analog to Digital converters ADC1 and ADC2 of ESP32 can be used to map the voltages from 0V to 3.3 V to numbers between 0 to 4096. All the analog pins are listed with numbers in the following table:

| Analog Pins | ESP32 Pins |
|---|---|
| ADC2_0 | D4 |
| ADC2_2 | D2 |
| ADC1_0 | VP |
| ADC1_3 | VN |
| ADC1_4 | D32 |
| ADC1_5 | D33 |
| ADC1_6 | D34 |
| ADC1_7 | D35 |
| ADC1_8 | D25 |
| ADC1_9 | D26 |
| ADC2_0 | D4 |
| ADC2_2 | D2 |
| ADC2_3 | D15 |
| ADC2_4 | D13 |
| ADC2_5 | D12 |
| ADC2_6 | D14 |
| ADC2_7 | D27 |

I2C (Inter-Integrated Circuit) Interface of ESP32:

I2C interface of ESP32 is used for communications between ESP32 (Master) and sensors (Slaves). For such communications, the ESP32's D22 and D21 pins are allocated. All the I2C pins are listed with PINs in the following table:

| For I2C Communications | ESP32 Pins |
|---|---|
| SCL | D17 |
| SDA | D16 |

DAC Pins of ESP32:

| DAC Pins | ESP32 Pins |
|---|---|
| DAC1 | D25 |
| **DAC2** | **D26** |

Touch Pins of ESP32

There are 9 touch pins in ESP32 wroom 30 pin microcontroller. They are listed from Touch 0 to T9 excluding T1 which is not there in the 30-pin microcontroller.

| Touch Pins | ESP32 Pins |
|---|---|
| Touch 0 | D4 |
| Touch 2 | D2 |
| Touch 3 | D15 |
| Touch 4 | D13 |
| Touch 5 | D12 |
| Touch 6 | D14 |
| Touch 7 | D27 |
| Touch 8 | D33 |
| Touch 9 | D32 |

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

Transmitter and Receiver Pins of ESP32:

Although ESP32 has three UART (Universal Asynchronous Receiver Transmitter) interfaces, only the following pins of UART2 are safe options to use while using the devices like distance sensors.

In this article, first, the pin diagram of ESP32 wroom 30-pin microcontroller is given. The ESP32 microcontroller can be used for a variety of applications while making IOT circuits. Its pins can be used as GPIO pins, analog pins, touch pins, UART pins, receiver/ transmitter, I2C communications, or for other purposes such as basic power connections. In this article, first, the pin layout is given, then the pins are presented in tabular forms after differentiating these into different categories. Along with the specified purpose for which the pins can be used,

| Transmitter/ Receiver Pins | ESP32 Pins |
|---|---|
| TX2 | D22 |
| RX2 | D21 |

Fingerprint Identification Module:


Figure. 9

This is a fingure print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port.

Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks.

Features
Integrated image collecting and algorithm chip together, ALL-in-One
Fingerprint reader can conduct secondary development, can be embedded into a variety of end products
Low power consumption, low cost, small size, excellent performance
Professional optical technology, precise module manufacturing techniques
Good image processing capabilities, can successfully capture image up to resolution 500 dpi
Specifications
Fingerprint sensor type: Optical
Sensor Life: 100 million times
Static indicators: 15KVBacklight: bright green
Interface: USB1.1/UART(TTL logical level)
RS232 communication baud rate: 4800BPS~115200BPS changeable
Dimension: 55*32*21.5mm
Image Capture Surface 15—18(mm)
Verification Speed: 0.3 sec
Scanning Speed: 0.5 sec
Character file size: 256 bytes

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11424

Template size: 512 bytes
Storage capacity: 250
Security level: 5 (1,2,3,4,5(highest))
False Acceptance Rate (FAR) :0.0001%
False Rejection Rate (FRR): 0.1%
Resolution 500 DPI
Voltage :3.6-6.0 VDC
Working current: Typical 90 mA, Peak 150mA
Matching Method: 1: N
Operating Environment Temperature: -20 to 45° centigrades

## CONCLUSION

It used to take a long time for pupils as well as instructors to manually record each student's attendance in the test room. A facial identification system, which is often used to verify users via identification verification services, operates by recognizing and quantifying face features in a given image. A collection of features may be used to compare an individual's face to an electronic image or a video clip. A technology for recognizing faces has been developed that is prepared to be used in the proposed system for the purpose of live examinee authentication with little to no human intervention to validate the candidate. This system is a study of the various attendance-taking tools currently available. Additionally, a completely computerized system may take its place. The administration of exam attendance may be improved with the use of this method. The administration will have to perform less work and will save time thanks to this approach. The recommended classification performance evaluation in terms of specificity, sensitivity, precision, accuracy, and score has been demonstrated using a confusion matrix. The recommended classification fared better than 10 current state-of-the-art classifiers in terms of recognition precision, according to the findings.

## REFERENCES

[1] "The 8051 Microcontroller and Embedded systems" by Muhammad Ali Mazidi and Janice Gillispie Mazidi, Pearson Education.
[2] Artificial „Gummy" Fingers on Fingerprint Systems", Proceedings of SPIE,.
[3] E. I. Bridget, Examination Verification System Using Biometric (A Case Study of WAEC), July 2013.
[4] J.Galbally , S.Marcel, and J.Fierrez, "Biometric antispoofing methods : A survey in face recognition ,"IEEE Access, Vol.2,pp.1530-1552,2014.
[5] A.Toosi, A.Bottino , S.Cumani ,P. Negri, and P.L.Sottile,"Feature fusion for finger print liveness detection: a comparative study,"IEEE Access , vol.5,pp.23 695-23 709,2017.
[6] L. S. Ezema, C. K. A. Joe-Uzuegbu, J. N. Eneh and I. Amanze, "Fingerprint based exam hall authentication system using microcontroller," International Journal of Scientific and Engineering Research, Volume 6, Issue 7, July 2015

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License